NUOVA EDIZIONE
SETTEMBRE 2018

Rapporto

Clusit

2018

sulla sicurezza ICT
in Italia

SECURITY 10 ANNI
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Indice

Prefazione di Gabriele Faggioli **5**

Introduzione al Rapporto **7**

Panoramica dei cyber attacchi più significativi del 2017 e del primo semestre 2018

- Introduzione alla tredicesima edizione 9
- Analisi dei principali cyber attacchi noti a livello globale del primo semestre 2018 15
- Analisi FASTWEB della situazione italiana in materia di cyber-crime e incidenti informatici 33
- Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2017 47
- Il punto di vista del CERT-PA 53
- Attività e segnalazioni del CERT Nazionale 61
- Rapporto 2017 sullo stato di Internet e analisi globale degli attacchi DDoS e applicativi Web 73
- Ransomware 2017 in Italia - WannaCry, NotPetya/EternalPetya, BadRabbit... ma non solo 85

SPECIALE FINANCE

- Elementi sul Cyber-crime nel settore finanziario in Europa 95
- Analisi del Cyber-crime in Italia in ambito finanziario nel 2017 106
- Carding - Tecniche di vendita: evoluzioni recenti e future 117

SPECIALE GDPR

- GDPR ai blocchi di partenza 129
- Il percorso verso il GDPR - Survey a cura dell'Osservatorio Information Security & Privacy del Politecnico di Milano 137
- La notifica del Data breach: opportunità o adempimento burocratico? 145

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC **155**

FOCUS ON 2018

- INDUSTRY 4.0: La nuova frontiera dei cyber criminali nell'anno del GDPR 169
- Maritime e Sicurezza IT 177
- Email Security: I trend rilevati in Italia nel corso del 2017 185
- Attacchi e difese nel Cloud Computing nel 2017 194
- La Cyber Security, una priorità per il Board 203
- La governance dei fornitori: adottare un maturity model efficace 211

- Il fattore umano nella gestione dell'innovazione e dell'information security aziendale (Social Engineering e Social Profiling) 216
- La diffusione delle criptovalute: rischi e opportunità in tema di sicurezza e regolamentazione del mercato 222

Glossario **235**

Gli autori del Rapporto Clusit 2018 . . . . . **252**

Descrizione CLUSIT e Security Summit **271**

ASTREA Advanced Security Training Research, Events Agency Via Copernico, 38 - 20125 Milano

Prefazione

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una serie di fonti e che non può che farci giungere a una sola conclusione: nel 2017 il cybercrime è andato del tutto fuori controllo.

La stima dei danni globali causati dal fenomeno ammontano a circa 500 miliardi di dollari. Si tratta di un vero e proprio "salto quantico".

Mentre scrivo queste righe si sta votando in Italia.
Si tratta di elezioni politiche di grande importanza cadute in un momento di attenzione mediatica spasmodica sul fenomeno cybercrime e di grandi investimenti in sicurezza perlomeno sul fronte delle aziende grandi e grandissime per via dei progetti di adeguamento al GDPR. Tuttavia, nonostante questa "tenaglia" mediatico/normativa che ben difficilmente si ripresenterà nel breve periodo, la campagna elettorale non ha tenuto in nessuna considerazione il tema della sicurezza informatica e della necessità di aumento dell'attenzione dei cittadini, della pubblica amministrazione e delle imprese su questo fenomeno.

In termini numerici, nel Report leggerete che si è assistito ad una crescita del 240% degli attacchi informatici rispetto al 2011, anno a cui risale la prima edizione del Rapporto Clusit, e del 7% rispetto al 2016. Ma non è tanto il dato numerico a spaventare quanto invece l'elemento qualitativo sottostante: oggi il fenomeno mira a interferire in maniera pesante non solo nella vita privata dei cittadini (peraltro vittime nel 2017 di crimini estorsivi su larghissima scala) quanto invece sul piano finanziario e geopolitico.
Insomma, il gioco si fa serio e un altro innalzamento del livello potrebbe non essere sopportabile.
Alcuni dati: il Rapporto Clusit 2018 sottolinea come il Cybercrime (la cui finalità ultima è sottrarre informazioni, denaro, o entrambi), è sempre la prima causa di attacchi gravi a livello mondiale (76% degli attacchi complessivi, in crescita del 14% rispetto al 2016).
Inoltre, sono in forte aumento rispetto gli attacchi compiuti con finalità di Information Warfare con un preoccupante +24% rispetto al 2016 ed ancora il Cyber Espionage (lo spionaggio con finalità geopolitiche o di tipo industriale, a cui va tra l'altro ricondotto il furto di proprietà intellettuale) cresce del 46% rispetto al precedente periodo di osservazione.
Il dato più interessante di tutti, e più preoccupante, è però quello relativo ai costi generati globalmente dalle sole attività del Cybercrime: dal Rapporto Clusit 2018 emerge infatti che sono quintuplicati per un importo complessivo, come già scritto a inizio prefazione, di 500 miliardi di dollari nel 2017. Si deve considerare, nel calcolo, che nel corso del 2017 truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari.
E l'Italia come è messa in questo contesto?
Sulla base delle cifre in gioco a livello globale noi stimiamo che l'Italia nel 2016 abbia subito danni derivanti da attività di cyber crimine per quasi 10 miliardi di euro. Non abbiamo dati

più recenti e non interessa forse neanche sapere se la cifra sovra o sottostima i danni.
L'ordine di grandezza è sintomatico di un problema più ampio perché comunque sia i danni appaiono essere 10 volte superiori alla stima degli investimenti in sicurezza risultate dalle ricerche dell'Osservatorio Sicurezza & Privacy del Politecnico di Milano.

Come nelle precedenti edizioni, il Rapporto Clusit 2018 dedica nei cosiddetti "Focus On" approfondimenti a singoli settori e a problematiche particolarmente attuali in tema di sicurezza cyber, a firma di esperti autorevoli. Quest'anno sono in evidenza la Sicurezza Marittima, l'Industria 4.0, il Cloud, la Mail Security, il Business Risk, le attività di Profiling, la diffusione delle criptovalute e la Blockchain, il Ransomware, la Gestione dei Fornitori.

Come già accaduto nei mesi precedenti al Rapporto Clusit 2017 l'attenzione mediatica sul tema è fortissima e si contano a centinaia se non a migliaia gli eventi che vengono organizzati in Italia e che ruotano attorno, in questo momento storico, alla sicurezza informatica e al GDPR.
Per questo motivo ci aspettiamo che gli investimenti in sicurezza aumentino così come ci attendiamo che sempre più forte sarà la spinta verso la esternalizzazione con la finalità di aumentare la sicurezza delle imprese e pubbliche amministrazioni che non avranno mai la capacità economica di proteggersi adeguatamente.

Vi lascio quindi alla lettura del Rapporto Clusit 2018 che avete fra le mani, augurandomi ancora una volta che la nostra ricerca serva ad aumentare la consapevolezza della necessità di una maggiore e sempre più efficace cultura della sicurezza informatica.

Ringrazio tutti coloro che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2018 e mi auguro che le elezioni politiche ci consegnino un governo ancora più attento a questa tematica e che miri alla cultura della sicurezza informatica fin dai più giovani e che completi e renda attuabile un quadro di indirizzo e normativo che permetta di raggiungere gli importanti traguardi necessari per vincere una sfida difficilissima.

2.500 copie cartacee, oltre 70.000 copie in elettronico e più di 300 articoli pubblicati nel 2017, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il rapporto inizia con una panoramica degli eventi di cyber-crime più significativi degli ultimi 12 mesi. Possiamo dire che il 2017 si è caratterizzato come "l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia". Per quanto riguarda gli impatti, i numeri parlano chiaro: nel periodo considerato dalle nostre analisi (2011-2017), i costi generati globalmente dalle sole attività cybercriminali sono quintuplicati, passando da poco più di 100 miliardi di dollari nel 2011 a oltre 500 miliardi nel 2017, quando truffe, estorsioni, furti di denaro e dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari. Fatte salve tutte le considerazioni di dettaglio a partire dai dati raccolti per il 2017, il problema più grave ed urgente rimane la cronica (e drammatica) insufficienza degli investimenti in cyber security nel nostro Paese, che ci pone sostanzialmente ultimi tra i paesi avanzati e rischia di condizionare seriamente lo sviluppo dell'Italia ed il benessere dei suoi cittadini nei prossimi anni.

Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB, che ha analizzato la situazione italiana sulla base di oltre 35 milioni di eventi di sicurezza (circa il doppio dell'anno scorso).
L'analisi degli attacchi è poi completata da due contributi tecnici: il "Rapporto 2017 sullo stato di Internet ed analisi globale degli attacchi DDoS e applicativi Web" e "Ransomware 2017 in Italia – WannaCry, NotPetya/EternalPetya, BadRabbit… ma non solo".
Seguono le rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni, del CERT Nazionale e del CERT-PA.

Presentiamo a questo punto l'abituale capitolo dedicato al settore FINANCE, con 3 contributi: "Elementi sul Cyber-crime nel settore finanziario in Europa"; "Analisi del Cyber-crime in Italia in ambito finanziario nel 2017"; "Carding – Tecniche di vendita: evoluzioni recenti e future".

Nel momento in cui sta andando in stampa il Rapporto Clusit, mancano solo novanta giorni alla scadenza del 25 maggio ma tutto il 2018 sarà l'anno di avvio dell'era del GDPR. Ci è parso quindi indispensabile inserire nel Rapporto 2018 uno "Speciale GDPR", che contiene 2 contributi, "GDPR ai blocchi di partenza" e "La notifica del Data breach: opportunità o adempimento burocratico?". Lo Speciale GDPR contiene anche i risultati di una survey realizzata dagli Osservatori del Politecnico di Milano sull'impatto del GDPR sulle aziende italiane.
Anche in questa edizione del rapporto, troviamo un'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.

Questi sono infine i temi trattati nella sezione FOCUS ON: «INDUSTRY 4.0: La nuova frontiera dei cyber criminali nell'anno del GDPR"; "Maritime e Sicurezza IT"; "Email Security: I trend rilevati in Italia nel corso del 2017"; "Attacchi e difese nel Cloud Computing nel 2017"; "La Cyber Security, una priorità per il Board; "La governance dei fornitori: adottare un maturity model efficace"; "Il fattore umano nella gestione dell'innovazione e dell'information security aziendale (Social Engineering e Social Profiling)"; "La diffusione delle criptovalute: rischi ed opportunità in tema di sicurezza e regolamentazione del mercato".

Analisi dei cyber attacchi più significativi del 2017 e del primo semestre 2018

Introduzione alla tredicesima edizione

Come di consueto in questo aggiornamento del Rapporto CLUSIT 2018, giunto ormai al suo settimo anno di pubblicazione[1], analizziamo i più gravi cyber attacchi noti (Italia inclusa) avvenuti a livello globale negli ultimi 15 semestri, e li confrontiamo con le tendenze emerse nei primi 6 mesi dell'anno in corso. A partire da questi dati proviamo a fornire un'interpretazione neutra e ragionata dell'evoluzione delle minacce cibernetiche nel mondo.
L'analisi è basata sull'attenta valutazione di tutte le informazioni pubblicamente disponibili in merito a un campione di attacchi "gravi" che, a questo punto, è costituito da oltre **7.500** incidenti noti avvenuti tra il gennaio 2011 e il giugno 2018 (dei quali oltre 1.100 nel 2017 e ben **730** nel primo semestre 2018), ed è volutamente espressa con un taglio divulgativo, non-tecnico, in modo da risultare fruibile al maggior numero possibile di lettori.
Come *premessa metodologica*, va sottolineato che le statistiche ed i commenti presentati di seguito sono relativi a un campione necessariamente limitato, per quanto ragionevolmente significativo, rispetto al numero degli attacchi informatici gravi effettivamente avvenuti nel periodo in esame.
Questo accade sia perché *un buon numero* di aggressioni non diventano *mai* di dominio pubblico, oppure lo diventano *ad anni di distanza,* quando le vittime ne vengono a conoscenza (solitamente quanto più gli attacchi sono sofisticati e gravi), sia perché in molti casi è interesse dei bersagli non pubblicizzare gli attacchi subiti, se non costretti da circostanze o normative particolari (come auspicabilmente avverrà da quest'anno, quantomeno in Europa, con la piena applicazione del Regolamento GDPR[2] e della Direttiva NIS[3]).
Per sua natura quindi il nostro campione, basato su dati di dominio pubblico, rappresenta una situazione *parziale e meno critica rispetto alla realtà*.
In particolare, in questo studio sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage ed information warfare, che emergono più difficilmente.
Ciò premesso, quest'anno per la prima volta introduciamo anche una *valutazione della gravità degli attacchi analizzati*, classificandoli in base a tre livelli di "Severity", e presentiamo alcune analisi statistiche in merito, il che ci consente di offrire nuovi spunti di riflessione a chi si occupi di cyber risk management e di cyber strategy, sia a livello aziendale che istituzionale, grazie alla maggiore comprensione dei rischi per macro-settore resa possibile da questo ulte-

[1] Ovvero alla tredicesima edizione, considerando anche gli aggiornamenti semestrali

[2] https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati

[3] https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf

riore elemento di analisi.
Confidando che anche quest'anno il Rapporto CLUSIT possa apportare un utile contributo all'evoluzione del dibattito nazionale in merito all'evoluzione costante (ed esponenziale) delle problematiche globali di sicurezza cibernetica, che si riflettono sempre più, inevitabilmente, anche sul buon funzionamento delle nostre istituzioni democratiche e sul benessere sociale ed economico del nostro Paese, auguriamo a tutti una buona lettura.

2017, il "salto quantico" della cyber-insecurity

Anticipando alcune delle conclusioni che seguono, sia pure alla luce delle cautele espresse più sopra in merito alla composizione del nostro campione, possiamo affermare che il 2017 è stato l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, evidenziando un trend di costante crescita degli attacchi, della loro gravità e dei danni conseguenti, trend che in base alle nostre analisi persiste ormai senza interruzione da 7 anni, e che il 2018 si appresta a battere questo triste primato.
Nel biennio 2016-2017, con un'accelerazione sensibile nell'ultimo anno, il livello di cyber-insicurezza ha effettuato globalmente un "salto quantico", un vero e proprio cambiamento di fase, tanto che il Ministro della Difesa tedesco Ursula von der Leyen ha recentemente affermato "*cyber attacks are the single greatest threat to global stability*"[4], mentre il World Economic Forum, nel suo ultimo Global Risk Report[5] pubblicato nel gennaio 2018, ha classificato i rischi derivanti da cyber attacchi al *terzo posto* tra i maggiori rischi globali[6], subito dopo disastri naturali ed eventi climatici estremi (nel Report 2011 erano semplicemente menzionati a margine, tra i "nuovi rischi da considerare").

Se dovessimo riassumere in tre concetti-chiave la situazione, potremmo dire che il 2017 si è caratterizzato come "l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia", il che è molto preoccupante, perché questo scenario prefigura concretamente l'eventualità di *attacchi con impatti sistemici molto gravi*.
Per comprendere il livello inaudito e straordinario di queste "nuove" minacce, ricordiamo le pesantissime interferenze di natura "cyber" avvenute durante le campagne presidenziali americana[7] e francese[8], gli attacchi realizzati tramite centinaia di migliaia di device IoT

4 https://www.cnbc.com/2018/02/17/munich-security-conference-german-defense-minister-on-global-stability.html
5 https://www.weforum.org/reports/the-global-risks-report-2018
6 https://www.infosecurity-magazine.com/news/cyberattacks-global-risk-2018/
7 http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/
8 https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html

compromessi[9], gli attacchi (spacciati per campagne ransomware) con finalità geopolitiche basati sui malware Wannacry e NotPetya, i furti per centinaia di milioni di dollari realizzati ai danni di primari istituti bancari (non quindi ai danni dei loro clienti) compromettendo il sistema SWIFT[10], i numerosi data breach che hanno coinvolto complessivamente miliardi di account[11], le crescenti applicazioni in ambito militare di tecniche e strumenti cyber[12], gli attacchi ad infrastrutture critiche[13], la diffusione endemica di crimini estorsivi realizzati su larga scala tramite attacchi basati su ransomware[14] e di cryptominers[15], etc.

In Italia, per quanto il numero di attacchi gravi di dominio pubblico presenti nel nostro campione sia bassissimo rispetto al totale (il che è dovuto *esclusivamente* alla scarsa propensione a denunciarli da parte delle nostre organizzazioni), ricordiamo la singolare vicenda di presunto spionaggio attribuita ai fratelli Occhionero[16], l'attacco ai sistemi non classificati della Farnesina[17], quello ad un sistema del Dipartimento per la Funzione Pubblica[18], l'attacco di Phishing (con malware allegato) contro oltre 200.000 vittime, quasi tutte italiane, realizzato in luglio dalla botnet Andromeda[19], attacchi contro gli utenti di una primaria telco[20] e di una primaria banca[21], il recente furto di quasi 200 milioni di dollari in cryptovalute da un Exchange italiano[22], etc.

Per quanto riguarda gli impatti, i numeri parlano chiaro: nel periodo considerato dalle nostre analisi (2011-2017), i costi generati globalmente dalle sole attività cybercriminali sono *quintuplicati*, passando da poco più di 100 miliardi di dollari[23] nel 2011 a oltre 500 miliardi nel 2017, quando truffe, estorsioni, furti di denaro e dati personali hanno colpito quasi un

---

9 https://www.darkreading.com/vulnerabilities---threats/satori-botnet-malware-now-can-infect-even-more-iot-devices/d/d-id/1330875?

10 https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack

11 https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/

12 https://themerkle.com/ukraines-power-grid-hacked-twice-in-one-year/

13 https://www.tripwire.com/state-of-security/featured/ransomware-hits-san-francisco-transport-system-free-rides-for-all-as-73000-demanded/

14 http://news.softpedia.com/news/one-single-ransomware-gang-made-over-121-million-508394.shtml

15 https://www.forbes.com/sites/tonybradley/2018/01/31/ransomware-and-cryptomining-spiked-in-2017-according-to-report/

16 http://formiche.net/2017/01/10/hacker-giulio-occhionero-renzi-monti-draghi/

17 http://www.analisidifesa.it/2017/02/lattacco-hacker-alla-farnesina/

18 http://news.softpedia.com/news/hacker-breaks-into-italian-government-website-45-000-users-exposed-510332.shtml

19 http://news.softpedia.com/news/andromeda-botnet-satisfies-pizza-craving-with-july-spam-campaign-targeting-italy-506415.shtml

20 http://csecybsec.com/download/zlab/20171202_CSE_3mobileUpdater_Report.pdf

21 http://news.softpedia.com/news/unicredit-bank-hacked-400-000-accounts-exposed-517184.shtml

22 http://www.ilsole24ore.com/art/finanza-e-mercati/2018-02-10/criptovalute-furto-200milioni-dollari-una-piattaforma-italiana-115147.shtml

23 https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0907_02

miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari[24].
Questo senza contare i danni causati dal furto di proprietà intellettuale realizzato da organizzazioni governative e para-governative dedite al Cyber Espionage (che nel 2017 ha generato solo negli Stati Uniti danni nell'ordine dei 600 miliardi di dollari[25]), né le conseguenze sistemiche generate dalle crescenti attività di Information Warfare (sia legate a finalità di psycological warfare e di influenza indebita che di vero e proprio conflitto), i cui impatti sono incalcolabili, ma sicuramente crescenti.
Tutto ciò ci porta a riflettere sul fatto che il Cybercrime, pur rappresentando un problema enorme e facendo la parte del leone nel nostro campione per le ragioni sopra esposte, è ormai diventato *l'ultimo dei nostri problemi in ambito cibernetico dal punto di vista della sua pericolosità intrinseca*, nel senso che purtroppo ormai ci troviamo a fronteggiare problemi *ben peggiori*.

Analizzando i dati del recente (febbraio 2018) Rapporto pubblicato dal Council of Economic Advisers (CEA) americano[26], si evince che nonostante tutti gli investimenti realizzati, nel 2016 il costo per l'economia USA derivante da "malicious cyber activity" è stato stimabile tra 57 e 109 miliardi di dollari, che corrispondono allo 0,3-06% del PIL americano di quell'anno, a fronte di una sua crescita del 1,6% nello stesso periodo. Visto diversamente, questo significa che nel 2016 il costo delle minacce cibernetiche ha rappresentato per gli USA l'equivalente di un terzo (o di un quarto) della crescita della loro economia.
Un altro studio relativo a perdite subite in UK nel 2016 dal solo settore business stima che 2,9 milioni di aziende inglesi siano state colpite da qualche tipo di attacco informatico, perdendo complessivamente 29 miliardi di sterline (40 miliardi di dollari)[27].
Sfortunatamente non possiamo, per la (ormai critica) mancanza di dati e statistiche ufficiali, svolgere una valutazione analoga per l'Italia, ma d'altra parte non possiamo ritenere che i danni subiti dal nostro Paese, a parità di tutte le altre condizioni al contorno, siano percentualmente molto distanti da quelli rilevati in altre nazioni avanzate come USA e UK. Se così fosse, a grandi linee e fatte le debite proporzioni, l'Italia nel 2016 avrebbe subito danni derivanti da sole attività cybercriminali per quasi *10 miliardi di euro*, pari quindi ad una frazione consistente della finanziaria di quell'anno[28] e a *dieci volte tanto* il valore attuale degli investimenti italiani in ICT Security29.

---

[24] https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking

[25] https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html

[26] https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

[27] https://www.itgovernance.co.uk/blog/2016-cyber-security-breaches-cost-uk-businesses-almost-30-billion/

[28] http://www.gazzettaufficiale.it/eli/id/2016/12/21/16G00242/sg

[29] http://www.infodata.ilsole24ore.com/2017/01/30/cybersicurezza-italia-investito-quasi-un-miliardo-euro/

Tutto ciò non implica che tutte le risorse umane e tecniche ed i processi di sicurezza cibernetica messi in campo in questi anni da privati e governi siano da considerare inutili, ed anzi possiamo ragionevolmente ipotizzare che senza di essi la situazione sarebbe risultata assai più grave, ma certamente siamo costretti a concludere, dati alla mano, che non siano stati sufficientemente efficaci da invertire le tendenze in atto – ciò che dovrebbe essere il nostro vero obiettivo, giunti a questo punto. Un anno fa, presentando con preoccupazione i dati relativi al 2016, scrivevamo:
Gli investimenti italiani in ICT Security (da non confondere, come spesso ancora accade, con la Cyber Security), pur essendo cresciuti in un anno del 5% e sfiorando ormai il miliardo di euro, sono risultati assolutamente insufficienti rispetto al valore del mercato italiano di beni e servizi ICT (pari a 66 miliardi di euro), e soprattutto rispetto alla percentuale di PIL che oggi viene generata grazie all'applicazione dell'ICT da parte di organizzazioni pubbliche e private e dai privati cittadini.

Fatte salve tutte le considerazioni di dettaglio che svolgeremo più avanti a partire dai dati raccolti per il 2017 e per il primo semestre 2018, a nostro avviso il problema più grave ed urgente rimane questo, ovvero la cronica (e drammatica) insufficienza degli investimenti in cyber security nel nostro Paese, che ci pone sostanzialmente ultimi tra i paesi avanzati e rischia di condizionare seriamente lo sviluppo dell'Italia ed il benessere dei suoi cittadini nei prossimi anni.
A titolo di esempio, senza voler sempre citare USA, UK, Francia o Germania, il governo dello stato americano della Georgia (10 milioni di abitanti, con un PIL pari a un quinto di quello italiano) nel 2018 investirà 60 milioni di dollari per istituire un Cyber Innovation and Training Center ed altri 35 per avviare un incubatore di aziende specializzate in cyber security[30], il che, fatte le proporzioni con i 150 milioni di euro di investimenti in cyber security annunciati dall'Italia nel 2016[31] ci fa ben comprendere il tipo di gap che dobbiamo colmare. Questa spesa, a valle di analisi quantitative puntuali, deve essere commisurata alle minacce ed ai danni attuali, pena (nel migliore dei casi) una crescente, significativa erosione dei benefici attesi dal processo di digitalizzazione della nostra società.

In questo senso, l'assordante silenzio di tutte le forze politiche sulle tematiche di sicurezza cibernetica nel corso della campagna elettorale[32] non fa ben sperare, ed anzi è sintomo di una drammatica mancanza di sensibilità in materia, che deve essere urgentemente ricondotta a dei livelli accettabili per un Paese tecnologicamente avanzato come il nostro, a fronte del rischio di un'ulteriore perdita di credibilità e competitività sul piano internazionale.
Ci sono anche segnali positivi, naturalmente: nel febbraio 2017 abbiamo rinnovato, semplificandolo e razionalizzandolo, l'assetto istituzionale della nostra difesa cibernetica con il

[30] https://www.scmagazine.com/the-economics-of-cybersecurity/article/720084/

[31] https://www.corrierecomunicazioni.it/digital-economy/cybersecurity-150-milioni-di-risorse-ecco-il-dettaglio-delle-spese/

[32] Al momento della stesura del Rapporto Clusit 2018

c.d. "Decreto Gentiloni"[33], mentre durante il G7 di Taormina del maggio 2017 i partecipanti hanno sottoscritto una "Declaration on Responsible States Behavior in Cyberspace"[34], fortemente voluta dall'Italia, che è un piccolo ma importante passo nel campo della Cyber Diplomacy. Non solo, nel marzo 2017 abbiamo aggiornato il "Piano nazionale per la protezione cibernetica e la sicurezza informatica"[35] del 2013, producendo un documento concreto, chiaro e puntuale, apprezzato in tutto il mondo, ma ora dobbiamo assolutamente dargli corpo e sostanza, anche alla luce di quanto emerso nella articolata "Relazione sulla politica dell'informazione per la sicurezza 2017", presentata al Parlamento a febbraio 2018[36].

Per questo una modifica *radicale* dell'attuale modello di investimenti in materia di sicurezza ICT non è più rimandabile (da conseguire tramite maggiore sensibilizzazione ed awareness, nuovi strumenti normativi, incentivazioni tramite sgravi fiscali e interventi diretti, forme di moral suasion, etc), anche considerato che le normative europee in via di applicazione (pensiamo in particolare alla GDPR, finalizzata alla tutela della privacy, o al NIS, che si applica solo a particolari settori critici) introducono obblighi e controlli che coprono *solo in piccola parte* le attuali problematiche di cyber security, e per loro natura non possono costituire, come molti sembrano pensare, la panacea di tutti i mali cibernetici.

Sottostimare i rischi, procrastinare l'adozione di contromisure adeguate ed affidarsi alla "buona sorte" o alla buona volontà dei singoli, oppure, come spesso accade in Italia, pretendere di poter "fare le nozze coi fichi secchi" non sono più opzioni percorribili.

[33] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

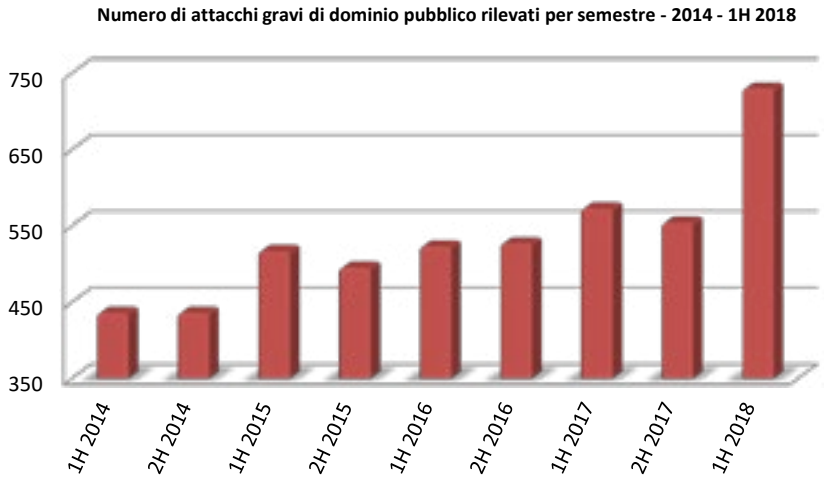
[34] https://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf

[35] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[36] http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf

Analisi dei principali cyber attacchi noti a livello globale del primo semestre 2018

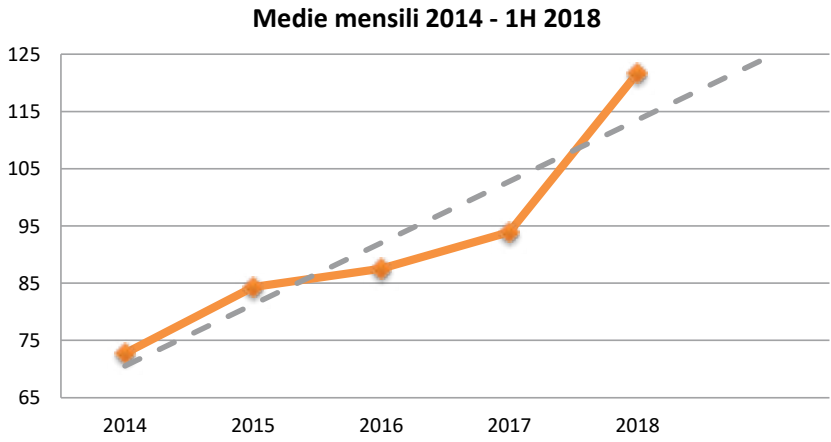
In questa sezione, come di consueto, il Rapporto CLUSIT 2018 propone una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nell'anno precedente, confrontandoli con una serie storica che parte dal 2011. Questa seconda edizione 2018 aggiorna i dati presentati a febbraio 2018 (relativi al 2017) con i dati relativi al primo semestre 2018.
Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del quadriennio 2014-2017, più restrittivi rispetto ai criteri che avevamo applicato negli anni 2011-2013, dal momento che nell'arco di questi 90 mesi si è verificata una sensibile evoluzione degli scenari e che alcune categorie di attacchi, che potevano essere ancora considerati "gravi" nel 2011-2013, sono oggi diventati *ordinaria amministrazione* (per esempio, i "defacement" di siti web).
Lo studio si basa su un campione che al 30 giugno 2018 è costituito da **7.595** attacchi noti di particolare gravità, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti, avvenuti nel mondo (inclusa quindi l'Italia) dal primo gennaio 2011, di cui **1.127** registrati nel 2017 (**+240%** rispetto al 2011, **+30%** rispetto al 2014 e **+ 7,33%** rispetto al 2016) e, dato mai registrato in precedenza dal 2011, ben **730** nel primo semestre 2018.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

A parità di criteri, in questo primo semestre 2018 abbiamo classificato come gravi un numero di attacchi superiore rispetto a tutti i semestri analizzati a partire dal 2014, pur scartando una grande quantità di incidenti "minori" per evitare di confrontare, nell'ambito dello stesso campione, situazioni che hanno causato la perdita di milioni di euro o il furto di milioni di account con, per fare un esempio tra molti, un attacco DDoS di lieve entità verso una banca o un sito web istituzionale. Ciò non significa che questo genere di attacchi ad impatto minore non sia a sua volta in rapida crescita.
Dal punto di vista numerico, dei 7.595 attacchi gravi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 15 semestri (7 anni e mezzo), nel primo semestre 2018 ne abbiamo raccolti e analizzati 730, contro i 554 del secondo semestre 2017 (+ **31,77**%) con una media di **122 attacchi gravi al mese** (rispetto ad una media di 94 al mese nel 2017, e di 88 sui 7 anni). Il picco maggiore di attacchi si è avuto nel febbraio 2018 con 139 attacchi, il valore più alto negli ultimi 4 anni e mezzo.

Queste le medie mensili degli attacchi registrati nel periodo 2014 – primo semestre 2018, suddivise per anno:



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

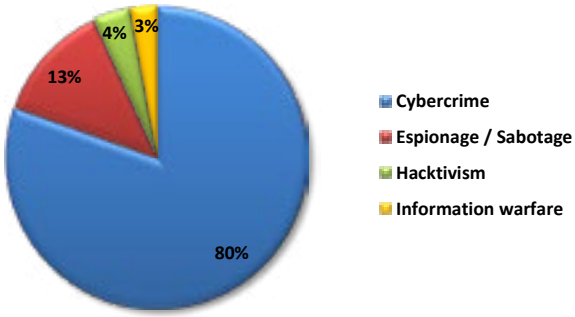
Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto. Come in passato abbiamo evidenziato nella colonna più a destra i trend osservati.
Da qui in avanti, per comodità di consultazione ed omogeneità dei criteri di classificazione degli attacchi, presentiamo il confronto solo dei dati dell'ultimo quadriennio, rimandando alle edizioni precedenti del Rapporto Clusit per i dati relativi al triennio 2011-2013.

Distribuzione degli attaccanti per tipologia

ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2H 2017	1H 2018	Variazioni 1H 2018 su 2H 2017	Trend 1H 2018
Cybercrime	526	684	751	857	434	587	35,25%	↑
Hacktivism	236	209	161	79	34	29	-14,71%	↓
Espionage / Sabotage	69	96	88	129	55	93	69,09%	↑
Information Warfare	42	23	50	62	31	21	-32,26%	↓
TOTALE	**873**	**1.012**	**1.050**	**1.127**	**554**	**730**	**+31,77%**	↑

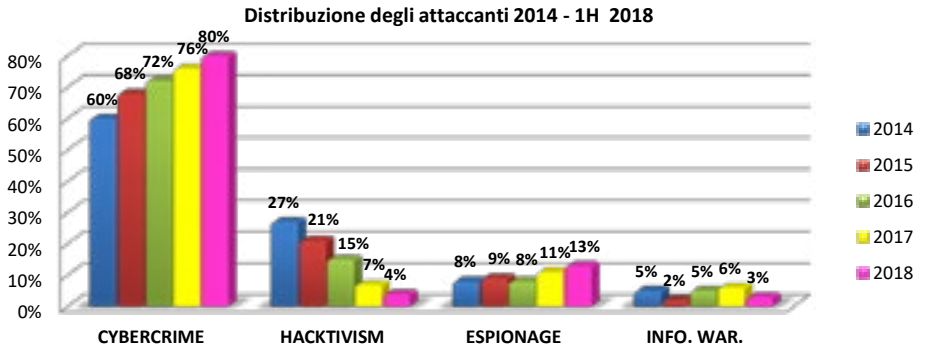
Complessivamente, rispetto al secondo semestre 2017, il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche per il primo semestre 2018 cresce del **31,77%**. In termini assoluti, nel 2017 le categorie "Cybercrime", "Cyber Espionage" e "Information Warfare" fanno registrare il numero di attacchi più elevato degli ultimi 7 anni. Nel 1H 2018 diminuisce ulteriormente la componente riferibile all'Hacktivism, sembra diminuire anche l'Information Warfare, mentre rispetto al 2H 2017 crescono in modo tangibile gli attacchi con motivazione cybercriminale **(+35%)** ed in modo impressionante quelli riferibili ad attività di cyber espionage **(+69%)**.
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra Information Warfare ed Espionage: sommando gli attacchi di entrambe le categorie presenti nel nostro campione, nel 1H 2018 si assiste ad un aumento importante rispetto al 2H 2017 (114 contro 86).

Tipologia e distribuzione degli attaccanti 1H 2018



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Già nel 2014 il Cybercrime si era confermato la prima causa di attacchi gravi a livello globale (60%), salendo al 68% dei casi analizzati nel 2015. Nel 2016 tale percentuale era il 72%, che sale al 76% nel 2017 ed all'**80%** nel 1H 2018, mostrando un trend inarrestabile. Va sottolineato che già dal 2015 si è assistito alla diffusione ormai endemica di attività cyber criminali "spicciole", che in questo campione di incidenti gravi non sono rappresentate (per esempio le quotidiane campagne di estorsione realizzate tramite phishing e ransomware, che hanno colpito moltissime organizzazioni e cittadini italiani), trend che si è ulteriormente rafforzato nel triennio 2016-2018.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

L'Hacktivism diminuisce ulteriormente, passando da quasi un terzo dei casi analizzati nel 2014 al **4%** del 1H 2018.

Per quanto riguarda le attività di Espionage (nonostante la scarsità di informazioni pubbliche in merito) rispetto al 2017 la loro percentuale sul totale passa dal 11% al **13%**, mentre l'Information Warfare mostra un calo, dal 6% al **3%**.

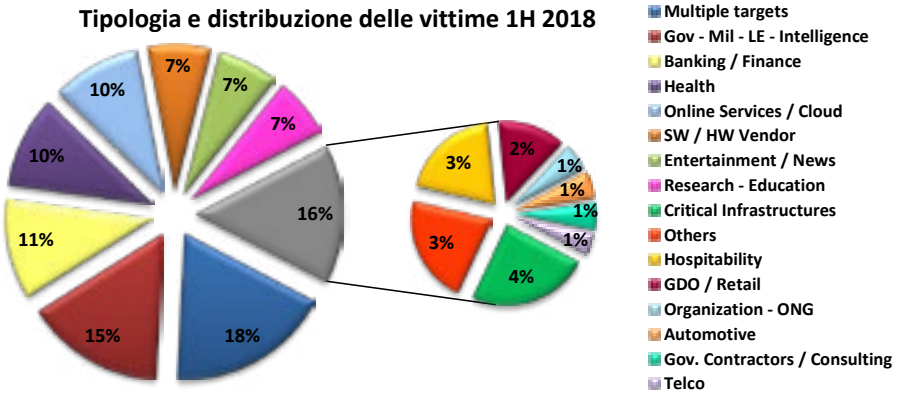
Distribuzione generale delle vittime per tipologia

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2H 2017	1H 2018	Variazioni 1H 2018 su 2H 2017	Trend 1H 2018
Institutions: Gov - Mil - LEAs - Intelligence	213	223	220	179	73	111	52,05%	
Others	172	51	38	40	19	24	26,32%	
Entertainment / News	77	138	131	115	49	49	0,00%	
Online Services / Cloud	103	187	179	95	47	71	51,06%	
Research - Education	54	82	55	71	21	48	128,57%	
Banking / Finance	50	64	105	117	71	80	12,68%	
Software / Hardware Vendor	44	55	56	68	41	50	21,95%	
Telco	18	18	14	13	8	5	-37,50%	
Gov. Contractors / Consulting	13	8	7	6	4	6	50,00%	
Security Industry	2	3	0	11	7	3	-57,14	
Religion	7	5	6	0	0	2	-	-
Health	32	36	73	80	45	73	62,22%	
Chemical(Medical	5	2	0	0	0	1	-	-
Critical Infrastructures	13	33	38	40	24	27	12,50%	
Automotive	3	5	4	4	2	6	200,00%	
Org / ONG	47	46	13	8	4	6	50,00%	
Multiple Targets	-	-	49	222	114	131	14,91%	
GDO / Retail	20	17	29	24	12	15	25,00%	
Hospitability	-	39	33	34	13	22	69,23%	

Rispetto al 2H 2017, nel 1H 2018 la crescita percentuale maggiore di attacchi gravi si osserva verso le categorie "Automotive" (**+200%**), "Research/Education" (**+128%**) e "Ho-

spitability" (**+69%**), seguite da "Health" (**+62%**), "Institutions" (**+52%**), "Online Services/ Cloud" (**+52%**) e da "Consulting" (**+50%**).
Dobbiamo qui sottolineare l'emergenza di un nuovo fenomeno, a nostro avviso molto importante, che conferma la nostra percezione di aver assistito nel 2017 ad un "salto quantico" nel livello della cyber-insicurezza globale.

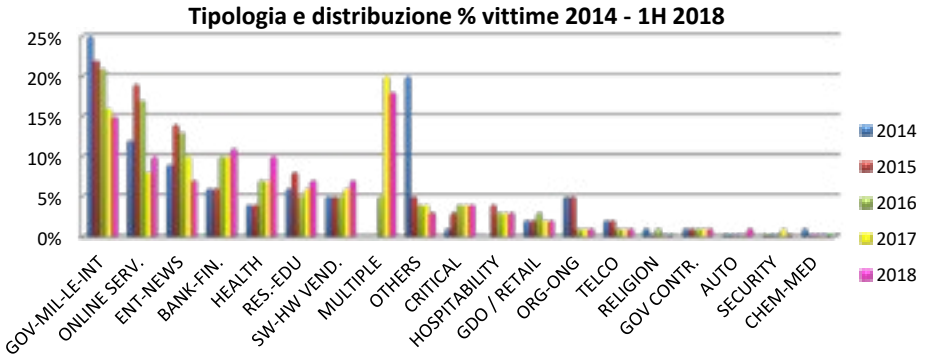
Nel 2016 abbiamo introdotto la nuova categoria "Multiple Targets", per rendere conto del crescente numero di attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti a categorie differenti, di conseguenza molti attacchi verso organizzazioni appartenenti ai settori più disparati sono oggi confluiti nella categoria, che rispetto al 2H 2017 cresce ulteriormente del **15%**.
All'interno della categoria "Multiple Targets", che rispetto al 2016 nel 2017 mostrava una *crescita a tre cifre*, sono compresi attacchi verso vittime appartenenti a *tutte le altre categorie*, a dimostrazione del fatto che non solo ormai tutti sono diventati bersagli, ma anche che gli attaccanti sono diventati sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando a massimizzare il risultato economico (si pensi ai furti di cryptovalute ai danni di grandi Exchange, ad esempio l'attacco a Coincheck[37]) o il danno inflitto alle vittime (come nel caso di NotPetya[38]), a seconda dei casi.
Per quanto riguarda la categoria "Ricettività" (Hospitability), introdotta nel 2015 per rendere conto di un certo numero di attacchi gravi verso organizzazione alberghiere, ristoranti, residence e collettività (tipicamente per colpirne gli utenti), tali attacchi proseguono anche nel 1H 2018, intensificandosi, crescendo del **69%**.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

[37] http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
[38] https://www.helpnetsecurity.com/2017/08/17/notpetya-losses/

Per i motivi sopra illustrati, anche nel 1H 2018 al primo posto assoluto si posiziona la categoria "Multiple Targets" (**18%**), superando anche questa volta il settore "Gov", in diminuzione al **15%**, che dal 2011 al 2016 è sempre stato al primo posto nel nostro studio.
Rispetto al 2017, "Banking/Finance" mantiene il terzo posto (**11%**), mentre "Health" balza al quarto posto (**10%**), con "Online Services / Cloud" (**10%**) e "Online Services/Cloud" (**10%**).
Salgono al **7%** "Software/Hardware Vendor", "Research/Education" e "Entertainment/News", mentre "Critical Infrastructures" sale al **4%** e la categoria "Others" (anche a causa dell'introduzione della nuova categoria "Multiple Targets"), scende al **3%**.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Tramite questo grafico si può apprezzare facilmente l'incremento straordinario degli attacchi gravi compiuti in parallelo verso bersagli multipli (quindi con impatti potenzialmente sistemici) occorso nel periodo 2017 – 1H 2018.

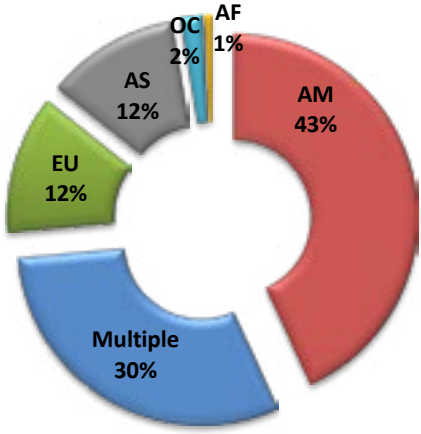
Distribuzione generale delle vittime per area geografica

La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.

Rispetto al 2017, nel 1H 2018 si confermano al primo posto le vittime di area americana (**43%**), mentre, in attesa che la piena applicazione di GDPR e NIS faccia emergere molti attacchi ad oggi non noti perché non denunciati dalle vittime, gli attacchi verso realtà basate in Europa scendono leggermente (dal 16% al **12%**) e aumentano quelli rilevati contro organizzazioni asiatiche (dal 10% al **12%**).

Crescono ancora, per i motivi esposti in precedenza, i singoli attacchi gravi verso bersagli multipli distribuiti globalmente (categoria "Multiple"), dall'11% del 2016 al **30%** del 1H 2018 (era il 28% nel 2017).

Appartenenza geografica delle vittime per continente 1H 2018

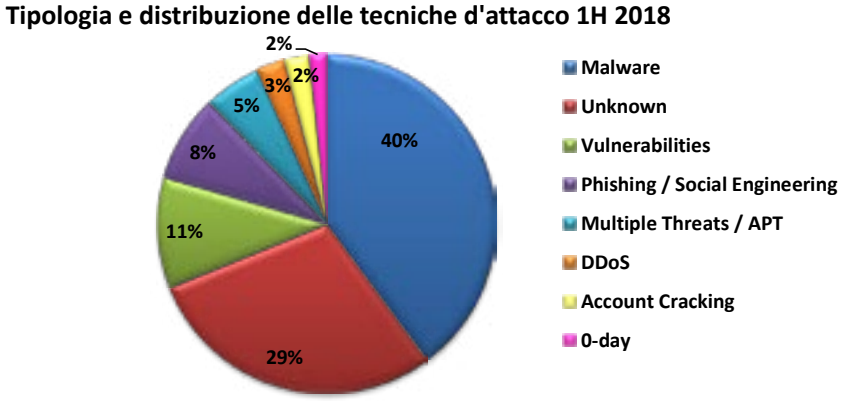


Distribuzione delle tecniche di attacco

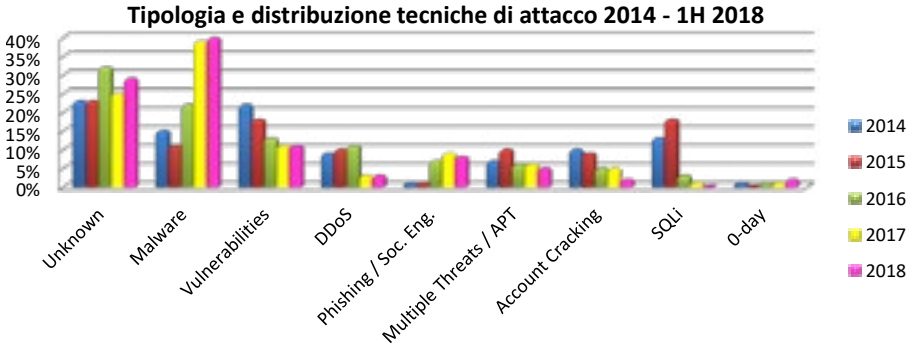
TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2H 2017	1H 2018	Variazioni 1H 2018 su 2H 2017	Trend 1H 2018
SQL Injection	110	184	35	7	1	0	-100,00%	
Unknown	199	232	338	277	137	212	54,74%	
DDoS	81	101	115	38	19	20	5,26%	
Known Vulnerabilities / Misconfigurations	195	184	136	127	56	77	37,50%	
Malware	127	106	229	446	237	291	22,78%	
Account Cracking	86	91	46	52	20	17	-15,00%	
Phishing / Social Engineering	4	6	76	102	50	61	22,00%	
Multiple Techniques / APT	60	104	59	63	27	40	48,15%	
0-day	8	3	13	12	5	12	140,00%	
Phone Hacking	3	1	3	3	2	0	-100,00%	

Le tecniche sconosciute (categoria "Unknown") passano al secondo posto con una crescita del **54%** rispetto al 2H 2017, superate dalla categoria "Malware" che si conferma al primo posto. L'uso di Malware come vettore di attacco aumenta sensibilmente nel 1H 2018, facendo segnare una crescita del **22%** rispetto al 2017. A questo dato va sommata la crescita della categoria "Multiple Threats / APT" (**+48%**), che include attacchi più articolati e sofisticati, per quanto quasi sempre basati *anche* sull'utilizzo di malware.

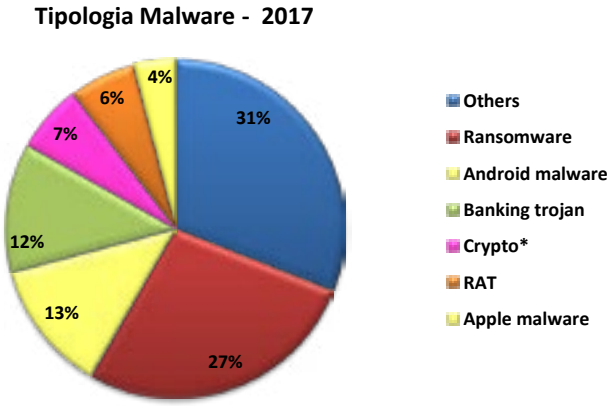
I DDoS crescono leggermente del **5%** mentre le SQL injection sembrano ormai un problema superato, quantomeno all'interno del nostro campione di attacchi gravi. Lo sfruttamento di vulnerabilità note ritorna a crescere (**+37%**), così come cresce in modo impressionante l'utilizzo di vulnerabilità "0-day", (**+140%**), per quanto questo dato sia ricavato da un numero di incidenti noti limitato e risulti probabilmente sottostimato. In calo gli attacchi basati su tecniche di "Account Cracking" (**-15%**).
In sostanza ormai gli attaccanti possono fare sempre più affidamento sull'efficacia del malware "semplice", prodotto industrialmente a costi decrescenti, e delle tecniche di Phishing / Social engineering (**+22%**), per conseguire la gran maggioranza dei loro obiettivi, ma dimostrano anche una sofisticazione crescente (sensibile aumento di "0day" e "Multiple Techniques").



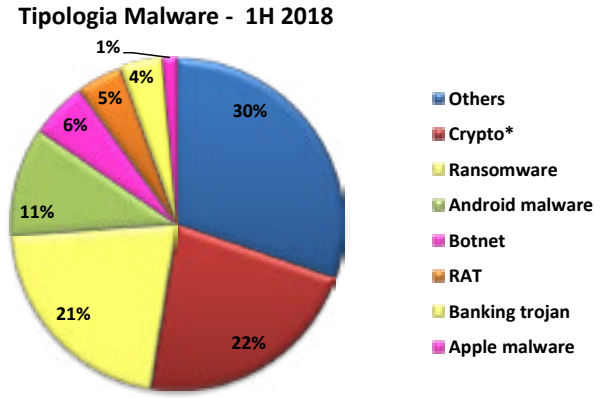
Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, Phishing, malware "semplice") rappresenti nel 1H 2018 ancora il **61%** del totale (era il 68% nel 2017), implica che gli attaccanti *riescono ancora a realizzare attacchi di successo contro le loro vittime con relativa semplicità e a costi molto bassi, oltretutto decrescenti* – forse una delle considerazioni più preoccupanti tra tutte quelle svolte fin qui.



Data la crescita impressionante della categoria Malware, da quest'anno presentiamo anche un'analisi di dettaglio relativa alle tipologie di malware osservate nel nostro campione. Di seguito la situazione nel 2017 e l'evoluzione nel 1H 2018.



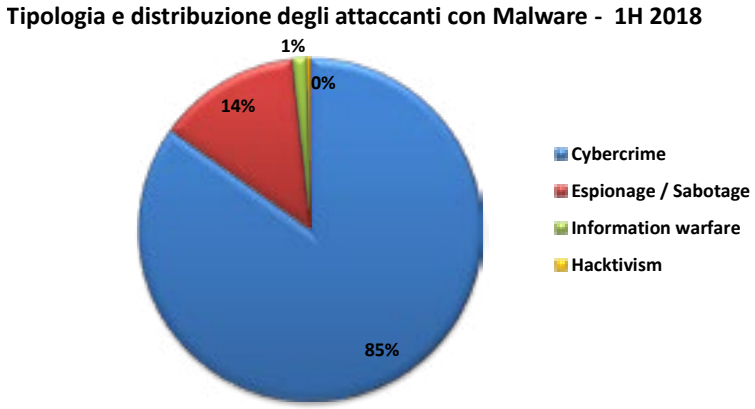
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia



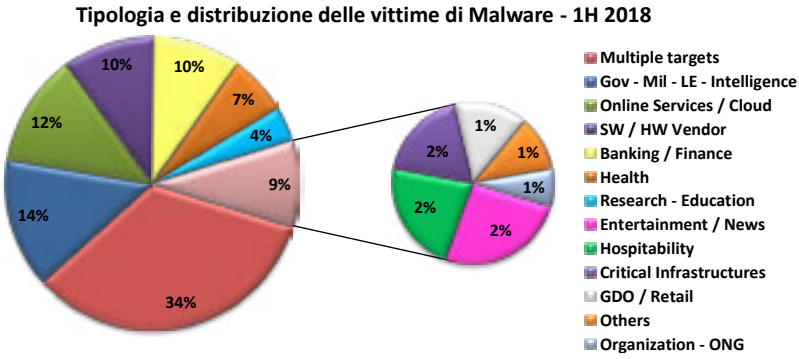
© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Dal grafico si possono osservare alcuni fenomeni interessanti, tra questi che i Cryptominers, quasi inesistenti in passato, nel corso del 2017 sono arrivati a rappresentare il 7% del totale e nel 1H 2018 hanno raggiunto il **22%**, superando di poco i Ransomware (+21%), a dimostrazione della dinamicità degli attaccanti e della rapidità con la quale evolvono le minacce.

Ad oggi quindi Ransomware e Cryptominers rappresentano il 43% del malware "semplice" utilizzato. Nel grafico successivo si può osservare la distribuzione percentuale dell'uso di malware in base alle categorie di attaccanti, con una evidente e schiacciante percentuale di attacchi realizzati dalla categoria Cybercrime (85%).



Infine, per la prima volta rappresentiamo con un grafico la distribuzione delle vittime colpite da malware:



Come è ragionevole aspettarsi, al primo posto troviamo la categoria "Multiple Targets" (**34%**), a dimostrazione della **scala planetaria del Cybercrime** e del fatto che il malware "semplice", prodotto industrialmente in infinite varianti aggiornate quotidianamente, viene

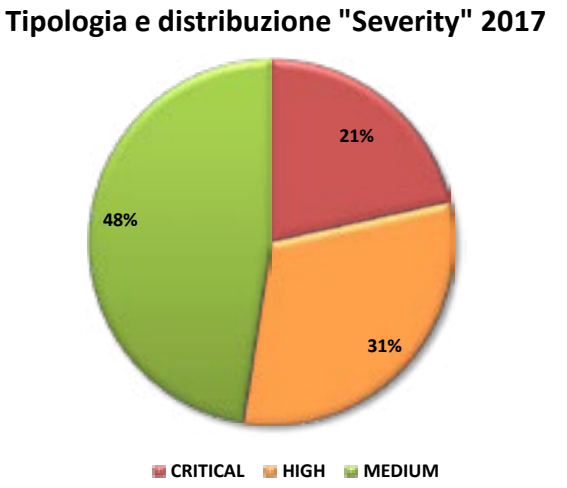
usato principalmente per realizzare campagne criminali globali, che prescindono cioè da area geografica e settore merceologico / dimensione delle vittime.

Analisi della "Severity" degli attacchi

Come anticipato nell'introduzione di questa analisi, dal 2017 abbiamo introdotto una significativa novità, che ha richiesto da un lato un profondo aggiornamento del nostro approccio nell'analizzare e classificare gli attacchi del nostro campione e, dall'altro, l'utilizzo di maggiore tempo e risorse.

Abbiamo definito tre categorie o livelli di **impatto** (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come "gravi"): Medio, Alto e Critico.
Va premesso che questo genere di analisi si scontra spesso con la scarsità di informazioni dettagliate di dominio pubblico relative ai singoli incidenti, e che pertanto deve considerarsi basata su una stima necessariamente ad alto livello degli impatti.

Le variabili che contribuiscono a comporre la valutazione dell'impatto per ogni singolo attacco analizzato sono molteplici, ed includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.
Per il 2017, l'analisi degli impatti stimati ci presentava questo quadro generale:

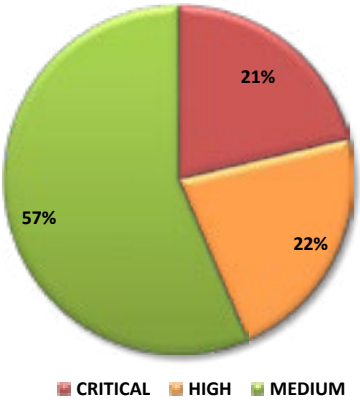


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

Gli attacchi con impatto "Medio" rappresentavano quasi la metà del totale (**48%**), quelli di livello "Alto" un terzo (**31%**) e quelli di livello "Critico" un quinto (**21%**).

Nel 1H 2018 il quadro cambia leggermente, mostrando una tendenza alla "polarizzazione" della Severity degli attacchi tra il livello Medium e quello Critical, con una diminuzione degli attacchi classificati come High.

Tipologia e distribuzione severity 1H 2018

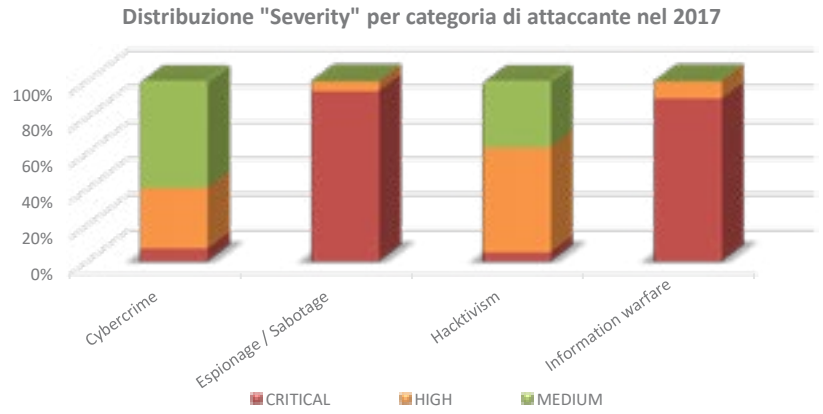


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

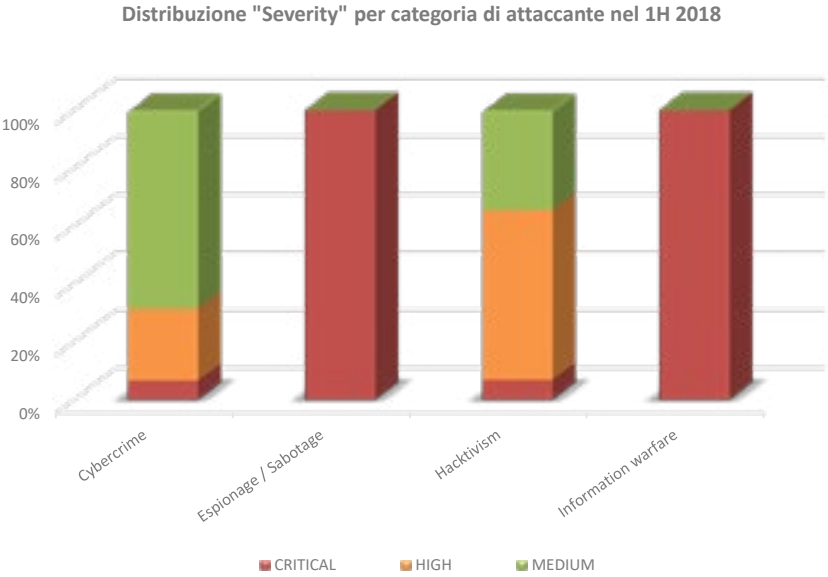
Come si può notare, nel nostro campione gli attacchi di tipo "Critical" rimangono stabili al **21%**, mentre quelli di livello "High" scendono dal 31% al **22%**, e di conseguenza quelli di livello "Medium" salgono dal 48% del 2017 al **57%** del 1H 2018.

Una spiegazione plausibile di questa variazione è che gli attacchi realizzati da soggetti cybercriminali con malware semplice, pur crescendo fortemente dal punto di vista numerico, generino una quantità di danni relativamente più modesta per singolo attacco (trattandosi di operazioni "mordi e fuggi" nelle quali gli attaccanti cercano di massimizzare i profitti nel minor tempo possibile e senza suscitare troppo clamore, che potrebbe danneggiarne gli "affari").
Questo purtroppo non significa che in termini assoluti i danni siano in diminuzione, quanto piuttosto che, allargandosi la "base" di attaccanti verso il basso grazie alla disponibilità di malware a basso costo, gli attacchi compiuti da questi soggetti risultino percentualmente meno gravi per le singole vittime rispetto all'anno scorso.

Raggruppando i dati per le consuete categorie (Attaccanti, Vittime e Tecniche di attacco) emergono ulteriori elementi di interesse.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

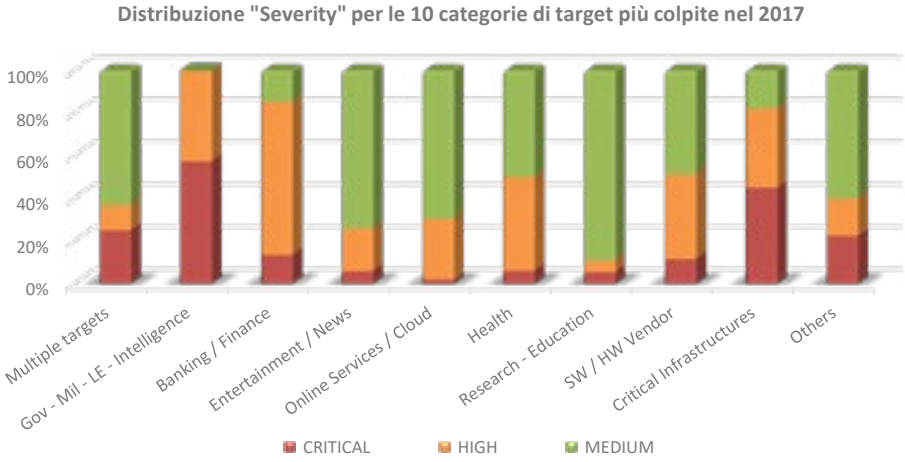


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

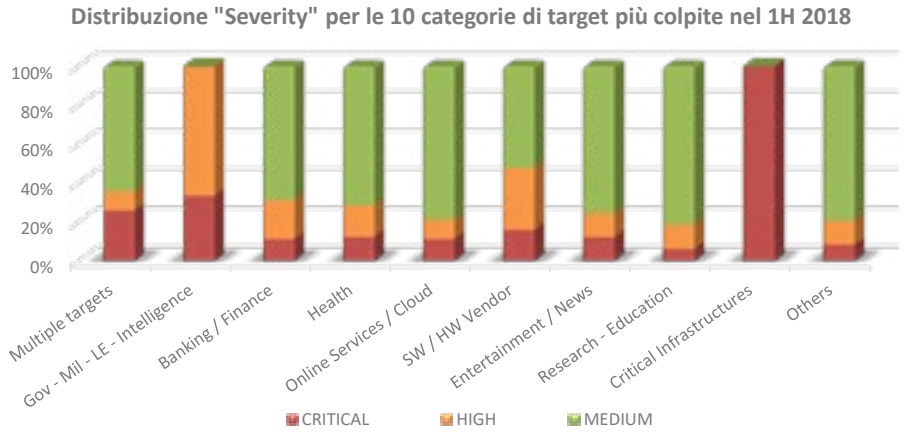
Come si evince da confronto tra i due grafici, si assiste ad un peggioramento complessivo della Severity degli attacchi compiuti con finalità di Information Warfare ed Espionage, mentre gli attacchi realizzati dal Cybercrime, pur crescendo numericamente e come quantità di danni complessiva, hanno nel 1H 2018 una Severity relativa inferiore al 2017.

Interessante anche notare come l'Hacktivism, pur in diminuzione, presenti nel 1H 2018 una percentuale di attacchi con impatto di tipo "Critical" più alta che nel 2017.

Questo il confronto tra le Severity degli attacchi stimate per il 2017 e per il 1H 2018 verso le 10 categorie di vittime più colpite.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

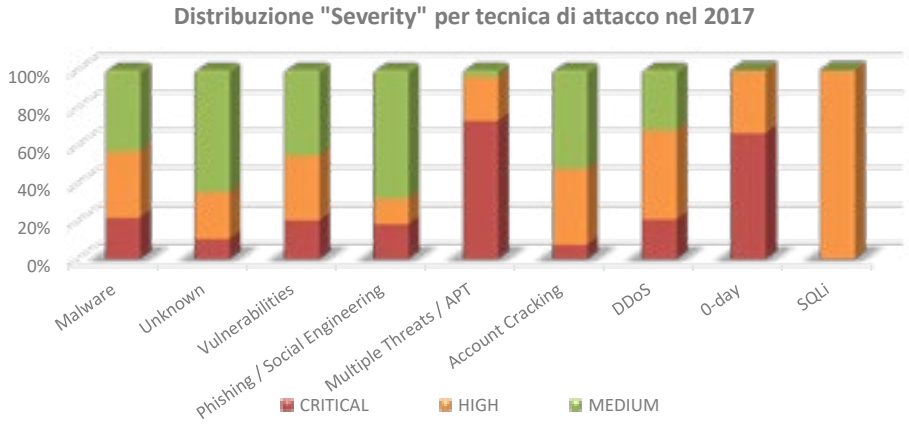


© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

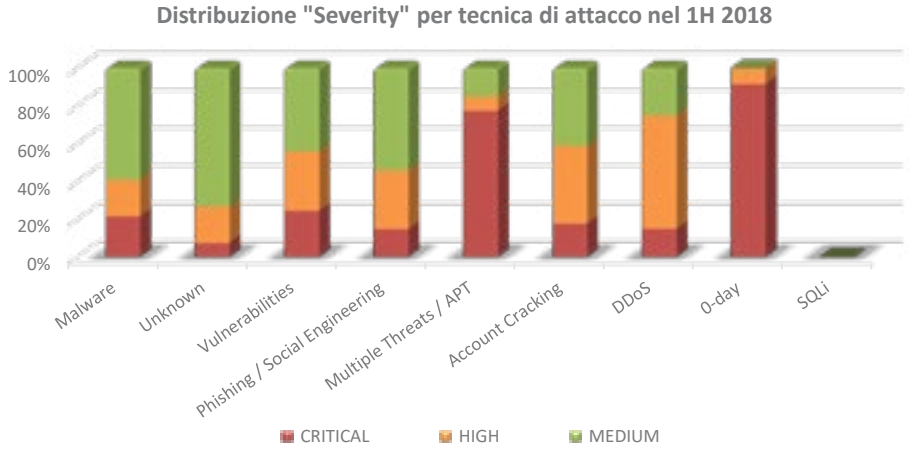
Si può notare come anche nel 1H 2018 le categorie "Gov" e "Critical Infrastructures" abbiano subito il maggior numero di attacchi con Severity "Critical" (con una crescita particolarmente notevole di attacchi molto gravi verso infrastrutture critiche), e salta all'occhio l'au-

mento di attacchi di tipo "Critical" al settore "Health", mentre con riferimento ad attacchi verso la categoria "Multiple targets" (numericamente la più rappresentata nel campione) dal punto di vista della Severity la situazione è rimasta sostanzialmente stabile.

Per quanto riguarda il confronto tra Severity 2017 e 1H 2018 dal punto di vista delle tecniche di attacco utilizzate, gli attacchi con impatto più critico sono quelli realizzati tramite APT e 0-day (quindi più sofisticati e stealth, spesso con motivazioni geopolitiche e finalità di Espionage e Information Warfare). La Severity degli attacchi condotti con queste tecniche cresce in modo significativo nel 1H 2018 rispetto al 2017.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia - aggiornamento giugno 2018

Molto simili in percentuale gli attacchi con impatto "Critico" realizzati tramite Malware, Vulnerabilità note, Phishing e DDoS, mentre prevalgono gli impatti di tipo "Alto" nel caso di attacchi condotti tramite tecniche di Account Cracking, DDoS e SQL injection. Anche da questo grafico si può notare quanto illustrato in precedenza in merito alla Severity degli attacchi realizzati tramite Malware semplice, che sembra diminuire percentualmente nel 1H 2018 rispetto al 2017.
Nel corso dei prossimi mesi, a partire dall'edizione 2019 del Rapporto Clusit nella quale analizzeremo i dati dell'intero 2018, disponendo di maggior dati potremo svolgere ulteriori considerazioni in merito ai trend ed alle variazioni osservabili sotto questo nuovo profilo di indagine.

Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici

Introduzione e visione d'insieme

Il 2017 è stato un anno particolarmente complicato per tutto ciò che concerne l'ambito della cyber-security. Si conferma un trend di crescita degli attacchi importante dell'11% rispetto all'anno precedente, soprattutto per quanto concerne la diffusione di malware. Tra i principali attacchi, si confermano anche nel 2017 quelli di tipo "ransomware" che infettano il pc, criptando i dati dei sistemi e dei dischi di rete connessi, costringendo l'utente al pagamento di un riscatto per avere la possibilità di accedere nuovamente ai dati.
Le aziende più esposte sono sicuramente quelle che non adottano un approccio strutturato al problema e che, infettate e senza un backup aggiornato, si trovano a dover pagare il riscatto per non interrompere la propria attività lavorativa.

L'altro trend significativo di malware in crescita è costituito da i così detti "miners", dei veri e propri software in grado di generare crypto valuta (ad esempio bitcoin) sfruttando la capacità di elaborazione di tutte le macchine "infettate". Tale infezione può avvenire o tramite software malevolo presente direttamente sulla macchina, oppure semplicemente visitando siti web compromessi.
In questo caso non c'è un vero e proprio furto di dati ma viene sfruttata tutta la capacità di calcolo della macchina attaccata con un conseguente alto dispendio di energia elettrica.
Ci sono però anche segnali positivi relativamente alla diffusione di nuove tecnologie, più accessibili dal punto di vista economico e che rispondono alle sempre crescenti minacce riuscendo in qualche caso a prevenire i così detti attacchi "zero-days" sfruttando tecniche evolute di machine learning e artificial intelligence.

Nei prossimi capitoli entreremo nel dettaglio dei vari attacchi fornendo un quadro di sintesi di quanto rilevato nel corso del 2017 in relazione alle principali minacce informatiche.

Dati analizzati

Quest'anno abbiamo raccolto oltre 35 milioni di eventi di sicurezza (una base dati pari a circa il doppio di quella utilizzata per il report 2016). Il dominio di analisi è costituito dai dati ottenuti dal Security Operations Center e relativi agli indirizzi IP appartenenti all'Autonomous System (AS) Fastweb: oltre 6 milioni di indirizzi pubblici su ognuno dei quali possono comunicare decine o anche centinaia di dispositivi e server attivi presso le reti dei Clienti.

I dati raccolti sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni esterne come ad esempio la Shadowserver Foundation, fonte autorevole e molto dettagliata in merito all'evoluzione delle botnet e dei relativi malware.
I dati sugli attacchi di Distributed Denial of Service, sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto di questo tipo di attacchi.

Allo stesso modo le informazioni relative alle principali tipologie di minacce riscontrate sono state raccolte da piattaforme interne utilizzate per attività di Incident Management.
Le indicazioni relative alle frodi sul protocollo VOIP sono invece frutto delle analisi effettuate dal Dipartimento di Fraud Management della Direzione Security di Fastweb.
È importante sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza sia dei Clienti sia di Fastweb stessa.

Tipologia di Malware e di Botnet

La composizione dei Malware e Botnet che interessano le macchine appartenenti all'AS di Fastweb si è evoluto rispetto alla precedente rilevazione dell'anno 2016. Infatti troviamo diverse minacce già presenti lo scorso anno, ma la vera novità riguarda la diffusione massiva di nuovi malware, ancora sconosciuti e non identificati.

Il principale rilevato si chiama Gozi e copre il 17% dei malware totali individuati. Gozi, rientra nella categoria degli Spyware ed è in grado di monitorare i computer compromessi per intercettare le credenziali di accesso alle banche online. Nei primi posti, troviamo anche quest'anno Nivdort seguito da ZeroAccess.
Nivdort, scoperto nel 2007 è in grado di compiere furto di password e modifica di configurazioni di sistema, oltre a favorire il download di malware addizionali. ZeroAccess, scoperto nel 2011 rende il PC infetto parte di una Botnet (rete di pc zombie che svolgono operazioni più disparate sotto diretto controllo degli attaccanti) principalmente impiegato per il mining dei bitcoin e la generazione di crypto valute.

Ci sono due novità importanti rispetto alla nostra rilevazione del 2016, in particolare l'ingresso di Mirai. Questo è un malware che trasforma i sistemi informatici in botnet controllabili da remoto. I suoi obiettivi principali sono i dispositivi elettronici di consumo, come telecamere casalinghe e router. La botnet creata da Mirai è stata utilizzata in alcuni dei maggiori attacchi DDoS del 2017.
Infine rileviamo un 15% di software malevoli che non sono ancora stati catalogati di cui non si conoscono tutti i dettagli.

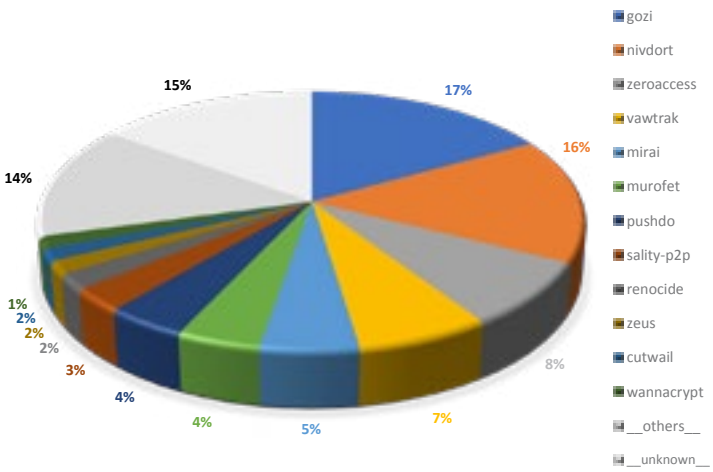


Figura 1 - *Analisi dei Malware rilevati (Dati Fastweb relativi all'anno 2017)*

Andamento temporale

Il grafico di seguito mostra la diffusione temporale degli host infetti e parte di botnet per l'anno 2017. Come si può notare il trend è stato altalenante durante tutto l'anno caratterizzato da una crescita negli ultimi mesi dell'anno.

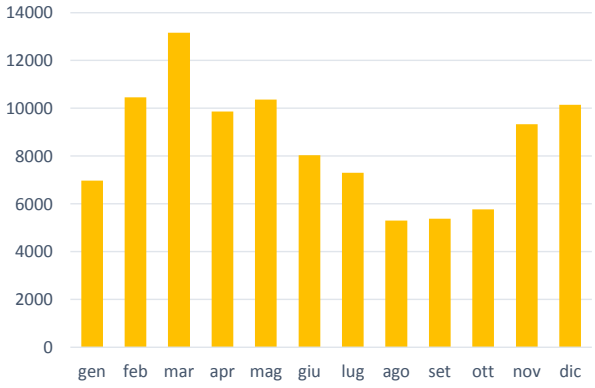


Figura 2 - *Distribuzione temporale del numero di Malware rilevati (Dati Fastweb relativi all'anno 2017)*

Principali famiglie di malware e botnet

Analizzando i trend temporali delle varie tipologie di malware si nota una decisa flessione di gozi e nivdort mentre per gli altri il trend è pressoché costante.
È importante però evidenziare come, a partire da settembre, siano cresciuti in maniera significativa gli eventi (quasi 5000 nei mesi di novembre e dicembre) relativi a minacce non ancora conosciute e catalogate. Tale tipologia di attacchi è più pericolosa della media perché queste ultime non sono rilevabili da sistemi tradizionali poiché non ancora riconosciute dai principali sistemi di protezione (ad esempio gli antivirus). Per questo motivo sul mercato stanno nascendo diverse soluzioni che utilizzando tecniche di analisi comportamentale e machine-learning in grado di rilevare queste tipologie di infezioni. Purtroppo la diffusione di tali tecnologie di nuova generazione è ancora marginale e abbastanza costosa rispetto alle soluzioni tradizionali.

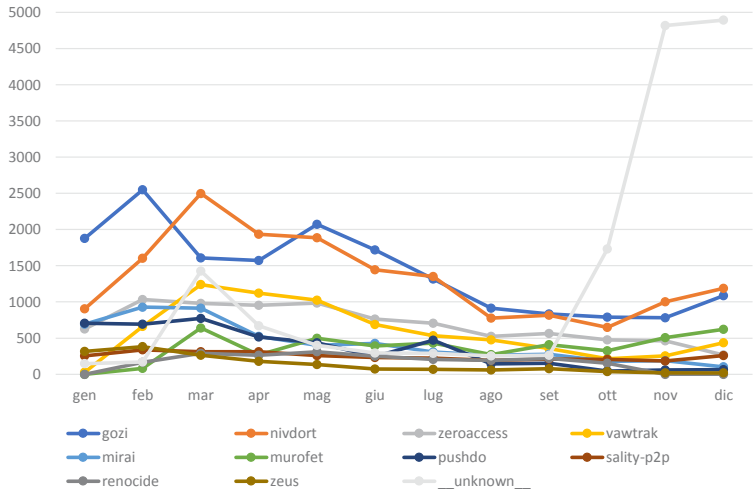


Figura 3 - *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2017)*

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di Command and Control (C&C) rappresentano le macchine utilizzate per l'invio dei comandi alle macchine infette da malware (bot) utilizzato per la costruzione della botnet.
È confermato che anche quest'anno ben oltre la metà dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb si trovano negli Stati Uniti (59%). Tale dato è però in calo e si nota come i centri C&C stiano crescendo in maniera importante anche in Europa (+22% rispetto all'anno 2016).

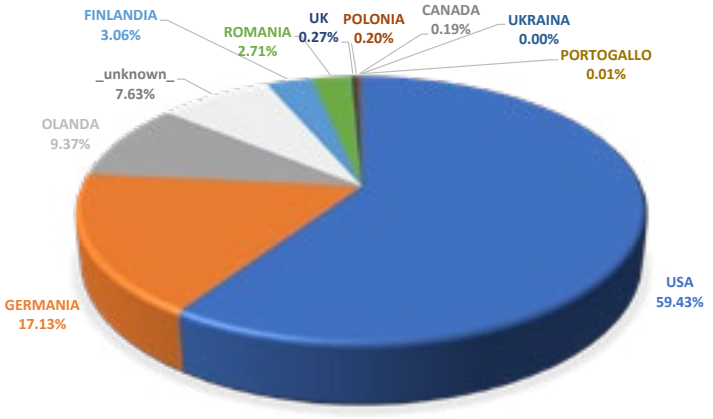


Figura 4 - *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2017)*

Attacchi DDOS (Distributed Denial of Service)

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio.

Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete. Gli attacchi DDoS (Distributed Denial of Service) amplificano la portata di tali minacce. Un attacco DDoS viene infatti realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.

Naturalmente gli effetti di un attacco DDoS possono essere devastanti sia a causa della potenza che possono esprimere, ma anche per le difficoltà insite nel poterli mitigare in tempi rapidi (se non attraverso la sottoscrizione di un specifico servizio di mitigation).

Quanti sono stati gli attacchi DDOS nel 2017?

Nel 2017 sono state rilevate oltre 7.000 anomalie riconducibili a possibili attacchi DDoS diretti verso i Clienti Fastweb. Durante l'anno il numero delle anomalie mensili è quasi raddoppiato e nell'ultimo trimestre ha raggiunto volumi importanti.

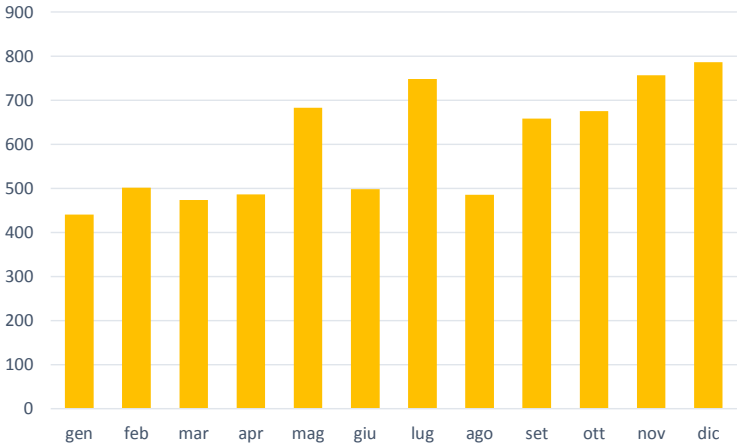


Figura 5 - *Distribuzione mensile delle anomalie DDoS (Dati Fastweb relativi all'anno 2017)*

Quali sono i settori più colpiti

Abbiamo voluto fornire maggiori dettagli in merito alla distribuzione dei target degli attacchi DDoS andando ad esplicitare i settori merceologici maggiormente colpiti da questo tipo di attacchi.

Come si evince dal grafico successivo, il fenomeno riguarda senza esclusione un esteso numero di settori tra i quali i più esposti risultano essere le aziende in ambito servizi e in particolare Finance, Insurance e Media oltre alle maggiori istituzioni governative (soprattutto Ministeri e Pubbliche Amministrazioni centrali).

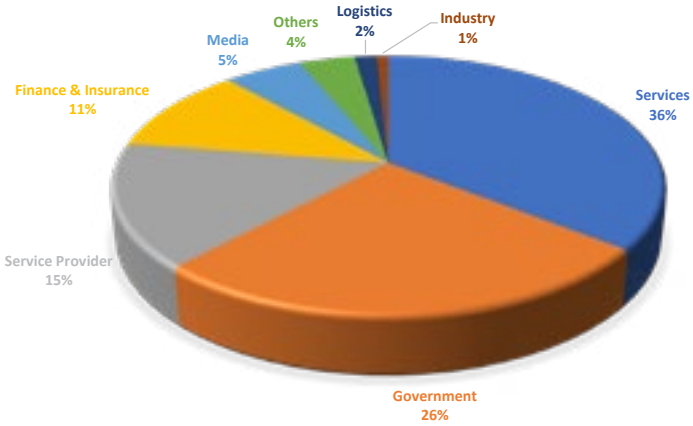


Figura 6 - *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2017)*

Il volume degli attacchi DDoS

Il grafico seguente rappresenta il volume degli attacchi DDOS durante l'anno. La piattaforma di mitigation utilizzata per la protezione dei Clienti, gestisce ogni mese attacchi che occupano una banda variabile tra i 20 Gbps e i 200 Gbps.
Come si può notare il trend è in crescita, soprattutto se si considera la seconda metà dell'anno, con picchi di attacchi a oltre 180 Gbps nel mese di settembre 2017.
Rispetto al 2016, che aveva registrato valori medi di attacchi pari a 11 Gbps, quest'anno ci si attesta a 59 Gbps. Un incremento importante pari a circa 6 volte rispetto al dato medio registrato lo scorso anno.

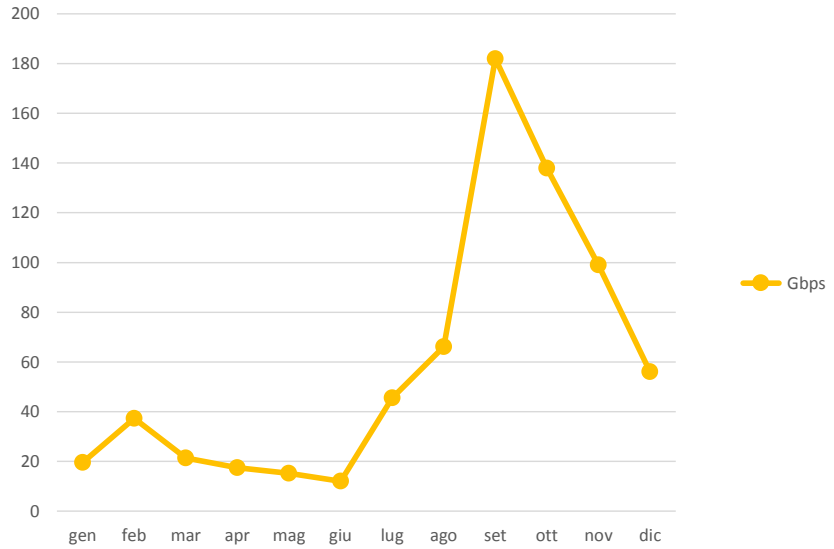


Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS (Dati Fastweb relativi all'anno 2017)*

Qual è la durata di un attacco DDOS?

Le tecniche di attacco DDoS e i relativi metodi di mitigazione si evolvono nel tempo. Nel corso degli anni, con il consolidamento delle tecniche di difesa, la durata degli attacchi è mediamente diminuita.
Si è osservato che quest'anno oltre l'95% degli attacchi è durato meno di 3 ore, mentre i rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. È importante però evidenziare che il 3% di questi durino oltre le 24 ore consecutive.

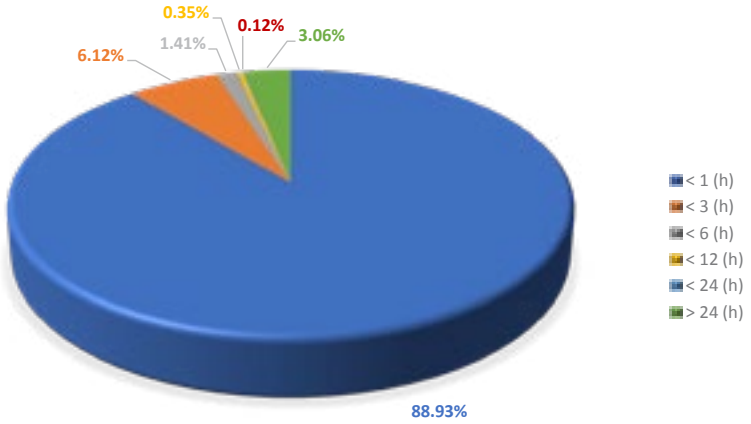


Figura 8 - *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2017)*

Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate possono essere diverse, nell'anno 2017 abbiamo rilevato tre tipologie ricorrenti con una prevalenza di attacchi di tipo "SYN Flood" che registrano il 93% del totale.
Di seguito una breve descrizione delle diverse varianti di minacce DDOS:

- **SYN Flood**
  L'attaccante manda un grande numero di pacchetti di tipo SYN alla vittima con indirizzo sorgente alterato: il risultato è che la macchina vittima cercherà di rispondere con pacchetti di tipo SYN-ACK che non avranno mai risposta in quanto l'indirizzo di destinazione sarà inesistente. In un breve arco di tempo tutte le risorse della macchina vittima saranno esaurite.
- **UDP Flood**
  Un attacco basato sull'UDP flood si avvia mandando un grande numero di pacchetti UDP verso un host remoto anche in questo caso falsificando l'indirizzo IP sorgente. Come risultato, l'host remoto:
  1 Controllerà se esiste un'applicazione in ascolto su quella porta.
  2 Si renderà conto che non esiste alcuna applicazione in ascolto.
  3 Invierà dunque un pacchetto di risposta "ICMP Unreachable".
  In questo modo, per un gran numero di pacchetti UDP, il sistema vittima sarà costretto ad inviare altrettanti pacchetti ICMP, portandolo ad essere irraggiungibile da altri client.
- **DNS Amplification**
  Il DNS Amplification Attack o DNS Reflector attack è un attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive)

inviando a questi ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza (IP spoofing).

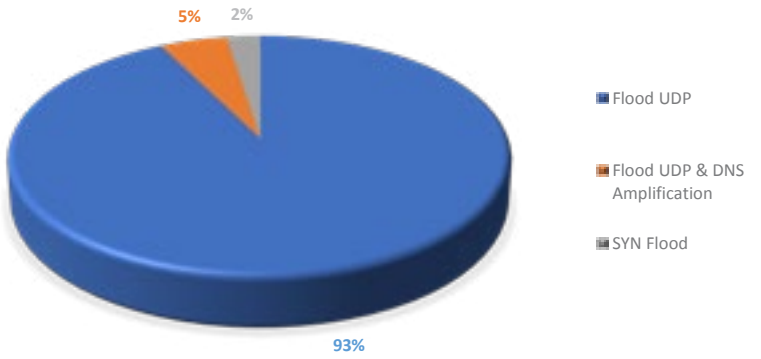


Figura 9 - *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2017)*

Attacchi ai Protocolli Voip

Le principali minacce

I servizi VOIP (Voice Over Internet Protocol) rappresentano una modalità di trasmissione di voce e traffico multimediale su reti IP dove le comunicazioni vocali vengono convertite, pacchettizzate e trasmesse sotto forma di traffico dati.
In questo modo è possibile abilitare chiamate tra PC e telefoni IP, ma anche verso la rete telefonica classica (tramite una conversione del formato effettuata tipicamente dalla rete dell'operatore).
Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere dato che può sfruttare le sinergie con la rete dati. D'altra parte questo meccanismo è caratterizzato da possibili vulnerabilità (tipiche di una classica rete IP) e può ampliare la superficie d'attacco alla quale le Aziende sono esposte.
Le particolarità e vulnerabilità dello specifico protocollo possono infatti rappresentare un'ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di Social Engineering e intercettazione fino a possibili interruzioni di servizio (DoS e DDoS) e Service Abuse (dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale).

I dati Fastweb

Nell'ambito dello studio delle attività illecite condotte sfruttando tali protocolli, anche nel 2017 il Dipartimento di Fraud Management della Direzione Security di Fastweb ha continuato ad analizzare i trend degli attacchi legati alle piattaforme VOIP dei nostri Clienti confrontandoli con quanto accaduto negli anni precedenti e con l'equivalente impatto legato alla più tradizionale tecnologia TDM.

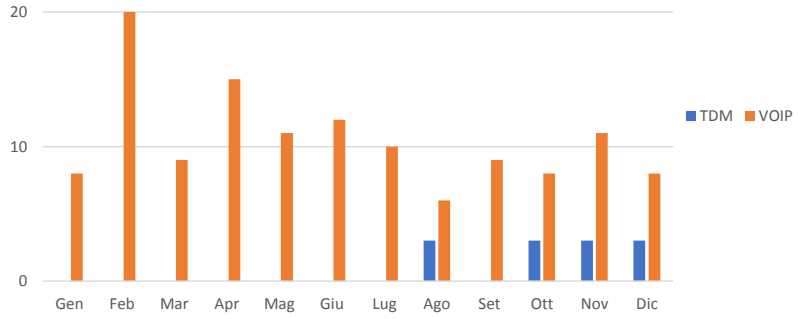


Figura 10 - *Andamento delle frodi durante l'anno (Dati Fastweb relativi all'anno 2017)*

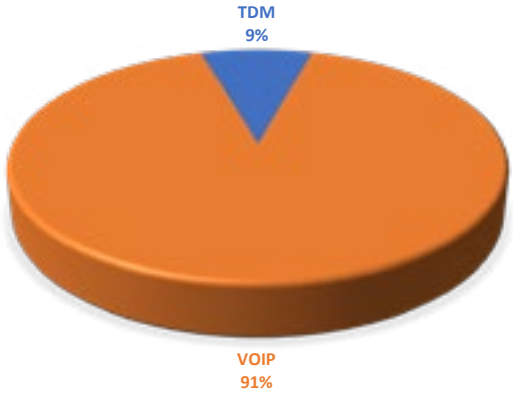


Figura 11- *Truffe VOIP vs TDM (Dati Fastweb relativi all'anno 2017)*

I dati osservati mostrano che circa la metà degli attacchi all'infrastruttura VOIP è diretta verso Clienti di tipo SMALL, piccole imprese che si rivolgono al VOIP per usufruire dei vantaggi legati ai costi più contenuti, ma che spesso non possiedono particolari competenze di tipo tecnico e dove il rischio di utilizzare dispositivi non correttamente configurati né monitorati è più elevato rispetto ad altri segmenti di clientela.

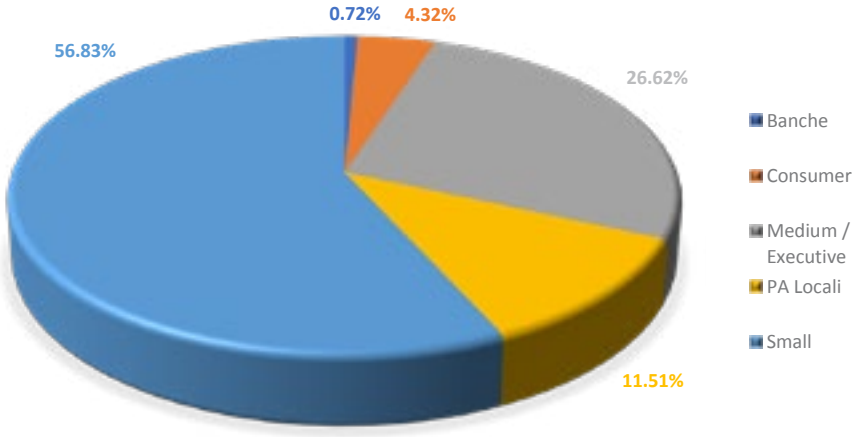


Figura 12 - *Vittime di truffe VOIP (Dati Fastweb relativi all'anno 2017)*

La maggior parte delle frodi riscontrate riguarda casi di 'Service Abuse', ovvero attacchi volti a generare traffico illecito verso direttrici a tariffazione speciale. Nel grafico sotto, si evidenziano i principali paesi ospitanti le direttrici che hanno generato frodi.

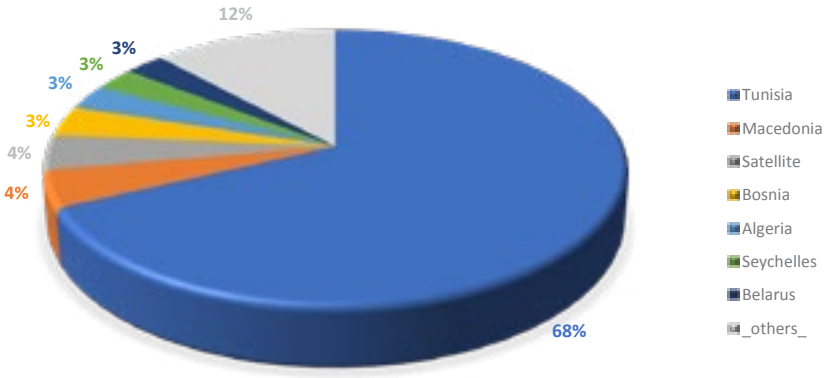


Figura 13 - *Paesi ospitanti le direttrici dei principali attacchi (Dati Fastweb, anno 2017)*

Ulteriori vulnerabilità

Servizi critici esposti su Internet

In questo paragrafo viene messo in evidenza il numero di dispositivi che espongono servizi direttamente su Internet privi anche di livelli minimi di protezione. Ciò significa che questi host sono facilmente attaccabili e esposti a rischi elevati di compromissione.
I dati del 2017 riportano oltre 70.000 macchine che espongono servizi critici direttamente su Internet, il grafico in calce rappresenta le tipologie di servizi esposti.
Al primo posto troviamo Telnet, protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando, al secondo posto troviamo RDP, utilizzato per la connessione remota ad un PC. Un attaccante potrebbe sfruttare questo protocollo per prendere il controllo completo della macchina.
Di rilievo è anche la quantità di macchine che espongono SMB, utile per la condivisione di file e stampanti nelle reti locali ma che se esposto su internet può essere utilizzato per accedere ai documenti e file condivisi.

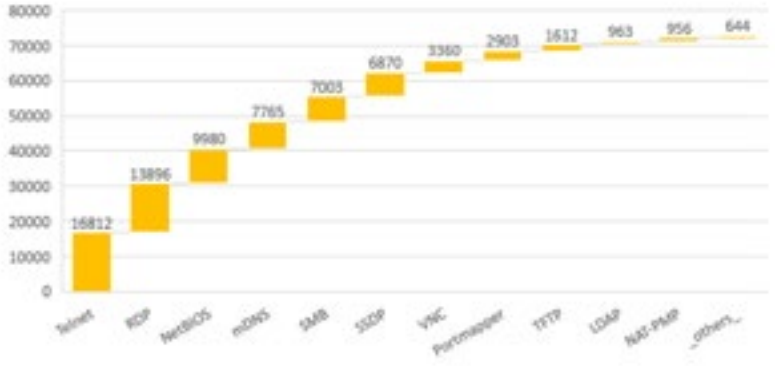


Figura 14 -*Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2017)*

Blacklist

Una blacklist è una lista dove vengono inseriti e catalogati indirizzi IP classificati come fonte di e-mail di SPAM.

Ci sono diversi motivi per cui si può essere inseriti nelle liste nere, di seguito cercheremo di analizzare i principali:

- Invio di e-mail massive dal proprio indirizzo
- Nel testo o nell'oggetto delle e-mail inviate sono presenti caratteri e simboli in genere utilizzati nelle mail di SPAM
- Il pc è infetto da virus che invia autonomamente e ciclicamente email infette.

Dalle nostre rilevazioni abbiamo notato che oltre 40.000 IP sono stati inseriti almeno una volta nelle blacklist durante il 2017. Il grafico di seguito rappresenta le città maggiormente colpite.

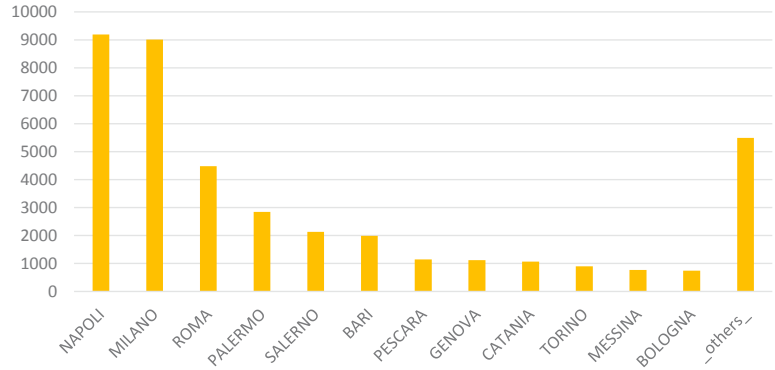


Figura 15 - *Host in Blacklist per città (Dati Fastweb relativi all'anno 2017)*

Considerazioni finali

Alla luce delle analisi effettuate, lo scorso 2017 è stato sicuramente un anno particolare: si è evidenziato un trend in crescita in termini di infezioni da malware dovuto principalmente a tecniche sempre più evolute per l'infezione: i malware moderni infatti sono in grado di superare in maniera semplice i sistemi di difesa tradizionali. Inoltre le frodi sono maggiormente personalizzate e puntano a colpire un target mirato di vittime (ad esempio un particolare settore merceologico).
Se consideriamo invece gli attacchi Distributed Denial of Service, si nota un netto incremento del numero di attacchi ma soprattutto della loro portata in Gbps. Questo fenomeno è caratterizzato dal fatto che è sempre più semplice ed economico accedere agli strumenti sul deep/dark web per poter letteralmente "noleggiare" una botnet e portare a termine un attacco con poco dispendio di energie.
Ciò che risulta chiaro è che le tecniche di attacco si evolvono in maniera veloce come velocemente si stanno evolvendo i sistemi di difesa e di protezione. È importante quindi mantenersi al passo con la sicurezza, soprattutto nei contesti aziendali per minimizzare i rischi di infezione.
La pubblicazione in gazzetta ufficiale a maggio 2016 del GDPR (Regolamento Generale sulla Protezione dei Dati Personali) definito a livello europeo, ha contribuito in maniera importante allo sviluppo e relativa messa in sicurezza delle infrastrutture aziendali e siamo sicuri che nei primi mesi del 2018 ci sarà un'ulteriore accelerata dovuta all'entrata in vigore dell'impianto sanzionatorio a partire dal 25 maggio 2018.

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2017

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2017 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati che, anche a fronte della Direttiva del Ministro dell'Interno del 15 Agosto 2017, sono di precipua competenza di questa Specialità.

Nell'ambito della **pedopornografia online** sono stati operati **55** arresti e **600** denunce; tra le operazioni più significative, coordinate dal Servizio Polizia Postale e delle Comunicazioni, si segnala l'operazione Sweep Web del Compartimento Polizia Postale e delle Comunicazioni di Firenze che ha condotto all'esecuzione di **45** perquisizioni e **4** arresti per pornografia minorile l'operazione Black Shadow, condotta dal Compartimento Polizia Postale e delle Comunicazioni di Trento, nell'ambito della quale sono state eseguite **37** perquisizioni e **10** arresti per detenzione e divulgazione di materiale pedopornografico .
Dalle complesse operazioni di prevenzione, è scaturita una assidua attività di monitoraggio della rete che ha visto coinvolti ben **28784** siti internet, di cui **2077** inseriti in black list.
Si conferma la rilevanza del fenomeno dell'adescamento di minori online che ha registrato **437** casi trattati che hanno portato alla denuncia di **158** soggetti e all'arresto di **19**.
A tal proposito, significativa è stata l'attività denominata Bad Queen condotta dal Compartimento Polizia Postale di Trieste che ha portato al deferimento all'A.G. di **7** soggetti.
Senza dimenticare le indagini avviate a seguito delle segnalazioni dei genitori come l'operazione "12 Apostoli" del Compartimento Polizia Postale di Catania, che ha arrestato **4** persone costituenti una associazione a delinquere finalizzata alla violenza sessuale aggravata ai danni di minori.
Di rilievo è l'attività di collaborazione con organismi internazionali: sono stati elaborati circa **176** ReportNCMEC dai quali sono scaturite importanti attività di indagine.

Un sensibile aumento, rispetto al 2016, è ravvisabile in materia di reati informatici contro la persona (ad es. diffamazione, cyberstalking, trattamento illecito di dati personali, sostituzione di persona) per i quali sono state denunciate **917** persone e arrestate **8**.
Di evidente incremento è l'attività di contrasto alla minaccia cyber svolta dal Centro Nazionale Anticrimine per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), attestata dal rilevante aumento del numero di alert diramati alle infrastrutture critiche nazionali che, rispetto al 2016, si è quasi quintuplicato sino a raggiungere **31524**.
La tempestiva condivisione dei c.d. "indicatori di compromissione" dei sistemi informatici con i fornitori di servizi pubblici essenziali ha consentito di rafforzare gli strumenti volti alla protezione della sicurezza informatica, garantita anche da una costate attività di monitoraggio.

In tale ambito, il Centro ha ulteriormente gestito monitoraggi della rete che hanno riguardato strutture sensibili di rilievo nazionale.
Inoltre in particolare la Sala Operativa del Centro ha gestito:

- **1032** attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- **83** richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

Tra le attività investigative condotte, in tale ambito, si segnalano **72** indagini avviate nel **2017** per un totale di **34** persone denunciate e l'arresto di **2.**

Tra le attività più significative, si segnalano l'operazione "*EyePyramid"* a seguito della quale è stato fermato il sodalizio composto dai fratelli Occhionero, entrambi arrestati, che si dedicava allo spionaggio informatico politico-istituzionale ed industriale e l'operazione "*Andromeda*" a seguito della quale è stata smantellata una rete botnet, ovvero un insieme di computer infettati da virus informatici e utilizzati dagli hacker per compiere svariati reati in tutto il mondo.

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2017 sono state sottoscritte 7 nuove convenzioni con il Gruppo Atlantia (con le società Aeroporti di Roma, Autostrade per l'Italia e Telepass), Lottomatica, Piaggio Aerospace, INAIL e A2A, oltre al rinnovo della convenzione in essere con Enel.
Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

Con riferimento al **financial cybercrime,** le sempre più evolute tecniche di *hackeraggio,* attraverso l'utilizzo di *malware* inoculati mediante tecniche di phishing, ampliano a dismisura i soggetti attaccati, soprattutto nell'ambito dei rapporti commerciali. Infatti lo scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando le somme verso conti correnti nella disponibilità dei malviventi. Il BEC (business e-mail compromise) fraud o CEO (Chief Executive Officer) fraud sono la moderna applicazione della tecnica di attacco denominata "man in the middle". Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, soprattutto perché inviate verso paesi extraeuropei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma **OF2CEN** (On line Fraud Cyber Centre and Expert Network) per l'analisi e il contrasto avanzato delle frodi del settore, nell'anno 2017, la Specialità ha potuto bloccare alla fonte su una movimentazione di **22.052.527€** ben **20.839.576€** e di recuperare **862.000€** della residuale parte relativa ai bonifici già disposti. La piattaforma in questione frutto di specifiche convenzioni intercorse mediante ABI con gran parte del mondo bancario, consente di intervenire in tempo quasi reale sulla segnalazione bloccando la somma prima che venga polverizzata in vari rivoli di prestanome.

Al riguardo, di rilievo è la recente operazione internazionale denominata "Emma3", coordinata dal Servizio Polizia Postale con la collaborazione di **21 Paesi** Europei e di Europol, volta a identificare i c.d. "money mules", primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito sui quali vengono poi accreditate le somme illecitamente acquisite. L'operazione in parola ha consentito di identificare **37** ***money mules*** di cui **32** arrestati e **5 denunciati**, nonché di bloccare oltre **150.000€**. Il contrasto al fenomeno dei "money mules" nel corso dell'anno ha consentito di recuperare complessivamente circa **370.000€**e di **denunciare 122** individui e di **arrestarne 39.**
Altra significativa attività di polizia giudiziaria l'operazione "Criptolocker" condotta dal Compartimento Polizia Postale e delle Comunicazioni di Catania che ha portato a individuare una associazione a delinquere di **7 persone, 4 delle quali arrestate,** con base operativa nel napoletano, che estorcevano denaro a imprenditori e professionisti in tutta Italia bloccando tutti i dati presenti all'interno dei pc delle vittime, criptandoli, ovvero colpendo le transazioni commerciali con attacchi cosiddetti *man in the middle*.

Nel settore del **cyberterrorismo** gli investigatori della Polizia Postale e delle Comunicazioni hanno concorso con altri organi di Polizia e di intelligence alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica.
In tal senso spicca l'operazione antiterrorismo denominata "Da'Wa" condotta dai Compartimenti di Perugia e Milano che ha portato all'arresto di 4 persone, tre tunisini ed un marocchino, che facevano proselitismo sul web, e ha consentito di emettere tre provvedimenti di espulsione nei confronti di altrettanti individui.
Nell'ultimo anno, la strategia mediatica messa in campo dalle organizzazioni terroristiche di matrice religiosa islamista ha indotto la Specialità a effettuare una costante attività di osservazione e analisi dei contenuti presenti in rete, coinvolgendo anche ulteriori strutture territoriali rispetto a quelle individuate nel 2016 al fine di individuare forme di proselitismo e segnali precoci di radicalizzazione.
L'attività, funzionale a contrastare il proselitismo e prevenire fenomeni di radicalizzazione, ha portato a monitorare circa **17000** spazi web e alla rimozione di diversi contenuti.
Con riferimento all'attività di monitoraggio del web per il contrasto al terrorismo di matrice islamica, giova evidenziare che gran parte dei contenuti illeciti pubblicati su internet vengono rimossi direttamente dai gestori delle principali piattaforme web i quali, grazie anche alla richiesta di maggiore collaborazione elaborata in numerose sedi istituzionali nell'ambito di progetti internazionali (es. EU Internet Forum) ai quali ha preso parte anche questa Specialità, stanno garantendo un'azione più incisiva per ridurre la proiezione esterna e virtuale del Califfato.
Ancora, si rappresenta, che il Servizio di Polizia Postale e delle Comunicazioni costituisce ***punto di contatto nazionale*** per l'IRU (Internet Referral Unit), Unità di Riferimento Internet in ambito Europol sviluppata sulla base del progetto *Check the Web*, con l'intento

di condividere con altri Paesi informazioni di intelligence e per rispondere alla necessità di agire tempestivamente quando si presentino contenuti pericolosi che riguardano la nostra od altre Nazioni, condividendo notizie di interesse generale.
L'IRU, infatti, effettua una approfondita analisi dei contenuti emersi in rete che possano essere di interesse per la sicurezza nazionale, condividendoli con i Paesi UE e con gli altri Paesi interessati.

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino.
La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni.

Nello specifico si evidenzia che lo scorso 1° Dicembre 2017, in occasione del "Maker Faire-Fiera dell'Innovazione" è partita la 5° Edizione di "***Una Vita da Social***", campagna itinerante della Polizia Postale e delle Comunicazioni, grazie alla quale sino ad oggi sono stati incontrati oltre **1 milione e 300 mila studenti**, **147.000 genitori, 82.500 insegnanti** per un totale di **10.750 Istituti scolastici** e **190** città italiane.
Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network.
A disposizione degli utenti è presente la pagina **facebook e twitter** di "Una vita da social", gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati gli appuntamenti, le attività, i contributi e dove i giovani internauti possono "*postare*" direttamente le loro impressioni ad ogni appuntamento.

Grande consenso ha riscosso la campagna **#cuoriconnessi**, iniziativa che attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online, vuole offrire uno spunto di riflessione per avviare importanti considerazioni sul peso delle parole, sul loro valore e sulla loro potenza, ma anche sulle responsabilità degli adulti.

Inoltre nel corso dell'anno sono stati realizzati incontri educativi su tutto il territorio nazionale raggiungendo oltre **250 mila studenti** e circa **2500 Istituti scolastici** per i quali è stata messa a disposizione anche un'email dedicata: progettoscuola.poliziapostale@interno.it.

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce.

Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.

Attività del Commissariato di PS online

Richieste di informazioni evase	**16.737**
Segnalazioni ricevute dai cittadini	**18.053**
Denunce presentate dagli utenti	**8.784**

A integrare la piattaforma online, anche l'App del Commissariato, scaricabile gratuitamente sul proprio smartphone o su tablet, sia per iOS che Android, con i seguenti dati:

Statistiche App

Richieste di informazioni evase	**937**
Segnalazioni ricevute dai cittadini	**407**
Download Play Store	**11.101**
Download iOS	**6.556**

Il punto di vista del CERT-PA

Il CERT-PA opera all'interno dell'Agenzia per l'Italia Digitale (AgID), alla quale il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ha affidato il compito di curare la sicurezza cibernetica delle Pubbliche Amministrazioni Italiane. Pur se la sua *constituency* di riferimento è formata solamente da Pubblica Amministrazione Centrale, Regioni e Città metropolitane, il CERT-PA ha da sempre supportato, pur se in modalità *best-effort*, tutte le altre PA che necessitano di assistenza.
In accordo alle regole tecniche per la sicurezza informatica delle PA, il CERT-PA è in grado di fornire alle amministrazioni richiedenti:

- *servizi di analisi e di indirizzo*, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;
- *servizi proattivi*, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative, lo sviluppo della *readiness* e della *preparedness*;
- *servizi reattivi*, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- *servizi di formazione e comunicazione* per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.

Attualmente vengono erogati i servizi di:

- *early warning*;
- *threat intelligence* ed analisi delle fonti;
- gestione delle segnalazioni;
- produzione ed invio di bollettini ed avvisi.

Nel corso del 2017 il CERT-PA ha provveduto non solo a consolidare la propria attività all'interno del sistema di protezione dello spazio cibernetico nazionale, anche in vista della prossima fusione con il CERT Nazionale indicata nel Piano Nazionale tra gli adempimenti previsti per il recepimento della Direttiva NIS, ma anche a sviluppare la propria struttura operativa dotandosi di nuove risorse e strumenti di supporto alle attività. A fianco di ciò sono stati attivati specifici Gruppi di lavoro e progetti di sperimentazione finalizzati a mettere a punto strumenti e protocolli di *infosharing* con l'obiettivo di costituire una rete nazionale di scambio automatico di IoC (indicatori di compromissione) validati e *actionable*, ossia direttamente utilizzabili senza interventi umani intermedi.

L'analisi della minaccia 2017

Anche nel corso del 2017, seguendo un trend oramai consolidato negli ultimi anni, il livello generale delle attività ostili verso la Pubblica Amministrazione si è ulteriormente accresciuto rispetto al passato. Ciò è dovuto sia al generalizzato aumento della minaccia in sé, che colpisce in modo trasversale tutti i settori della società compresa la Pubblica Amministrazione, sia alla sempre crescente "appetibilità" specifica della PA in quanto tale da parte di organizzazioni o anche di singoli individui portatori di interessi illeciti.
Come già nell'anno precedente, gli attacchi più rilevanti sono finalizzati soprattutto all'esfiltrazione di informazioni, che vanno da semplici credenziali di posta (spesso però in termini massivi) ad informazioni più specifiche e sensibili.
Tutto ciò ha comportato per il CERT-PA un sensibile incremento dell'attività, specialmente per quelle di carattere reattivo (analisi ed investigazione). A livello puramente numerico, nel corso del 2017 i sistemi automatici del CERT-PA (tutti sviluppati internamente) hanno ricevuto ed analizzato 4.232.537 IoC e 1.697 malware, mentre il lavoro degli analisti ha portato alla produzione e diffusione di 2.191 IoC qualificati.

Riepilogo dell'attività svolta

Le attività erogate dal CERT-PA verso la propria *constituency* si suddividono nelle seguenti categorie:

- **segnalazioni**: ricezione e gestione di segnalazioni relative a problemi di sicurezza informatica nell'ambito della Pubblica Amministrazione;
- **indagini**: attività di analisi di eventi di sicurezza;
- **bollettini**: emissione periodica di pubblicazioni riguardanti nuove vulnerabilità e minacce informatiche di interesse per le Pubbliche Amministrazioni;
- **avvisi**: emissione a circolazione ristretta di pubblicazioni che non possono essere classificate come vulnerabilità ad impatto diffuso, ma riguardano specifiche fattispecie ed eventi di interesse per le Pubbliche Amministrazioni;
- **vulnerability assessment**: emissione e circolazione ristretta di pubblicazioni riguardanti vulnerabilità pubbliche e/o *misconfiguration* di specifici *asset* dei membri della *constituency* (tipicamente *web application* ed altri servizi esposti sulla rete pubblica);
- **esercitazioni**: attività di formazione ed aggiornamento svolte in collaborazione con altri enti del settore.

A queste attività si affiancano quelle, riservate, connesse alla partecipazione del CERT-PA al sistema nazionale di protezione dello spazio cibernetico del nostro Paese, in particolare per quanto riguarda la partecipazione al Nucleo di Sicurezza Cibernetica istituito presso la Presidenza del Consiglio.

Segnalazioni

Le segnalazioni pervengono da varie fonti: dalle Pubbliche Amministrazioni stesse, da altri CERT o strutture di monitoraggio quali il CNAIPIC, o ancora dallo stesso CERT-PA mediante la propria costante attività di monitoraggio delle fonti pubbliche.

Nel corso del 2017 il CERT-PA ha gestito un totale di 521 segnalazioni rilevanti, rispetto alle 468 del 2016, con i massimi picchi nei mesi di maggio (66) e novembre (67) (**figura 1**).

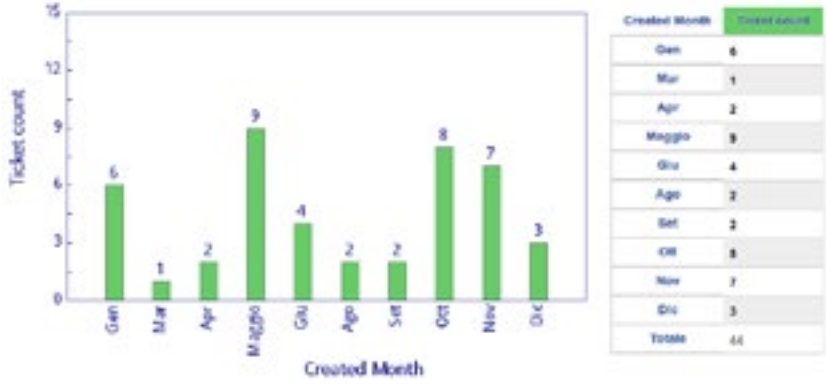
Created Month	Ticket count
Totale	521

Figura 1 - *Distribuzione mensile delle Segnalazioni*

Indagini

Le indagini sono attività di analisi e approfondimento anche piuttosto complesse su questioni che hanno maggior impatto per le Pubbliche Amministrazioni, che il CERT-PA svolge a seguito delle segnalazioni che riceve e delle attività di monitoraggio che conduce continuativamente.

Nel corso del 2016 il CERT-PA ha gestito un totale di 44 indagini, contro le 36 del 2016, con un picco massimo di 9 nel mese di maggio (**figura 2**).



Created Month	Ticket count
Totale	44

Figura 2 - *Distribuzione mensile delle Indagini*

Bollettini

I bollettini consistono nell'emissione di pubblicazioni dettagliate riguardanti nuove vulnerabilità e minacce informatiche di interesse per le Pubbliche Amministrazioni, che il CERT-PA produce a seguito delle proprie attività di analisi proattive o reattive. La circolazione dei bollettini non è limitata alla *constituency* ma è libera ed aperta a chiunque sia interessato, a seguito di semplice registrazione sul portale.
Nel corso del 2017 il CERT-PA ha emesso un totale di 20 bollettini pubblici, lo stesso numero rispetto al 2016, con un picco di ben 5 nel mese di gennaio (**figura 3**).

Figura 3 - *Distribuzione mensile dei Bollettini*

Avvisi

Gli avvisi consistono invece nell'emissione, a circolazione ristretta alla sola *constituency*, di pubblicazioni riguardanti minacce che non possono essere classificate come vulnerabilità ad impatto diffuso, ma riguardano fattispecie ed eventi di specifico interesse per le Pubbliche Amministrazioni.
Nel corso del 2017 il CERT-PA ha emesso 4 avvisi di questo tipo, nei soli primi tre mesi dell'anno (**figura 4**).

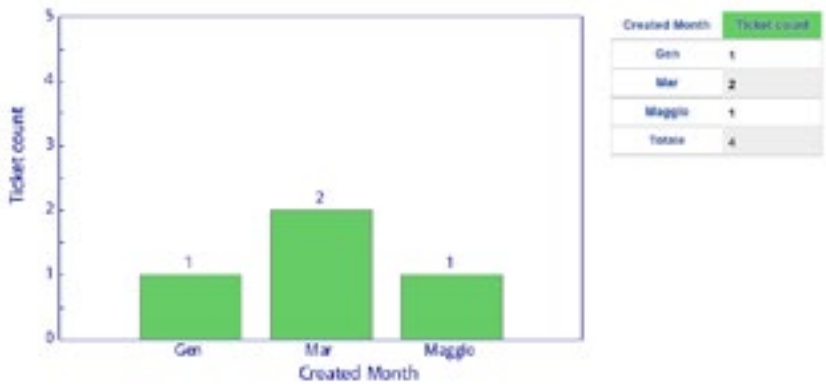


Figura 4 - *Distribuzione degli Avvisi*

Vulnerability assessment

Le attività di *vulnerability assessment* svolte dal CERT-PA consistono nella verifica di specifiche vulnerabilità pubbliche e/o errate configurazioni di specifici asset dei membri della *constituency* (tipicamente *web application* ed altri servizi esposti sulla rete pubblica) con conseguente emissione di un rapporto tecnico che identifica i problemi rilevati e le relative modalità di risoluzione.

Nel corso del 2017 il CERT-PA ha effettuato 5 vulnerability assessment a favore di altrettanti membri della propria *constituency*, contro i 3 effetuati nel 2016 (**figura 5**).

Figura 5 - *Distribuzione dei Vulnerability Assessment*

Attività di sviluppo e testing

Esiste inoltre un'ulteriore classe di attività svolte dal CERT-PA, che sono quelle di sviluppo e testing di tool ed applicazioni ad uso prevalentemente interno. Nell'ambito delle attività di ricerca e sviluppo, volte al miglioramento continuo nell'erogazione dei servizi alla propria *constituency*, il CERT-PA svolge infatti specifiche attività di progettazione, sviluppo e test di applicativi e servizi propri e di parti terze. Lo scopo di tali attività, che hanno carattere tipicamente progettuale, è quello di aumentare la qualità dei servizi resi in termini di efficacia ed efficienza, tramite un processo controllato che ha come *input* principale i *feedback* provenienti dai membri della *constituency*.
Nel corso del 2017 il CERT-PA ha portato avanti 4 progetti di sviluppo, alcuni dei quali iniziati già nel 2016, riguardanti ambiti quali: lo sviluppo di una *Web application* per il monitoraggio OSINT delle minacce cibernetiche, il test di prodotti di *sandboxing* di parti terze, lo sviluppo di una Web application per la gestione di vulnerabilità applicative e IoC noti, il coordinamento di un Gruppo di Lavoro nazionale incaricato di definire le modalità di comunicazione di eventi di sicurezza mediante utilizzo di protocolli e linguaggi standard (STIX, TAXII).

Piani per il 2018: il CERT-PA e la Direttiva NIS

Un fattore di accelerazione nell'evoluzione delle strutture di sicurezza cibernetica nazionale, al quale si deve almeno in parte anche l'emanazione del Decreto Gentiloni e del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, è la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, meglio nota come Direttiva NIS, che deve essere recepita e diventare operativa entro maggio prossimo.

Recepimento della NIS: l'Italia non è impreparata

Nonostante gli alti lai che da più parte si sono levati e continuano a diffondersi, il Paese, grazie allo sforzo prodotto a partire dal 2013 non si trova all'anno zero, ma, al contrario, può vantare una normativa di tutto rispetto ed un'applicazione di tutto rispetto.

Organizzazione CS nazionale: i CERT nazionali

L'organizzazione per la sicurezza cibernetica nazionale, che nella sua attuale configurazione e consistenza è stata ben descritta nella Relazione sulla politica dell'informazione per la sicurezza – Anno 2017 recentemente pubblicata, poggia su strutture operative tra le quali è consolidata una stretta collaborazione: il CNAIPIC della Polizia Postale, Il CIOC della Difesa ed i CERT di AgID e del MISE, destinati rispettivamente al settore pubblico ed al settore privato.

CERT vs. CSIRT

Già oggi i due CERT, già dal Piano nazionale di marzo 2017 destinati ad una cooperazione sempre più stretta fino alla riunificazione delle risorse, svolgono le funzioni di risposta agli incidenti che la NIS pone in capo agli CSIRT. Anzi svolgono un'attività di monitoraggio ed

analisi dello spazio cibernetico, nonché di individuazione delle misure di contrasto delle nuove minacce, che sono proprie di un CERT e che fanno interpretare al CERT-US (CERT federale USA) la "R" dell'acronimo come iniziale di "Readiness" piuttosto che di "Response". Occorre pertanto implementarli fornendo loro adeguate risorse economiche, lo sviluppo degli scorsi anni è avvenuto "senza oneri aggiuntivi per la finanza pubblica", e soprattutto umane, visto che gli attuali organici si contano sulle dita di una mano. Occorre inoltre dotarli degli strumenti necessari per gestire le notifiche, che sono la vera novità della NIS, nell'ambito della rete degli CSIRT da essa prevista.

Preservare l'esperienza

È però importante preservare le capacità di analisi, indagine ed approfondimento presenti oggi nel CERT-PA, con le quali si alimenta il CS-KDB, altrimenti l'evoluzione indotta dalla NIS sarebbe in realtà un'involuzione verso una sorta di Super-SOC (Security Operation Center) in grado esclusivamente di applicare strategie e direttive prodotte da altri, senza capacità di controllo e sviluppo delle competenze nazionali, in un campo in cui queste nascono più dalla capacità e dall'esperienza sul campo che dalla speculazione accademica, che pure è una componente determinante nella costruzione di qualunque conoscenza solida.

Il Piano Triennale dell'AgID

PT: Cos'è e da dove proviene

Sotto il profilo strategico, l'attività più impegnativa dell'Agenzia per l'Italia Digitale (AgID) è la redazione annuale del Piano Triennale per l'informatica nella Pubblica Amministrazione, che il Presidente del Consiglio dei ministri deve adottare ogni anno entro ottobre.
Tale adempimento, che risale al tempo dell'Autorità per l'Informatica nella P.A. (AIPA), definisce il percorso evolutivo dell'impiego delle tecnologie informatiche all'interno della Pubblica Amministrazione e quindi, in definitiva, traccia il solco entro cui questa nel suo complesso si evolve.

La sicurezza cibernetica nel PT

Il Piano 2017- 2019, approvato ed adottato lo scorso anno, individua una serie coordinata di interventi che partono dal livello infrastrutturale, materiale (reti e data center) ed immateriale (basi informative, piattaforme, servizi abilitanti), per articolarsi in ecosistemi verticali (sanità, scuola, giustizia, etc.) che forniscono servizi ai cittadini e le imprese. Esso presta particolare attenzione alla sicurezza cibernetica, anche a causa dell'interesse montante a livello mondiale che si è tradotto concretamente in una serie di interventi, dal "Decreto Monti" (DPCM 13 gennaio 2013), alla Direttiva 1 agosto 2015, al "Decreto Gentiloni" (DPCM 17 febbraio 2017), hanno dato forma al sistema di sicurezza cibernetica nazionale. Oltre alle attività più propriamente strategiche e regolamentari (quali ad esempio le Misure minime di sicurezza ICT per le pubbliche amministrazioni – Circolare AgID n.2/2017 del 18 aprile 2017) nel Piano viene dato un ruolo importante all'attività operativa condotta

dal CERT-PA (Computer Emergency Response Team della Pubblica Amministrazione), la struttura di AgID preposta alla prevenzione e gestione degli incidenti informatici nella PA.

Il CS-KDB

Nel PT è previsto che AgID, attraverso il CERT-PA, metta in campo una specifica infrastruttura immateriale, il Cyber Security Knowledge Data Base, quale risorsa di base per costruire molteplici strumenti destinati alla sicurezza delle informazioni e dei sistemi.

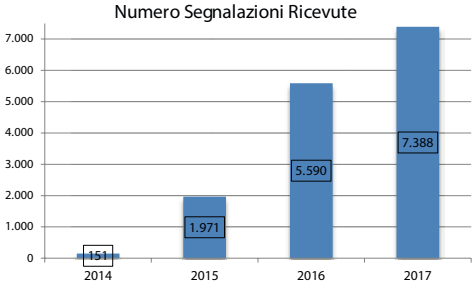
Infosec

Il primo nucleo di tale infrastruttura, destinata a raccogliere ed organizzare le conoscenze riguardo ai vari aspetti della sicurezza informatica, vulnerabilità, strategie di attacco, malware, siti malevoli, incidenti, misure di sicurezza, linee guida e quant'altro possa tornare utile ai fini del contrasto degli attacchi informatici, è già operativo in via sperimentale sotto l'etichetta Infosec ed a disposizione non solo delle pubbliche amministrazioni, ma di tutta la comunità cyber nazionale e anche internazionale, se è vero che nel mese di gennaio 2018 solo un terzo degli oltre 2 milioni di accessi che sono stati effettuati, proveniva dall'Italia.

Attività e segnalazioni del CERT Nazionale

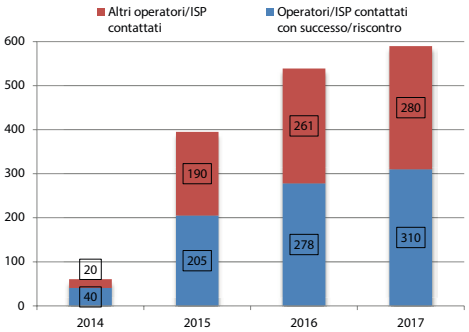
Le attività: alcuni dati

A circa 4 anni dall'avvio dell'operatività il CERT Nazionale è ormai una realtà riconosciuta tra gli addetti ai lavori nell'ambito della sicurezza informatica nazionale ed internazionale



Il grafico mostra l'incremento delle segnalazioni dall'avvio delle attività fino a dicembre 2017.

Parallelamente anche il numero di soggetti con i quali il CERT Nazionale si è interfacciato - come fornitore o consumatore di dati relativi alla sicurezza informatica dello spazio cibernetico italiano – ha presentato una crescita costante dal 2014 ad oggi.

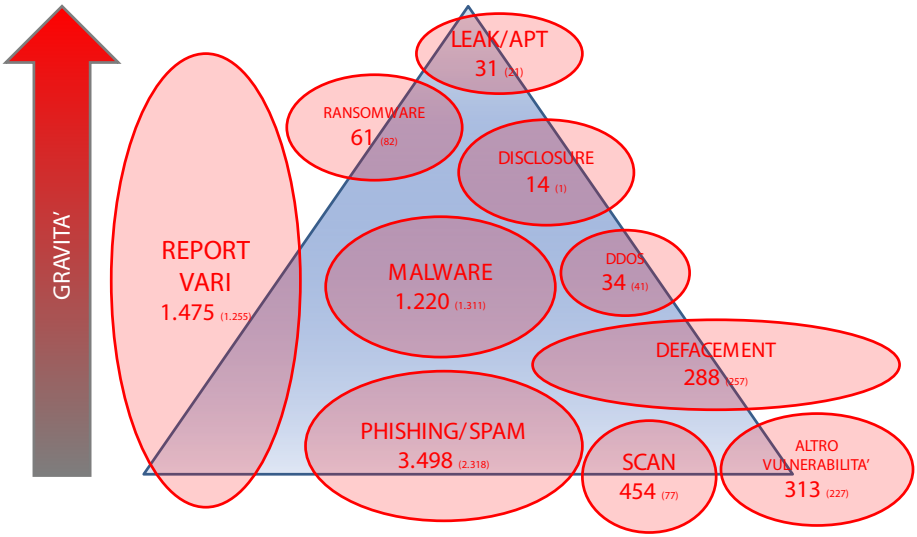


Di particolare importanza, in questo ambito, è il rapporto con gli Operatori TLC e gli *Internet Service Provider* italiani. Tra questi sono quasi 600 i soggetti ai quali il CERT Nazionale ha inviato segnalazioni di vario genere legate alla sicurezza informatica delle reti da questi gestite. Con la maggior parte dei provider si è instaurato un contatto proficuo che ha consentito la risoluzione delle problematiche.

Anche il numero il numero di omologhi CERT a livello internazionale con i quali il CERT Nazionale italiano è entrato in contatto è in costante crescita con un numero che si attesta ad oltre 50 soggetti di altrettanti Paesi.

Segnalazioni: le tipologie

Le tipologie di segnalazioni che giungono quotidianamente al CERT Nazionale sono di vario genere. Volendo darne una classificazione secondo un parametro di "gravità", basato essenzialmente sul tipo e la vastità dell'impatto, il 2017 ha continuato a registrare un notevole incremento delle segnalazioni legate al *phishing*, ma anche le compromissioni legate alla diffusione di *malware* (in particolare *ransomware*) e/o *botnet* hanno rappresentato una quota decisamente non trascurabile.



Nota: tra parentesi i valori relativi al 2016

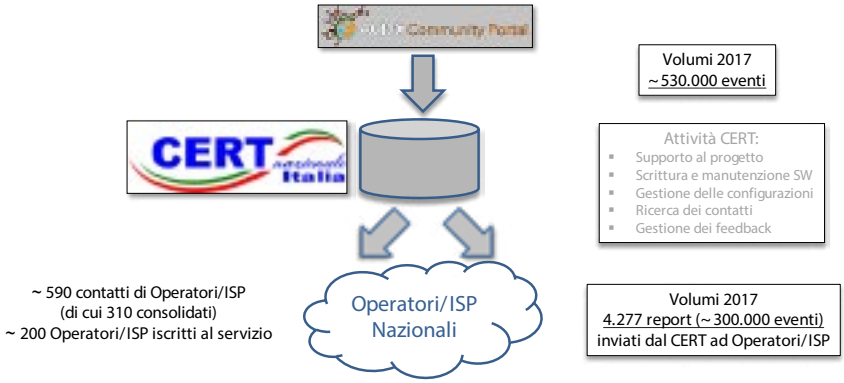
Seppure numericamente limitate, segnalazioni relative ad APT – *Advanced Persistent Threat* – o a compromissioni di credenziali (*leak*) rappresentano gli incidenti di più difficile risoluzione e di maggiore impatto.

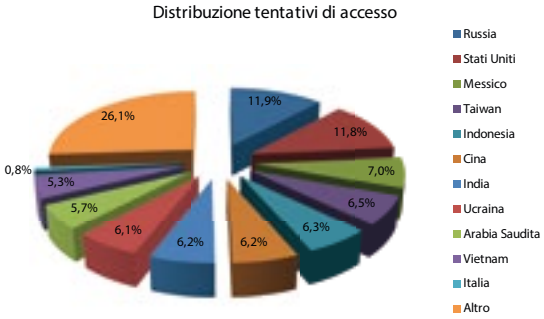
La rappresentazione riportata non è chiaramente esemplificativa dello stato dell'arte globale, ma una vista di quanto pervenuto al CERT Nazionale.

La reportistica periodica sulla quale il CERT Nazionale può contare rappresenta una fonte informativa estremamente interessante. I dati provengono sia da fonti interne, nella fattispecie le *honeypot* predisposte nell'ambito del progetto europeo ACDC (*Advanced Cyber Defence Center*), sia da fonti esterne. Le fonti esterne sono generalmente di tipo *semi-aperto*, ovvero fonti potenzialmente aperte ma per le quali il CERT Nazionale può contare su viste complessive dell'intero spazio di indirizzamento italiano, ma anche di tipo *chiuso*, tipicamente report provenienti da aziende di sicurezza o, più frequentemente, da omologhi CERT internazionali a fronte di attività specifiche di contrasto alla diffusione del *malware* e/o di *botnet*.

Rete anti-botnet

Nel corso del biennio 2016/17 è proseguita l'attività di diffusione agli Operatori coinvolti delle segnalazioni fornite dalla rete *anti-botnet* del progetto europeo ACDC (*Avanced Cyber Defence Center*, terminato nel corso del 2015, ma i cui risultati vengono ancora utilmente sfruttati).
L'informatizzazione della procedura di ricezione ed invio delle segnalazioni ha consentito di inviare oltre 4.000 report nel corso del solo 2017 agli oltre 200 Operatori iscritti al servizio.



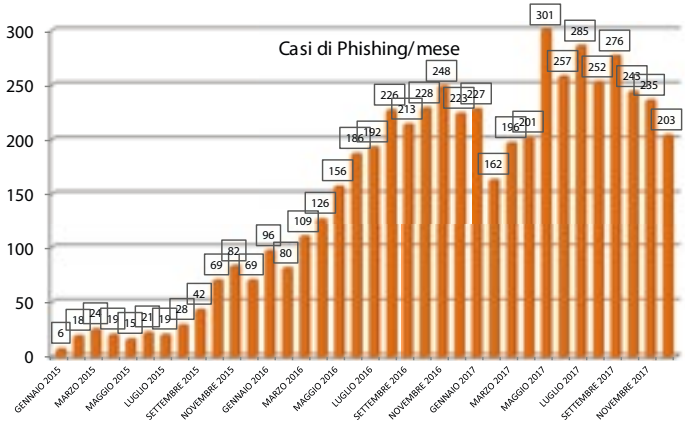


Tra l'altro la rete di *honeypot* predisposta nell'ambito del progetto, continua a raccogliere un notevole numero di eventi (oltre un miliardo nell'ultimo anno), tra tentativi di connessioni malevoli e tentativi di scaricamento di *malware*, consentendo anche di avere una ricca base dati sulla provenienza, a livello mondiale, di determinati tipi di attacco.

Il *phishing*

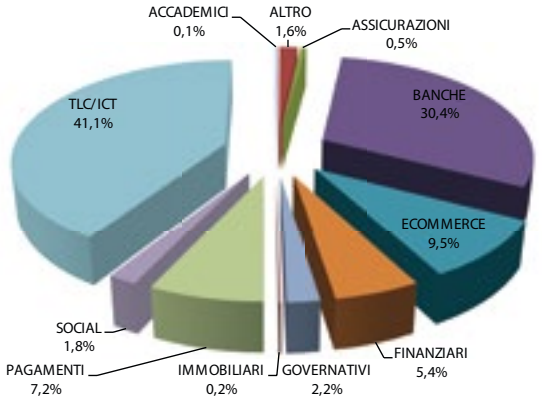
Nel corso del 2017 si sono registrate numerose campagne di *phishing* e *spear-phishing*, che restano i principali vettori di diffusione di *malware* e strumenti per la compromissione di

credenziali. In particolare diverse tecniche di *spear-phishing* sono state utilizzate per la diffusione di *malware* complessi e indirizzati a particolari settori merceologici.



Le segnalazioni di pagine di *phishing* ospitate su server italiani compromessi e pervenute al CERT Nazionale sono notevolmente cresciute nel corso del 2016 e del 2017, passando dalle circa 400 del 2015 alle oltre 2.000 del 2016 fino a superare le 2.800 nel 2017.

Generalmente questo tipo di segnalazioni giungono al CERT Nazionale solo dopo precedenti tentativi di contattare gli amministratori o di risolvere in altro modo l'incidente ed il numero rappresenta pertanto solo una parte del fenomeno, sebbene statisticamente rilevante.



La maggior parte degli attacchi hanno preso di mira grandi Operatori OTT (*Over The Top*) o del settore ICT e istituti bancari di tutto il mondo volti alla compromissione delle credenziali di accesso delle vittime. Molto diffusi sono stati anche i tentativi di compromissione di credenziali di servizi di *pagamento on-line*, di *social network* o di posta elettronica.
La compromissione dei siti utilizzati per le attività malevole si è rivelata spesso legata all'uso di CMS – *Content Management System* – obsoleti e vulnerabili per il mancato aggiornamento di vecchie versioni del software.

I principali incidenti

Il CERT Nazionale, grazie alla rete di *infosharing* (soprattutto con interlocutori internazionali, quali omologhi CERT nazionali o *Security Vendor*) riceve periodicamente report relativi a compromissioni da *malware*. Tali segnalazioni possono avere carattere periodico o *una tantum* e legate ad un singolo evento e, generalmente, si compongono di liste di macchine, e dei relativi indirizzi IP, compromesse da una specifica o da una pluralità di famiglie di *malware*. La compromissione è spesso rilevata da terze parti attraverso analisi di traffico specifiche (per esempio connessioni a *sinkhole* predisposti *ad hoc*) o di macchine a loro volta compromesse (per esempio C&C analizzati dopo la dismissione di infrastrutture fraudolente).

Tali segnalazioni, opportunamente analizzate, vengono inoltrate agli Operatori/ISP per le azioni di verifica e bonifica.

Nel corso del 2017 sono state lanciate diverse campagne informative, nei confronti degli operatori/ISP colpiti, relative a differenti *malware* o minacce di vario genere. Tra queste, per la loro particolare rilevanza, si ricordano:

- grazie all'operazione internazionale di *takedown* (risalente a dicembre 2016) della infrastruttura criminale "***Avalanche***", utilizzata per ospitare numerose *botnet*, il CERT Nazionale riceve informazioni relative a macchine appartenenti al *cyber* spazio italiano e verosimilmente compromesse, sulla base delle connessioni rilevate sui *sinkhole* della infrastruttura dismessa. Le famiglie di *botnet* rilevate hanno principalmente funzionalità volte al furto di credenziali o a frodi legate all'*online-banking*. Sulla base di tali informazioni il CERT Nazionale lancia delle campagne informative nei confronti degli Operatori/ISP coinvolti affinché, a loro volta, possano procedere con la disseminazione nei confronti degli utilizzatori finali;
- macchine compromesse con presenza di ***backdoor*** e potenzialmente sotto il controllo di criminali informatici;
- siti web compromessi, contenenti codice malevolo o oggetto di *defacement*;
- l'evento ***Wannacry*** ha rappresentato un evento epocale per la sua diffusione planetaria e per tutti i meccanismi di reazione che si sono resi necessari per la mitigazione degli effetti.

WannaCry, anche noto come *WCry*, *WanaCrypt0r* o *Wana Decrypt0r* 2.0, è una variante di *ransomware* che si è diffusa in maniera incontrollata in tutto il mondo a partire da venerdì 12 maggio 2017.
Il *malware* era stato individuato già qualche settimana prima dagli esperti di sicurezza del *MalwareHunterTeam*, ma inizialmente la sua diffusione appariva piuttosto limitata. Successivamente ha iniziato a diffondersi rapidamente su vasta scala sfruttando gli *exploit* denominati *EternalBlue* e *DoublePulsar*, parte di un pacchetto di strumenti di *hacking* rilasciato pubblicamente il 14 aprile 2017 dal collettivo di *hacker* noto come *Shadow Brokers* e che avrebbero sfruttato, tra l'altro, una vulnerabilità critica del protocollo **SMBv1** implementato nei sistemi Windows (**CVE-2017-0145**), per risolvere la quale Microsoft ha aveva già rilasciato opportune patch nel mese di marzo. Il CERT Nazionale ha immediatamente informato la propria constituency con l'emissione di alcuni avvisi sul proprio sito istituzionale e con la diffusione degli indicatori di compromissione.
Prima di attivare la funzionalità di *ransomware*, ovvero alla cifratura dei dati della vittima per poi procedere alla richiesta di un riscatto, il programma malevolo effettuava un controllo sull'esistenza online di alcuni URL: se non riceveva risposta dai domini codificati al suo interno, estraeva ed eseguiva sulla macchina della vittima un secondo componente, che implementava la funzionalità di cifratura. Nel caso, invece, in cui questi domini avessero risposto, il *malware* non si sarebbe attivato e avrebbe terminato la propria esecuzione. Questi domini, che funzionano quindi come dei veri e propri "***Kill Switch***", sono stati registrati, successivamente alla notizia della diffusione dell'infezione ed a seguito delle analisi effettuate su campioni di *malware*, da un ricercatore indipendente (*MalwareTech*) ed utilizzati come *sinkhole*, fermando l'azione del *malware* e rallentandone la diffusione, rendendo al contempo possibile l'individuazione di macchine compromesse che tentavano di connettersi a tali domini.
Nei giorni immediatamente successivi all'infezione, attraverso i canali di *infosharing* internazionale, il CERT Nazionale ha ricevuto, per tramite del CERT-EU, alcuni report relativi a connessioni registrate sui *sinkhole/kill switch* nel periodo compreso tra venerdì 12 a lunedì 15 maggio. Le informazioni sono state prontamente inviate agli Operatori coinvolti. Complessivamente sono stati rilevati circa **500 IP unici** appartenenti a reti italiane, a loro volta appartenenti a **43 AS differenti**, per un totale di circa **15.000 connessioni**;

- altri dati sono stati desunti giornalmente da servizi *semi-aperti* che mettono a disposizione del CERT Nazionale una vista dell'intero spazio di indirizzamento italiano, con particolare riferimento a macchine appartenenti a vari tipi di *botnet*.

Campagne Informative Preventive

Una seconda categoria di servizi offerti dal CERT Nazionale è di tipo proattivo, ovvero relativi ad informative riguardanti vulnerabilità o configurazioni scorrette potenzialmente utilizzabili da malintenzionati per attacchi informatici e, pertanto, volti a prevenire eventuali attacchi che possano sfruttare tali vulnerabilità.

Nel corso del 2017 sono state lanciate 18 *campagne di prevenzione*, con le quali sono state segnalate circa **70.000 macchine/IP esposte** a oltre 300 Operatori/ISP.

Le campagne sono state realizzate inviando ad ogni Operatore/ISP coinvolto, la lista delle macchine/IP afferenti alla propria rete che risultavano essere vulnerabili. L'obiettivo è sempre quello di sensibilizzare una corretta configurazione delle macchine da parte dei rispettivi amministratori di rete.

Nel dettaglio le principali campagne hanno riguardato:

- **CISCO SMI (Cisco Small Install):** si tratta di macchine con funzionalità Cisco Smart Install attiva ed aperta in rete. Questa funzionalità potrebbe essere utilizzata per leggere o, potenzialmente, modificare la configurazione dello switch (si veda *https://blogs.cisco.com/security/cisco-psirt-mitigating-and-detecting-potential-abuse-of-cisco-smart-install-feature*);

- **DNS Open Resolver:** si tratta di alcuni server DNS Open Resolver che risulterebbero essere aperti all'esterno e potenzialmente utilizzabili per attacchi di tipo *Cache Poisoning* o *DDoS* a danni di terze parti (si veda *https://www.us-cert.gov/ncas/alerts/TA13-088A*). Poiché tale servizio non richiede autenticazione, un malintenzionato, in assenza di altri accorgimenti di sicurezza, potrebbe tentare di accedere dall'esterno all'istanza attiva, prendendone il controllo;

- **IPMI** (*Intelligent Platform Management Interface, 623/udp*): IPMI è la specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC (*Baseboard Management Controller*) consente, tra le altre cose, l'accesso al *BIOS*, ai dischi ed ai dispositivi *hardware* in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno;

- **SMB** (*Server Message Block Protocol, 445/udp*): si tratta di macchine con protocollo SMB aperto in rete. È il protocollo utilizzato da *WannaCry* e attentamente monitorato dai criminali informatici nel corso dell'anno, come dimostra il crescente numero di *scan* rilevati sulla porta 445. Inoltre, ulteriori *disclosure* di vulnerabilità che affliggerebbero il protocollo *SMB* (come per esempio "*SMBLoris*": *https://certnazionale.it/news/2017/08/01/smbloris-scoperta-nuova-falla-di-smb-in-windows/*) potrebbero consentire anche ad attaccanti dotati di limitate capacità elaborative di portare attacchi di tipo "*Denial of Service*";

- **SMB IMPLANT:** si tratta di macchine che non solo avrebbero il protocollo SMB esposto, ma che risulterebbero anche essere state già compromesse con delle ***backdoor***. Nella immediatezza dell'attacco *WannaCry* il CERT Nazionale ha provveduto ad inviare

una serie di campagne informative al tempo stesso proattive e reattive con riferimento alle macchine coinvolte;

- **VNC** (*Virtual Network Computing, 5900/tcp*): l'apertura di tale protocollo all'esterno qualora non protetto (senza richiesta di autenticazione o con credenziali deboli, ma anche nei casi in cui il canale di comunicazione delle credenziali risulti in chiaro) o in una versione obsoleta rende le macchine ed i sistemi ospitati potenzialmente attaccabili da malintenzionati. Oltre al rischio della riservatezza dei dati, i malintenzionati potrebbero prendere il controllo totale della macchina con i conseguenti rischi, soprattutto nel caso in cui venissero ospitati servizi di controllo industriale (tipicamente *SCADA*), oltre a rendere teoricamente possibili movimenti laterali con conseguente compromissione di altri sistemi locali.
- **Vulnerabilità di servizi OwnCloud/NextCloud**, legata alla presenza e alla apertura in rete di installazioni non aggiornate del noto e diffuso software per la gestione di sistemi "*cloud*" locali. Alcune delle vulnerabilità presenti nelle versioni non aggiornate potevano essere sfruttate per accessi non autorizzati ai dati, con rischio per le informazioni sensibili contenute nei documenti contenuti nel sistema. Altre vulnerabilità avrebbero potuto invece essere sfruttate per l'esecuzione di codice arbitrario sul server che ospitava il sistema con possibile compromissione del sistema stesso. Sono state oltre 600 le istanze appartenenti a soggetti italiani, pubblici e privati, segnalate dal CERT Nazionale alle funzioni tecniche coinvolte.

Per restare nell'ambito delle attività di tipo preventivo il 2017 ha registrato un notevole aumento di segnalazioni provenienti da soggetti privati, generalmente ricercatori o esperti di sicurezza, talvolta anonimi.
Il CERT Nazionale si è impegnato nella verifica della correttezza e della affidabilità delle segnalazioni e, una volta accertata la presenza della falla o, in certi casi, della compromissione, ha proceduto all'inoltro delle stesse alle funzioni tecniche preposte. L'attività ha richiesto anche una attenta ricerca e valutazione dei soggetti ai quali inviare la segnalazione, dei quali si è sempre riscontrata la massima collaborazione e che hanno proceduto, in tempi generalmente molto stretti, alla risoluzione delle diverse problematiche di sicurezza rilevate.
Circa una dozzina i casi più seri che, nella maggioranza, mettevano a repentaglio informazioni personali della clientela. In altri casi a rischio erano le stesse credenziali di accesso. A questi si aggiungono quelli relativi a casi meno specifici ed a vulnerabilità di vario genere, tipicamente quelle che consentono classici attacchi di tipo *SQL Injection* o *Cross Site Scripting* (*XSS*).
La problematica riscontrata nei casi più gravi è stata quella di documenti teoricamente "riservati" ed invece pubblicamente disponibili in rete o comunque accessibili a soggetti non autorizzati, tipicamente per errori di programmazione con conseguenti falle di sicurezza di tipo "*Insecure Direct Object References*". Tali errori consentono, per esempio, ad un utente registrato ad un determinato servizio, di accedere non solo alla propria documentazione (come fatture, ordini, anagrafica ecc.), ma anche a quella appartenente ad altri utenti regi-

strati, con evidente problema di riservatezza delle informazioni, quando addirittura la problematica non si estenda anche alla possibilità di scrittura e/o modifica dei dati.
Le segnalazioni hanno riguardato diversi settori merceologici: dai **trasporti** alle **assicurazioni**, dalla **telefonia** all'**energia**.
È emerso che la fonte informativa proveniente da soggetti privati non malintenzionati può essere una preziosa risorsa per la prevenzione di incidenti gravi che in genere si concretizzano con il *leak* di informazioni (siano esse informazioni personali che credenziali di accesso ai sistemi) o con la *disruption* dei sistemi stessi.

Il sito web

Il sito web del CERT Nazionale (***https://www.certnazionale.it***) si rivolge a cittadini ed imprese con **notizie** di interesse generale legate alla sicurezza informatica, **bollettini** tecnici e **linee guida** di comportamento.

L'obiettivo è quello di trattare argomenti tecnici con la necessaria precisione, ma cercando di renderne i contenuti utili e comprensibili anche a chi non necessariamente ha profonde conoscenze tecniche.

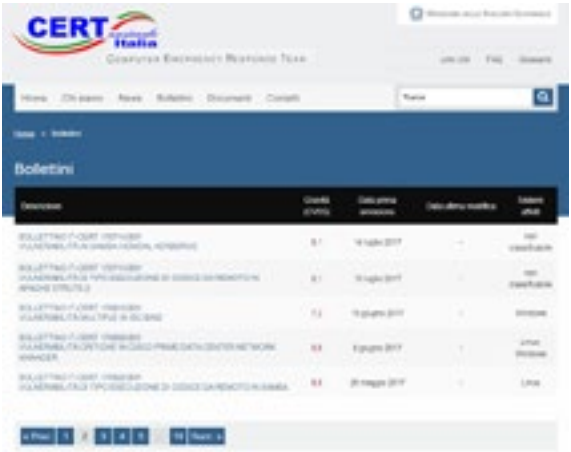
Le **notizie** (***news***), pubblicate con cadenza giornaliera, rappresentano da questo punto di vista un ragionevole compromesso tra una trattazione tecnica specialistica ed una informativa generale relativa alle problematiche di sicurezza del momento.
Le pubblicazioni contengono informazioni utili per tutti gli utilizzatori di sistemi informatici, a partire dalla descrizione delle problematiche di sicurezza rilevate in rete, alla disponibilità di aggiornamenti, a suggerimenti generali o particolari, per la protezione dei propri dati.
Particolare attenzione nel corso del 2017 è stata riservata alla problematica del *ransomware*, visti anche gli incidenti che hanno caratterizzato l'annata. In particolare il CERT Nazionale ha predisposto la notizia relativa a *WannaCry* e alle azioni preventive per evitare l'infezione non appena avuta evidenza dei dettagli dell'attacco e delle tecniche di mitigazione.

Analoga attenzione alla tempestività ed ai contenuti è stata riservata anche in altri casi di eventi a diffusione globale, anche se con un minore impatto mediatico a livello complessivo. Oltre a fornire elementi tecnici utili, tra i quali precisi indicatori di compromissione o indicazioni di massima sulla prevenzione e soluzione del problema, obiettivo dei comunicati resta quello di riassumere le azioni necessarie per evitare di diventare vittime di criminali informatici, spesso legate al buon senso più che a conoscenze tecniche particolarmente approfondite.

A tal fine particolare rilievo viene dato agli avvisi relativi alla pubblicazione di aggiornamenti di sicurezza per la piattaforme più diffuse, per le quali la raccomandazione è sempre quella di mantenere una versione non obsoleta sui propri sistemi.

I **bollettini** rappresentano invece un approfondimento tecnico specialistico, dedicato ai

soggetti più esperti del settore, su argomenti di particolare importanza, tipicamente vulnerabilità riscontrate su piattaforme o sistemi di vasta diffusione e con impatti potenzialmente molto estesi.



Nel corso del 2017, oltre alle attività di manutenzione ordinaria del sito, sono state pubblicate:

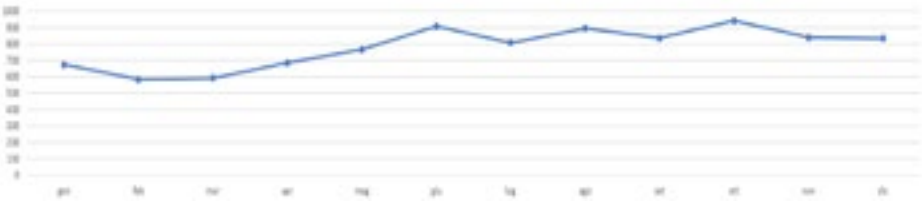
- **329 notizie** a valenza informativa di vasto interesse;
- **23 bollettini** tecnici specialistici.

Rapporto 2017 sullo stato di Internet e analisi globale degli attacchi DDoS e applicativi Web [a cura di AKAMAI]

1. Attività degli attacchi DDoS

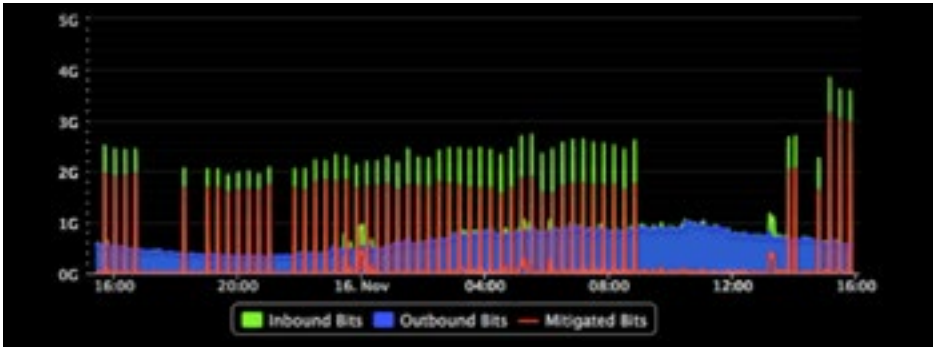
a. Un anno record per la frequenza degli attacchi

Come quasi ogni anno, il 2017 ha visto un incremento sostanziale nel numero totale di attacchi DDoS. La base di analisi, infatti, è di 9.362 attacchi, che significa una media di più di 25 attacchi al giorno.

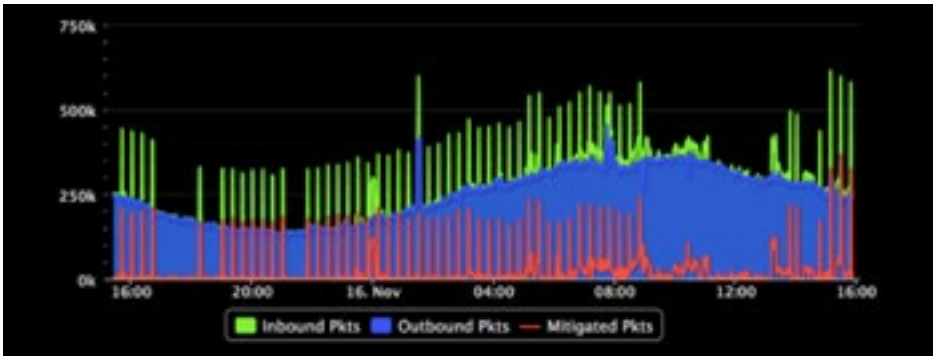


Il principale fenomeno da notare è che la dimensione massima degli attacchi è leggermente diminuita rispetto agli anni precedenti; ciò dipende dal fatto che le strategie di attacco sono cambiate nel tempo. Per lanciare attacchi DDoS c'è stato, infatti, un maggiore utilizzo di booter e stressers, che in ogni caso hanno un costo sul "mercato hacker", oltre a ciò il cambiamento sostanziale rispetto agli anni precedenti è la frequenza e persistenza degli attacchi su singolo bersaglio.
Basti considerare che soltanto nel Q3 2017 un singolo sito è stato attaccato 612 volte. Nell'arco dell'anno il record è di un sito attaccato più di 2000 volte.

Ill 2017 ha visto anche l'aumento degli attacchi cosidetti Hit & Run o Pulse Wave. Sono attachi di breve durata ma frequenti nell'arco di poche ore.
Un esempio di attacco Hit & Run è mostrato nelle figure qui di seguito, in cui la prima immagine illustra i bit per secondo e la seconda il numero di pacchetti al secondo.



Come precedentemente discusso il numero di attacchi nell'unità di tempo è molto alto, mentre la loro durata è decisamente bassa. Altro fenomeno importante degli attacchi Hit & Run è la loro capacità di mantenere alto il livello di pacchetti al secondo, che è tanto pericoloso quanto il bit per secondo. Sono i pacchetti al secondo, infatti, ad alzare il livello di consumo di risorse hardware e, conseguentemente, a rendere più incisivo un attacco.

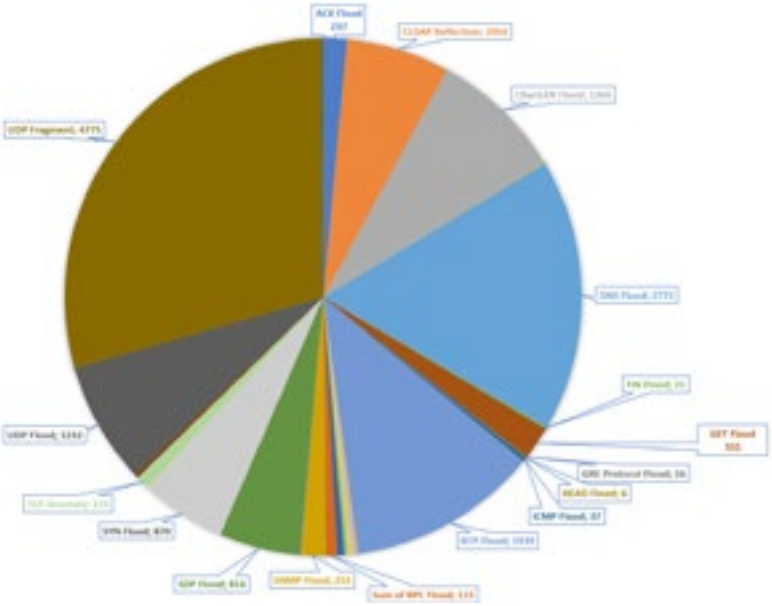


Ecco il fenomeno dominante del 2017: attacchi di minore persistenza ma ripetuti con frequenza molto alta. Il problema principale nella mitigazione di questo tipo di attacchi è relativo alla prontezza di riflessi nella mitigazione stessa. Bloccare un attacco che non dura più di 5 minuti è complesso, in quanto sono attacchi di durata molto vicina al limite minimo temporale per attivare correttamente le tecnologie di mitigazione.
"Pulse Wave" o "Hit & Run": facili da identificare, difficili da mitigare.

b. Vettori di attacco

Forti dell'esperienza degli anni passati, è stato confermato anche per quest'anno la dominanza, come vettore di attacco principale, dell'UDP Fragment. Ciò è dato dalla semplicità di esecuzione di volumi di traffico UDP, mentre la frammentazione degli stessi è altrettanto semplice, basta avere nozioni base di MTU (Maximum Transimssion Unit).

Per le caratteristiche di gestione dei volumi di traffico degli attacchi, seguono a breve distanza DNS Flood e NTP Flood, i quali offrono il massimo rendimento in termini di amplificazione, e in particolare il DNS Flood obbliga alla frammentazione UDP.



Mirai, e quindi attacchi basati su Botnet e GRE flood, sono rimasti anche se in piccola percentuale. Ciò è dovuto da un lato al progressivo abbandono della tecnologia basata su Mirai, mentre dall'altro lato alcune varianti di Mirai sono state utilizzate comunque nel 2017, dove, ad esempio, si sono verificati attacchi che hanno utilizzato SATORI, che, basati sul malware Mirai, hanno generato picchi da 109 Gbps.

Il fenomeno forse più interessante del 2017 è stato l'utilizzo di WireX, di cui segue un approfondimento nelle pagine sucessive.

c. Le principali nazioni sorgenti di attacco

Nonostante la Cina sia stata una tra le principali nazioni sorgente di attacchi ormai da più di un anno, nel 2017 è scesa al secondo posto, preceduta dagli Stati Uniti, i quali sono stati per buona parte dell'anno vicini a passare un ordine di grandezza rispetto la Cina.
I dati indicano come gli attacchi mensili provenienti dagli Stati Uniti siano vicini al milione di IP a settimana, mentre quelli provenienti dalla Cina si attestano poco sopra ai centomila. A seguire con qualche migliaio di IP a settimana troviamo Brasile, Germania, Francia e

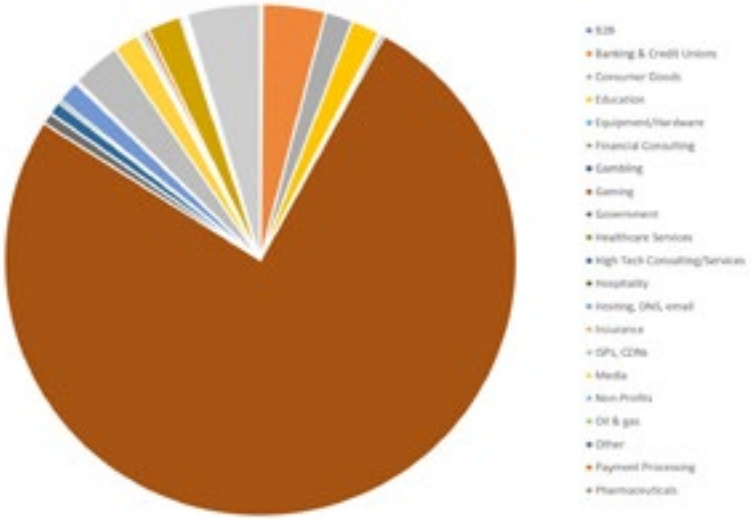
Inghilterra.
Costante nel tempo, con una media mensile di circa 36.000 IP si inserisce il Pakistan, che insieme all'Australia si pone tra le top 10 nazioni che maggiormente attaccano.

Q2 2017		Q1 2017		Q4 2016		Q3 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
Egypt	32%	U.S.	44%	U.S.	24%	China	19%
	44,198		594,986		180,652		81,276
U.S.	8%	U.K.	13%	U.K.	10%	U.S.	14%
	11,113		177,579		72,949		59,350
Turkey	5%	Germany	7%	Germany	7%	U.K.	10%
	7,049		87,780		49,408		44,460
China	4%	Canada	5%	China	6%	France	6%
	5,711		60,581		46,783		23,980
India	4%	Brazil	3%	Russia	4%	Brazil	3%
	5,224		43,863		33,211		13,502

d. Suddivisione per Vertical

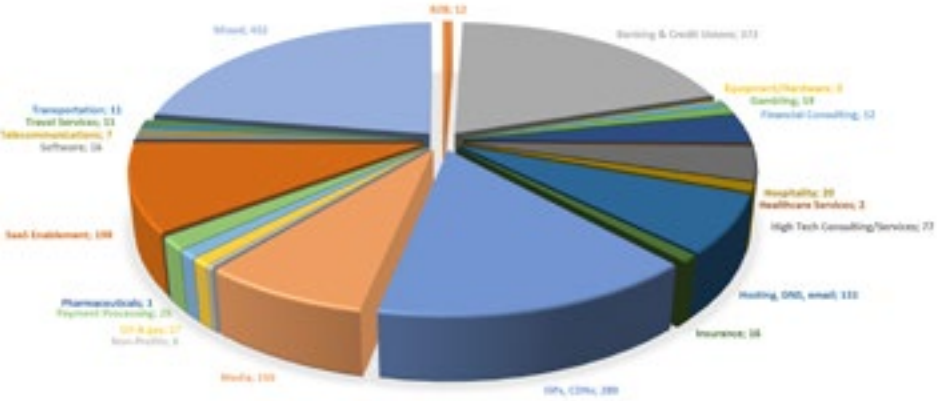
Considerando il 2017 come l'anno in cui il settore del Gaming è stato il più attaccato in assoluto con valori di ordine di grandezza superiore a tutti gli altri settori, è necessario riportare due indicazioni: una che lo include e una seconda che esclude il settore Gaming.

Il quadro riassuntivo della situazione generale è illustrato nel grafico di seguito, che illustra come il settore Gaming abbia subito 7109 attacchi nell'anno e quale sia il suo rapporto rispetto agli altri vertical.



Il settore Gaming storicamente ha sempre subito picchi di attacco verso la fine dell'anno, legati anche al Black Friday e al periodo natalizio. Nel 2017 questo settore ha avuto, contrariamente al solito, una quantità di attacchi pressochè costante nei mesi.

Se per chiarezza grafica si esclude il Gaming dall'analisi, la situazione risulta essere la seguente:



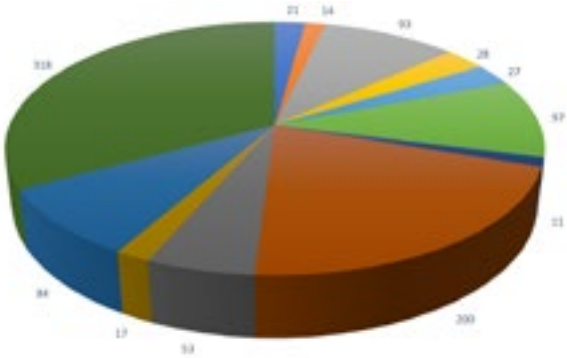
Dalla precedente immmagine risulta chiaro che alcuni fenomeni siano da considerare "naturali". Ad esempio il Vertical formato da aziende che offrono hosting o che trasmettono dati per conto dei loro clienti ("ISPs, CDNs" e "Hosting, DNS, email") è tra i più attaccati; ciò accade perchè in realtà ad essere attaccati sono i loro clienti.

È importante notare la quantità di attacchi subiti dai settori "Banking & Credit Unions" (373 attacchi) e dal settore "Media" (150 attacchi).
Il settore "Banking & Credit Unions", infatti, è stato particolarmente colpito nell'arco del 2017 con una varietà di attacchi sia di tipo DDoS che applicativi.
Da notare rispetto al grafico è il fatto che alcune aziende ricadono, per loro natura, all'interno di più di un vertical. Esse sono state raggruppate sotto la voce "mixed".

VERTICAL	N° di Attacchi
B2B	12
Banking & Credit Unions	373
Equipment/Hardware	3
Financial Consulting	12
Gambling	19
Government	68
Healthcare Services	2
High Tech Consulting/Services	77
Hospitality	20
Hosting, DNS, email	131
Insurance	16
ISPs, CDNs	289
Media	150
Mixed	432
Non-Profits	6
Oil & gas	17
Other	19
Payment Processing	29
Pharmaceuticals	1
SaaS Enablement	198
Software	16
Telecommunications	7
Transportation	11
Travel Services	11

Come indicato all'inizio del documento un fenomeno che ha caratterizzato il 2017 è la quantità di attacchi per singolo cliente, dovuto anche ad attacchi di tipo Hit & Run. Questo trend ha colpito tutti i vertical secondo la distribuzione illustrata nella figura che segue.

Vertical	N° di attacchi per singolo cliente
Banking & Credit Unions	21
Consumer Goods	14
Education	93
Government	28
High Tech Consulting/Services	27
Hosting, DNS, email	97
Insurance	11
ISPs, CDNs	200
Media	53
Payment Processing	17
SaaS Enablement	84
Electronics	318

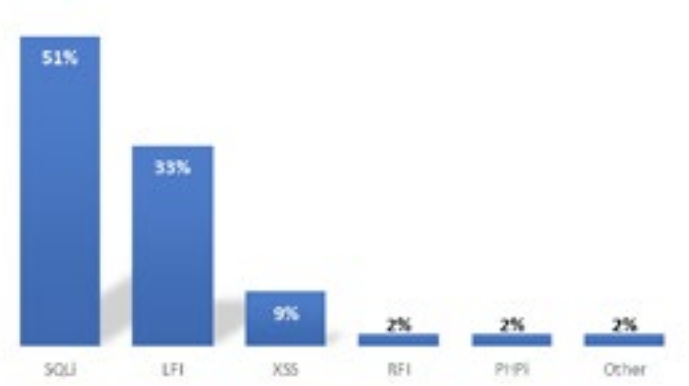


2. Attività degli attacchi applicativi web

a. Vettori di attacco

Per quanto riguarda i vettori di attacco il 2017 ha visto un leggero incremento rispetto al precedente anno con la stessa distribuzione di vettori.

Tre vettori compongono il 95% del totale degli attacchi applicativi: SQL Injection (SQLi), Local File Inclusion (LFI), Cross Site Scripting (XSS). Al contrario, Remote File Inclusion (RFI), PHP Injection (PHPi) e Malicious File Upload (MFU), sono stati registrati quasi solo come rumore di fondo.

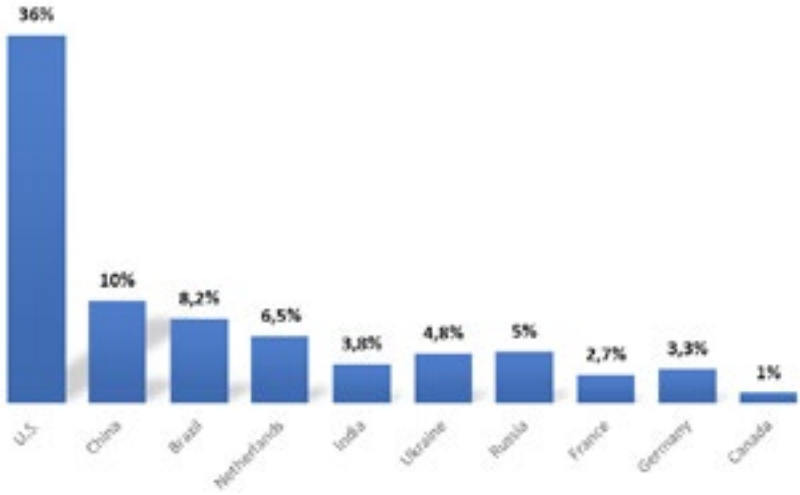


La maggior parte degli attacchi applicativi web è stata eseguita su protocollo HTTP (68%) invece che HTTPS (32%). Non c'è un'attenzione degli attaccanti verso applicazioni HTTPS

e molti strumenti non sono configurati per eseguire attacchi su SSL in modo predefinito. È quindi possibile e consigliato ottenere una semplice protezione di base cifrando i dati in transito, forzando il passaggio degli utenti da HTTP a HTTPS.

b. Le principali nazioni sorgenti di attacco

Abbiamo analizzato la sorgente degli attacchi dopo che la sessione TCP è stata stabilita. Nonostante questo, gli strumenti utilizzati cercano di nascondere la posizione reale dell'attaccante, non tramite manipolazione della sorgente dei pacchetti come viene fatto comunemente con il traffico UDP, ma tramite l'uso di VPN o server proxy.
I dati raccolti si basano quindi sull'indirizzo IP dell'ultimo hop osservato e mostrano gli Stati Uniti come la principale sorgente di attacchi applicativi web. Seguono Cina, Brasile e Olanda, tra i primi posti nella classifica dei paesi con più sorgenti di attacco.



c. Le principali nazioni destinazioni di attacco

Gli Stati Uniti sono la maggiore destinazione degli attacchi applicativi web: due terzi degli attacchi sono stati rivolti a server posizionati in territorio americano.
Moltissime organizzazioni, e le loro infrastrutture, hanno sede in questo paese, ci si aspetta quindi che i dati non cambino facilmente: gli Stati Uniti rimarranno il principale obiettivo degli attacchi anche in futuro. A seguire, Brasile e Germania sono risultati tra i paesi con maggiori attacchi subiti. L'Olanda, nonostante sia stata una frequente sorgente di attacchi, non compare tra i paesi più attaccati.

Approfondimento 1: WireX

Un fenomeno particolare visto nel corso del 2017 è stata la botnet denominata WireX.

WireX è un metodo di attacco di Denial of Service volumetrico destinato all'application layer.
Essa genera principalmente traffico di HTTP GET, anche se in alcune sue varianti pare in grado di generare traffico di POST Requests.
La prima volta WireX è apparsa durante i primi giorni di Agosto 2017 e data la sua peculiarità non è stata immediatamente notata, se non quando i ricercatori hanno cominciato a controllare particolari User-Agent che caratterizzano questa botnet.
A partire poi dal 15 Agosto WireX è cresciuta fino a lanciare attacchi che hanno coinvolto 70.000 IP sorgenti contemporaneamente e da più di 100 nazioni.
Il comportamento dai primi giorni di Agosto fino al 15 Agosto, in cui WireX ha lanciato attacchi di piccolissima entità, suggerisce che durante quel periodo la Botnet fosse ancora in via di sviluppo e che, conseguentemente, gli attacchi fossero dei test.
WireX come comportamento, genera richieste HTTP (HTTP GET) valide e correttmente formattate, simulando client e browser generici.
L'identificazione di WireX è possibile perchè inserisce nell'HEADER di richiesta uno user-Agent formato da una stringa di caratteri completamente random, come illustrato in alcuni esempi qui sotto.

```
User-Agent: jigpuzbcomkenhvladtwysqfxr
User-Agent: yudjmikcvzoqwsbflghtxpanre
User-Agent: mckvhaflwzbderiysoguxnqtpj
User-Agent: deogjvtynmcxzwfsbahirukqpl
User-Agent: fdmjczoeyarnuqkbgtlivsxhwp
User-Agent: yczfxlrenuqtwmavhojpigkdsb
User-Agent: dnlseufokcgvmajqzpbtrwyxih
```

Oltre a questi header ne sono poi stati riconosciuti altri come varianti.

```
User-Agent: xlw2ibhqg0i
User-Agent: bq5pdrxhka2ajr1g
User-Agent: 5z5z39iit9damit5czrxf655ok060d544ytvx25g19hcg18jpo8vk3q
User-Agent: fqe26ad5elvnyp3bdmc6ie0
User-Agent: m8al87qi9z5oqlwc8mb7ug85g47u
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; nl; rv:1.9.1b3)
Gecko/20090305 Firefox/3.1b3 (.NET CLR 3.5.30729)
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.7)
Gecko/20071018 BonEcho/2.0.0.7
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_7; en-us)
AppleWebKit/530.19.2 (KHTML, like Gecko) Version/4.0.2
```

A segito di questi primi eventi, tramite l'analisi di log, è stato possibile risalire ai vettori: WireX è generata da apparati Android e il malware che scatena la bot è annidato all'interno dell'applicazione denominata "twdlphqg_v1.3.5_apkpure.com.apk".

In un secondo momento sono state scoperte altre applicazioni dello stesso autore (o con nomi molto simili) e con simile descrizione.
Molte tra queste applicazioni fanno parte della categoria media e video players, suonerie.
Lanciando queste applicazioni, il malware lancia un servizio che interroga la Command & Control (tipicamente g.axclick.store) per ricevere i comandi di attacco.
WireX sfrutta una caratteristica dell'architettura Android che permette alle applicazioni di utilizzare risorse di sistema anche se le applicazioini stesse sono in background.

Approfondimento 2: fenomeno di extortion

Sebbene i fenomeni di extortion, principalmente tramite pagamenti in bitcoin, non siano putroppo un'eccezione ma una regola, è interessante notare che Akamai nel primo quarter del 2017 ha identificato un attacco di extortion decisamente anomalo e inusuale.

L'anomalia riguardo a questo attacco risiede nel fatto che non utilizza l'email per inviare le istruzioni di pagamento.

Allo stesso modo, questo tipo di attacco non avvisa di un prossimo attacco DDoS a fronte di un mancato pagamento.
Questo attacco lancia un DDoS che contiene le istruzioni di pagamento direttamente nella GET, la quale indica un URL di pastebin che a sua volta contiene le istruzioni per il pagamento, come illustrato qui di seguito.

```
GET /to_prevent_this_attack_pastebin.com/FAzyKAqE HTTP/1.1
Host: ********.net
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Accept: image/webp,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4
```

L'indirizzo pastebin, che viene automaticamente cancellato dopo 5 giorni dalla partenza dell'attacco, contiene il seguente testo

http://www.pastebin.com/FAzyKAqE

> Send 10 bitcoins to 13F2m8ctyRaFApp7x9eXmW1W39uE6Mo6SV
>
> We will never come back again.

In questo particolare caso non vi sono quindi sintomi del fatto che un attacco stia per essere lanciato, in quanto non ci sono avvisi né email.
L'attaccante deve quindi contare sul fatto che il bersaglio ispezioni i propri log e si renda conto del contenuto della GET.
Per dare tempo al destinatario di analizzare i log e recarsi sulla pagina pastebin, l'attacco è durato 8 ore consecutive.

Guardando al futuro

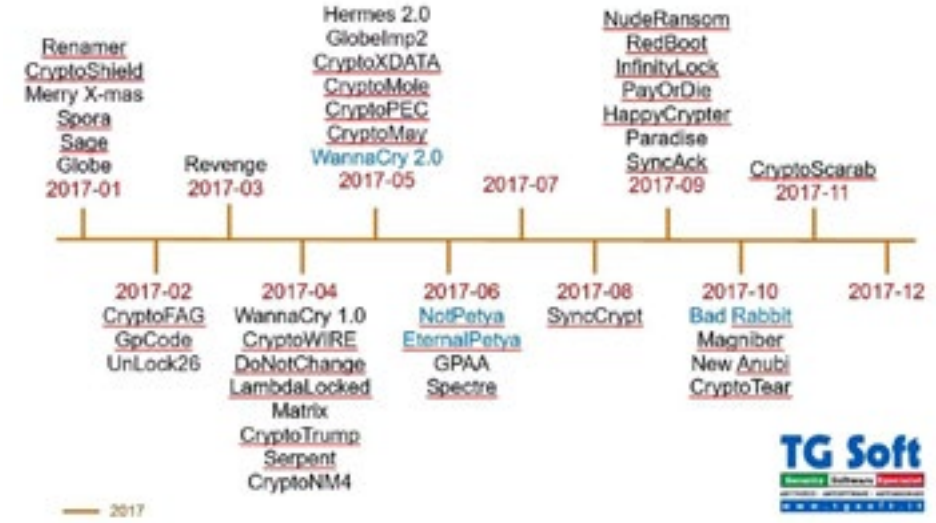
L'anno che si è appena aperto, secondo le previsioni di Akamai, vedrà una recrudescenza di attacchi sia a livello applicativo che DDoS e la frequenza sempre maggiore con cui il servizio di Threat Intelligence di Akamai rilascia bollettini ne è testimone.

SATORI, variante di Mirai, non ha sortito gli stessi effetti della sorella maggiore ma nuovi attacchi ci aspettano.
I fenomeni più importanti che saranno sempre più in auge sono gli attacchi Hit & Run e quelli "ibridi", in cui attacchi DDoS verranno mescolati ad attacchi applicativi.

La dimensione degli attacchi DDoS sta calando e ciò è dovuto alle mitigazioni messe a disposizione dei clienti, che rendono necessario per i malintenzionati trovare nuovi veicoli e nuovi modelli.
I DDoS che utilizzano un singolo vettore e che sfruttano al meglio i fenomeni di amplificazione non sono più efficaci come negli anni scorsi, ragion per cui i malintenzionati devono pensare a soluzioni complesse come WireX o l'attacco applicativo di extortion visto al paragrafo precedente.
Questo feonomeno porterà ad avere DDoS di dimensioni minori rispetto agli anni passati ma più complessi da identificare e gestire, dove il contributo di intelligence, che sfrutta tecnologie ma che deve poi essere analizzato da persone esperte che sappiano ragionare come gli attaccanti sarà sempre più determinante.

Ransomware 2017 in Italia – WannaCry, NotPetya/ EternalPetya, BadRabbit… ma non solo [A cura di TG Soft]

Anche nel 2017 i ransomware si sono presentati con tutta la loro devastante potenza distruttiva. Nei primi mesi del 2017 sono continuate in modo massivo le campagne del CryptoLocker (TorrentLocker), Cerber e Locky, ma non sono mancati i casi eclatanti di nuovi ransomware che hanno contraddistinto il 2017 tra maggio e ottobre.



Già a partire da gennaio troviamo una nutrita schiera di nuovi ransomware che hanno colpito anche l'Italia: Renamer; CryptoShield; MerryXmas; Spora; Sage e Globe.

Il Trojan.Win32.Renamer è da considerarsi un ransomware particolare, perché non cifra il contenuto del file, ma il nome del file, rendendo inaccessibile ogni esecuzione del programma colpito. Si diffonde attraverso un attacco al desktop remoto attraverso l'utente "*Guest*" o altri utenti con **password deboli**.
Quando il malfattore riesce ad entrare nel computer delle vittima esegue il payload con il **Trojan.Win32.Renamer**.
Ogni file viene rinominato aggiungendo il prefisso iniziale "**unCrypte@INDIA.COM_**" seguito dalla cifratura del nome originale con l'algoritmo **AES 256.**
Per conoscere il riscatto richiesto è necessario inviare un email a: unCrypte@INDIA.COM
Il riscatto richiesto da **Trojan.Win32.Renamer** è di 0,5 BTC.
Fortunatamente è possibile recuperare i file che sono stati cifrati riportandoli al loro nome originario senza, necessariamente, dover pagare il riscatto.

A febbraio sono stati segnalati *CryptoFAG*, *GpCode*, *UnLock26*.
Un marzo in frenata con un solo nuovo ransomware segnalato realmente circolante, si tratta del *Revenge*.

I segnali di febbraio e marzo avrebbero potuto lasciar pensare ad un forte rallentamento della diffusione di nuovi ransomware, ma ad aprile vi è una nuova recrudescenza del fenomeno: *WannaCry 1.0*; *CryptoWIRE*; *DoNotChange*; *LambdaLocked*; *Matrix*; *CryptoTrump*; *Serpent*; *CryptoNM4* sono solo alcuni dei nuovi ransomware scoperti. Molti di questi nuovi ransomware sembrano siano stati sviluppati per goliardia, come il *CryptoTrump* ispirato al presidente degli Stati Uniti d'America, ma altri, come WannaCry 1.0, danno inizio ad un nuovo filone di attacco che toccherà il suo apice il 12 maggio.

Il mese di maggio vede consolidarsi il fenomeno ransomware con: *Hermes 2.0*; *GlobeImposter 2.0*; *CryptoXData*; *CryptoMole*; *CryptoPec*; *CryptoMay* e ultimo, ma non ultimo, ***WannaCry 2.0***.

Il vettore d'infezione utilizzato da *GlobeImposter 2.0* nella campagna di maggio è stata la posta elettronica, dove il messaggio infetto conteneva in allegato un file zip con all'interno un Javascript con estensione **.js**.
Tale file **.js** ha funzione di dropper e quando viene eseguito, procede a scaricare ed eseguire il payload dal seguente sito: hxxp://pichdollard[.]top/admin[.]php?f=404

Una volta scaricato ed eseguito, il ransomware avvia un processo di cifratura dei file di dati presenti nel PC e nella rete.
Ai file cifrati da GlobeImposter 2.0 viene aggiunta l'estensione ***.crypt***, che avranno quindi la seguente struttura: *<nomefile>.<estensione>****.crypt***
Il riscatto richiesto è di 1 Bitcoin da accreditare sul seguente portafoglio (Wallet):
1FuCGsCmmGWZnDkzg2aa7y6RvK3KP7TG7K

Alla data di venerdì 19 maggio,il wallet dove vengono incassati i riscatti di GlobeImposter 2.0 risulta avere incassato solamente 1 bitcoin.
Dall'analisi del wallet, visti i ridotti incassi, sembrerebbe essere, per ora, un ransomware a bassa diffusione oppure un test per verificare se la metodologia di pagamento è da considerarsi agevole per gli utenti ricattati che volessero pagare il riscatto.

CryptoPEC alias **PEC 2017** è un ransomware che poteva avere un impatto devastante sugli enti/imprese italiani. Anche per il CryptoPEC il vettore d'infezione è stata la posta elettronica attraverso due tipologie distinte di campagne mail, entrambe scritte in un buon italiano. La prima è l'invio di un curriculum da parte di una fantomatica "Nevia Ferrara" che si proponeva come Analista Contabile, qui il target erano gli studi di commercialisti e più

in generale le aziende. Singolare è la mail del mittente: nevia.ferrara(at)agenzia-entrate.com
La seconda, sempre inviata dalla fantomatica "Nevia Ferrara", che intendeva rendere noto ad un Primo Cittadino, la propria denuncia riguardo un dissesto stradale che le ha provocato un incidente. In questo caso il target erano i comuni italiani.

La richiesta di riscatto era di 1 BTC se il pagamento avviene entro 120 ore, raddoppia se fatto successivamente ma non oltre i 30gg.
Tutti i file cifrati vengono rinominati con estensione **.PEC**
Analizzando le mail, gli autori sembrerebbero essere ragionevolmente italiani, anche se i Cyber-ricattatori si appoggiano a server olandesi per la loro infrastruttura e quindi potrebbero anche non essere italiani, ma godere di collaborazioni locali per la corretta redazione delle mail e dei testi delle pagine di richiesta di riscatto.
Le prime segnalazioni di attacchi CryptoPEC sono dei primi giorni di maggio, sebbene come impostazione potesse sembrare un ransomware particolarmente temibile e redditizio per i suoi creatori, il 12 maggio i Cyber-ricattatori danno l'annuncio della chiusura del progetto con il rilascio della Master Key, cioè della chiave di decrittazione universale.
Come già avvenuto per la chiusura del progetto "Tesla" nel maggio 2016 viene da chiedersi il perché di questa decisione… Naturalmente, ancora una volta, ai posteri l'ardua sentenza.

12 maggio 2017 – Attacco mondiale WannaCry 2.0

Venerdì 12 maggio 2017 si diffonde la notizia di un attacco mondiale di un nuovo potentissimo ransomware chiamato **WannaCry 2.0**.
La sua peculiarità di diffusione è che non utilizza un vettore di infezione "classico", come potrebbe essere tramite invio di email o siti infetti, ma sfrutta per la sua diffusione una vulnerabilità dei Sistemi Operativi Windows chiamata ***EternalBlue***.
Se nei precedenti vettori d'infezione giocava un ruolo fondamentale l'utente, ad esempio con l'apertura dell'allegato infetto, con EternalBlue non è necessario l'interazione da parte dell'utente per essere infettato. Ogni computer è potenzialmente attaccabile da un altro PC precedentemente infettato da WannaCry.
La vulnerabilità denominata ***EternalBlue*** è stata resa pubblica dal gruppo hacker **Shadow Brokers il 14** aprile 2017 che avevano "trafugato" questa informazione e l'arsenale di armi cibernetiche "rubandole" nell'agosto 2016 ad un altro gruppo di hacker chiamato **Equation Group,** probabilmente fornitori della **National Security Agency** (NSA) americana.
Il ransomware WannaCry procede a "scandagliare" gli indirizzi IP della rete alla ricerca di computer ove sia presente questa vulnerabilità e quindi procedere ad attaccarli.
Dall'analisi del codice di WannaCry 2.0 si rileva immediatamente la presenza di una funzionalità di Kill Switch che permette ai suoi autori, ma come vedremo anche ad altri, di bloccare l'attacco.
Gli autori di WannaCry hanno inserito un controllo per bloccare la propagazione di questa prima release verificando se è attivo il dominio hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com, e se questo risulta essere online il

ransomware termina senza fare ulteriori operazioni.
Dall'analisi del codice questo controllo sembra essere stato inserito in modo un po' affrettato, quasi "all'ultimo momento" poco prima del suo rilascio, probabilmente per paura delle possibili conseguenze che questo ransomware potesse avere.
Fatto sta, che un ricercatore inglese che si fa chiamare MalwareTech, analizzando il codice è riuscito ad intuirne la presenza e ha ben pensato di registrare il dominio, rallentando l'infezione. Gli autori del ransomware però si sono affrettati a mettere in circolazione release di WannaCry 2.0 senza Kill Switch.
Questo ransomware ha avuto un impatto mediatico a livello mondiale. I mezzi di informazione hanno diffuso notizie quanto mai allarmistiche, dell'ordine di 150 paesi colpiti e oltre 300.000 computer bloccati da WannaCry. Portando alla ribalta un tema troppo spesso trascurato riguardo alla sicurezza informatica dei computer, che inizia dall'aggiornamento dei Sistemi Operativi, infatti per evitare l'infezione sarebbe bastato aver effettuato gli aggiornamenti del S.O. resi disponibili da Microsoft già da oltre un mese.

I guadagni di WannaCry

Sulla base dei dati di diffusione del ransomware segnalati dai mezzi di informazione, incrociandoli con i tre wallet dove vengono indirizzati i pagamenti del riscatto in BitCoin, si evince che al 27 giugno 2017, cioè circa 45 giorni dopo l'inizio dell'attacco, l'incasso complessivo dei malfattori era costituito da 350 transazioni complessive cioè il pagamento di 350 riscatti, per un totale di poco superiore ai 50 BitCoin, che al cambio dell'epoca (2100 USD) corrispondevano a poco più di 122 mila dollari.

L'Impatto di WannaCry 2.0 sull'Italia

La copertura mediatica che questo attacco ha avuto per oltre una settimana, passando ogni giorno la notizia ai telegiornali, come anche a varie trasmissioni di intrattenimento con interviste e opinioni di vari esperti, ha fatto percepire a tutti di poter essere in ogni momento

sotto attacco o poter essere vittime di queste temibile minaccia. Tutto questo ha portato ad aumentare la consapevolezza del pericolo imminente non solo da parte dei tecnici informatici, ma anche dell'opinione pubblica.
L'impatto sull'Italia di WannaCry è stato fortunatamente meno critico di quello che l'opinione pubblica ha percepito probabilmente perché, questo ransomware, non aveva come prioritario l'attacco agli indirizzi IP italiani.

Chi potrebbe esserci dietro a WannaCry

Vi sono varie ipotesi su chi ci sia dietro a WannaCry, taluni dicono che si tratti della Corea del Nord e che dietro ci sia il famigerato gruppo Lazarus, quindi WannaCry 2.0 sarebbe da considerarsi un ransomware / malware di stato.
Si potrebbe anche ipotizzare che il gruppo Shadow Brokers abbia ritenuto opportuno dare una prova di efficacia delle tecnologie trafugate ad Equation Group facenti parte dell'arsenale delle armi cibernetiche di NSA, per dimostrare a potenziali interessati l'efficacia di questi codici e incrementarne il prezzo.
Viste le cifre ottenute con i riscatti pagati per attacchi da WannaCry 2.0 dell'ordine dei 120.000,00 USD al 27 giugno si ritiene di poter escludere che l'obiettivo possa essere quello di fare guadagni con i riscatti.
Anche in questo caso ai posteri l'ardua sentenza…

Non ha fatto in tempo a placarsi l'interesse mediatico su WannaCry che a giugno 2017 si scatena un attacco di NotPetya/Eternal Petya un ransomware / wiper simile alle creazioni di Janus nello specifico a Petya GoldenEye.

27 giugno NotPetya alias Eternal Petya

Martedì 27 giugno si scatena l'attacco di un altro ransomware che è fortemente somigliante a ***Petya***, in particolar modo alla versione Petya GoldenEye 4.0, che va a cifrare la Master File Table (MFT) dei dischi fissi. Anche in questa occasione viene sfruttata la vulnerabilità Eternal Blue che permettere la diffusione del malware/ransomware senza interazione con l'utente procedendo a "scandagliare" gli indirizzi IP della rete alla ricerca di computer ove sia presente questa vulnerabilità e quindi procede ad attaccarli infettandoli.
Questa release di Petya procede a cifrare la MFT con chiave generata dall'algoritmo SALSA20 mentre la cifratura dei file avviene con l'algoritmo AES.
Il riscatto è di 300 $ in BitCoin:

- i file cifrati possono essere recuperati pagando il riscatto;
- la MFT è cifrata con una chiave casuale non collegata al'ID della vittima che non ne permette il recupero anche pagando il riscatto.

NotPetya/Eternal Petya è Ransomware o Wiper ?

Questo malware è molto simile a ***Petya GoldenEye*** di Janus, ma non è una sua variante sebbene i due codici differiscano di soli 43 byte. Gli autori di ***NotPetya/EternalPetya*** han-

no eseguito un "dump" dei settori infetti di **Petya GoldenEye** da un computer infetto. Il codice di Petya GoldenEye a livello di settori è stato modificato con un hexeditor e inglobato nel progetto ***NotPetya/EternalPetya***. Come detto i due codici differiscono per qualche decina di byte, 43 per l'esattezza, ad esempio in NotPetya/EternalPetya è stata eliminata la visualizzazione del teschio della morte, che invece contraddistingue tutte le versioni di Petya realizzate da Janus. L'inglobazione del "dump" di Petya in NotPetya/EternalPetya, non ha permesso di gestire in modo corretto le generazione della chiave per cifrare l'MFT con il "core" di Petya GoldenEye e il corrispondente ID per la sua decifratura. Per questo motivo vi è l'impossibilità di decifrare l'MFT anche pagando il riscatto, molti ricercatori hanno quindi ipotizzato che si tratti invece di un wiper e non di ransomware. Janus, l'autore del codice originale del ransomware Petya, si è trovato, suo malgrado, coinvolto in questo attacco mondiale.

Lo stesso Janus dai suoi account twitter ha smentito che si tratti di una sua creazione e, forse sentendosi indirettamente responsabile dei danni prodotti, con l'intento di aiutare le vittime, ha rilasciato la Master Key di tutte le versioni di Petya, nella speranza che possa essere utile per la decifratura dell'MFT.

Purtroppo la Master Key rilasciata da Janus non è utile allo scopo.

Chi era l'obiettivo dell'attacco

Supermercato in Ucraina bloccato da NotPetya/EternalPetya

NotPetya si è diffuso principalmente in Ucraina e in alcune nazioni baltiche, fortunatamente l'obiettivo primario, come per WannaCry, non è stata l'Italia poiché in particolare per NotPetya non c'è la possibilità di recuperare la MFT.

Alcuni analisti ritengono che questo attacco sia opera dei famigerati hacker russi e che sia stato architettato/commissionato dalla Russia. Da cui si ritiene che l'impossibilità di decifrare l'MFT anche da parte dei Cyber-ricattori non sia un errore ma una scelta voluta e, se così fosse, non si dovrebbe più parlare di ransomware ma di wiper cioè di un malware realizzato al solo scopo di danneggiamento.

Di fatto un attacco deliberato alle infrastrutture informatiche ucraine.
Da analisi più approfondite sui vettori di infezione utilizzati, si è scoperto che la prima diffusione di ***NotPetya/EternalPetya*** è avvenuta attraverso l'aggiornamento del software gestionale M.E. Doc. Si è scoperto che il server per l'aggiornamento era stato precedentemente attaccato e che l'upgrade del software gestionale era stato modificato per contenere il dropper di NotPetya/EternalPetya. È interessante notare che nel mese precedente di maggio, lo stesso server per l'aggiornamento del gestionale M.E. Doc aveva distribuito un altro ransomware chiamato CryptoXDATA, noto anche con il nome di AES-NI. Dietro al ransomware CryptoXDATA (alias AES-NI) sembra vi sia un gruppo che si fa chiamare TELEBOTS, il quale potrebbe essere collegato anche agli attacchi di Black Energy alle centrali elettriche in Ucraina.

La risonanza mediatica a livello mondiale data dai media a **NotPetya** e all'impossibilità di poter recuperare i dati ha fortemente rallentato il rilascio di nuovi ransomware poiché i cyber-ricattatori hanno, probabilmente, preferito attendere qualche mese così che non fosse troppo fresco nell'opinione pubblica il ricordo che neanche pagando sarebbe stato possibile recuperare i dati resi inaccessibili dalla cifratura dell'MFT.

A settembre vi è stata la ripresa della produzione anche di nuovi ransomware a livello goliardico è doveroso citare ***NudeRansomware*** che per fornire la chiave di decifratura dei file richiede delle foto nude, almeno dieci, del proprietario del PC maschi o femmine indifferentemente, la *par condicio* prima di tutto!

Bad Rabbit il coniglio cattivo!

A ottobre riceve grande interesse mediatico il ransomware ***Bad Rabbit*** molto simile a NotPetya, poiché non si limita a cifrare i file , ma cifra anche i settori del disco fisso utilizzando un programma opersource chiamato "DiskCryptor". Bad Rabbit utilizza due vettori d'infezione per propagarsi:

- il primo, attraverso la navigazione su siti compromessi, dove viene richiesto di scaricare un finto Flash player;
- il secondo attraverso un attacco brute force delle credenziali attraverso il protocollo Samba per infettare il maggior numero di PC nella rete locale.

Bad Rabbit è simile a NotPetya/EternalPetya, ma oltre a cifrare i file di documento o dati, esso cifra anche i settori del disco fisso attraverso un driver modificato del programma "Disk Cryptor", rendendo inaccessibile il disco.

I Cyber-ricattatori, in questa occasione, nelle istruzioni per il pagamento del riscatto assicurano che la chiave di cifratura è realmente disponibile, naturalmente previo pagamento del riscatto. Vi è il forte sospetto che dietro a Bad Rabbit ci sia ancora il gruppo Telebots, che in questo caso hanno sostituito il problematico "dump" di Petya, con il programma di cifratura dei dischi "Disk Cryptor". In questo caso è però possibile decifrare il disco pagando il riscatto.

A novembre si diffonde anche in Italia ***CryptoScarab*** che si "innesca" tramite l'esecuzione di uno script (.VBS) contenuto in un file archivio (7z nei file analizzati dal CRAM) allegato ad una **falsa mail**.
Le caratteristiche del messaggio che il malcapitato utente riceve, sembrano quelle che si manifestano quando si ricevono delle scansioni di documenti nella casella di posta. Scansioni possibili mediante particolari stampanti multifunzione.

Attacchi Ransomware in Italia su computer reali verificati

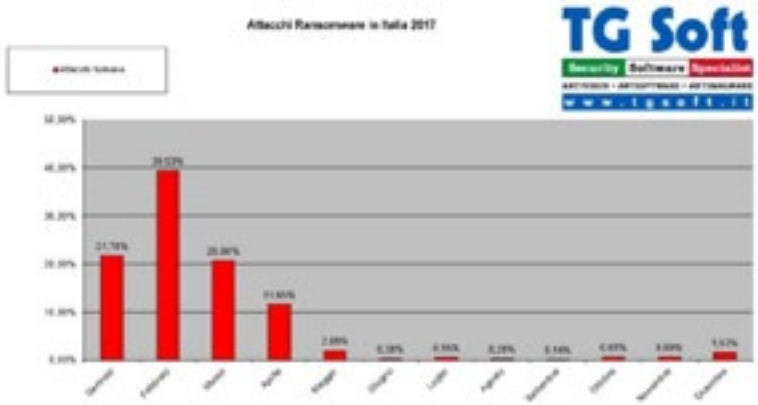
Si può notare che il primo grafico ha visto il picco degli attacchi Ransomware in Italia nel febbraio 2017 con quasi il 40% degli attacchi rispetto al totale dell'anno.

Questi per la maggior parte, sono riconducibili a ransomware persistenti come Cryptolocker. Da maggio queste campagne sembrano, almeno in Italia, essere scomparse o quasi.

Come già segnalato gli attacchi mondiali da WannaCry, NotPetya e BadRabbit, seppur temibilissimi, non trovano particolari riscontri oggettivi in Italia poiché, fortunatamente, il nostro paese non è risultato un obiettivo primario.
Singolare è l'andamento degli attacchi ransomware che tendono a concentrarsi nei primi 4/5 mesi dell'anno da gennaio a aprile/maggio, cosa già osservata nel 2016 e che si è ripetuta anche nel 2017 per poi andare scemando ma procedendo in modo più o meno stabile.
Gli attacchi Ransomware rilevati in Italia riguardano complessivamente 24 famiglie/tipologie distinte. L'ha fatta da padrone, praticamente incontrastato l'arcinoto **CryptoLocker** responsabile di oltre il 76% degli attacchi nell'anno.

Conclusioni

Il 2017 è stato contraddistinto da tre grandi attacchi ransomware a livello mondiale. Nei primi quattro mesi dell'anno era continuato il trend della campagne di ***CryptoLocker***, ***Cerber*** e ***CrySis***, già ben noti dal 2016. Da maggio in poi, queste tipologie di campagne sono scemate, lasciando il posto ad attacchi "spot", come abbiamo visto il 12 maggio WannaCry 2.0, 27 giugno NotPetya e il 24 ottobre Bad Rabbit.
Dall'analisi dei dati delle statistiche, si è notato un calo nelle campagne rispetto al 2016, non solo di quelle note, ma anche nello sviluppo di nuove famiglie di ransomware.



Quali aspettative per il 2018…

I ransomware, è bene ricordarlo, sono dei malware specificatamente progettati a scopo di ricatto e quindi con l'obiettivo del guadagno. Si ritiene che nel 2018 le aspettative dovrebbero far pensare ad una progressiva riduzione degli attacchi ransomware poiché non è irragionevole ipotizzare che alcuni dei Cryber-ricattatori possano valutare di concentrare i loro sforzi, ed alcuni probabilmente lo stanno già facendo, nella produzione e diffusione di malware che sfruttano i processori dei PC / Server colpiti per "minare" crypto-valute (BitCoin ma non solo…).

In questo modo non producono danni devastanti agli utenti infetti ma sfruttano "solamente" le risorse dei processori producendo dei più o meno sensibili rallentamenti dei PC / Server. Già da qualche tempo alcuni siti web sono stati opportunamente modificati sia dai loro proprietari, ma anche all'insaputa di questi, dove le pagine più visitate sono state integrate con dei codici di "mining" in grado di sfruttare le potenzialità di calcolo dei computer che consultano queste pagine per "minare" cripto-valute. Da queste pagine, può accadere che vengano anche rilasciati in modalità, più o meno nascosta, dei codici di "mining" anche sulla macchina locale di modo che l'estrazione di Cripto-Valuta possa continuare anche dopo la chiusura della/e pagina/e Web.

Alcuni elementi sul cybercrime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo e Domenico Raguseo, IBM]

Introduzione

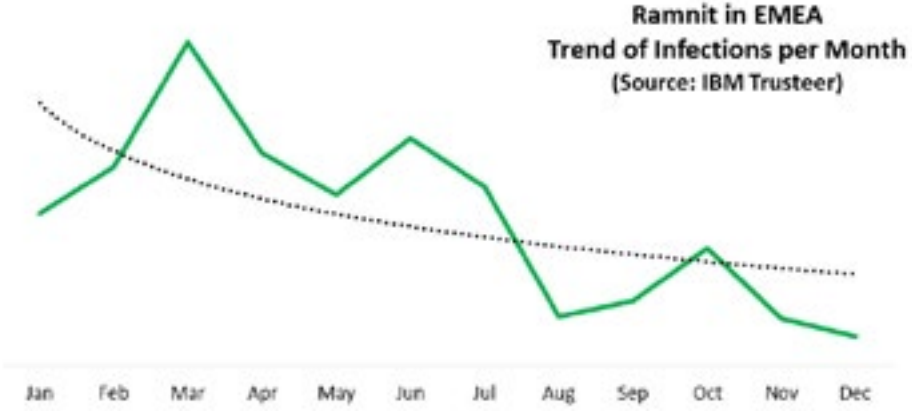
Il cybercrime finanziario ha visto importarti sviluppi nel 2017, con innovazioni nei malware usati per costruire le frodi finanziarie. Il fenomeno dei malware per frodi finanziarie è ormai territorio di gruppi criminali internazionali, ben organizzati e strutturati.
Nell'analisi che segue, IBM presenta e commenta i risultati delle proprie rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2017. Questo lavoro è stato possibile anche grazie ai contributi dei dati del team di ricerca IBM X-Force, le analisi di IBM Trusteer, e al lavoro quotidiano di molti IBMers che gli autori desiderano ringraziare.
Le fonti consultate sono elencate nella bibliografia al termine del capitolo.

Un anno di cybercrime finanziario

Alcuni di noi stavano ancora festeggiando il capodanno del 2017, quando in **Francia** partiva la prima campagna su vasta scala dell'anno, costruita sul malware per dispositivi mobili **Marcher**.
Marcher è un malware per Android, apparso alla fine del 2013, offerto in vendita nei siti underground in lingua russa. Il primo utilizzo degno di nota di Marcher avviene in Germania nel 2014, per poi espandersi in altre nazioni europee, e avere il suo periodo d'oro durante il 2016 in attacchi a banche in Francia, Polonia, e Austria. Nei suoi primi utilizzi, Marcher è stato usato principalmente per rubare dati di carte di credito su dispositivi Android, con una schermata di overlay all'accesso a Google Play che catturava l'inserimento del numero di carta di credito, la scadenza e il codice CVV2.
La campagna verso gli utenti di banche francesi inizia in realtà a fine Dicembre 2016, e raggiunge il suo picco ai primi di Gennaio 2017. Per questa campagna, gli autori specializzano il modulo di SMS hijacking per catturare il secondo fattore di autenticazione inviato dalla banca via SMS. Il malware effettua una data exfiltration inviando agli attaccanti la storia del browser, la lista di contatti e la lista della app installate sul dispositivo, ovviamente alla ricerca di app bancarie o informazioni sulla navigazione su siti di eBanking, e individuare la banca usata dall'utente. Caratteristica unica nel suo genere, Marcher valida in locale le credenziali, inviandole verso il Command and Control server (C&C) solo dopo che l'utente li ha effettivamente usati con successo per effettuare log in. Marcher mostra un numero esiguo di infezioni, ma con una alta percentuale di successo nella frode.

Come vettore di infezione per questa campagna, sono usate mail di phishing che invitano gli utenti a un aggiornamento urgente di Flash Player, con istruzioni dettagliate, e un link per scaricare l'aggiornamento, ovviamente da un sito non ufficiale.

L'aggiornamento trojan, una volta scaricato, chiede però anche l'autorizzazione ad accedere agli SMS, proprio per attivare modulo di SMS hijacking. Una autorizzazione insolita per un lettore multimediale. Questo dettaglio viene però ignorato da molti utenti e l'attacco ha inizio.
Negli stessi giorni, utenti di banche del **Regno Unito** divengono bersaglio di una campagna effettuata con il malware **Ramnit**. La stessa operazione colpisce anche altri istituti finanziari in nazioni di lingua
Inglese, principalmente in Australia e Canada, e si realizza attraverso una campagna di spam. Nel corso di tutto il 2017, Ramnit sarà responsabile di circa una infezione su quattro, attestandosi come uno dei malware finanziari più usato, secondo solo a Dridex.



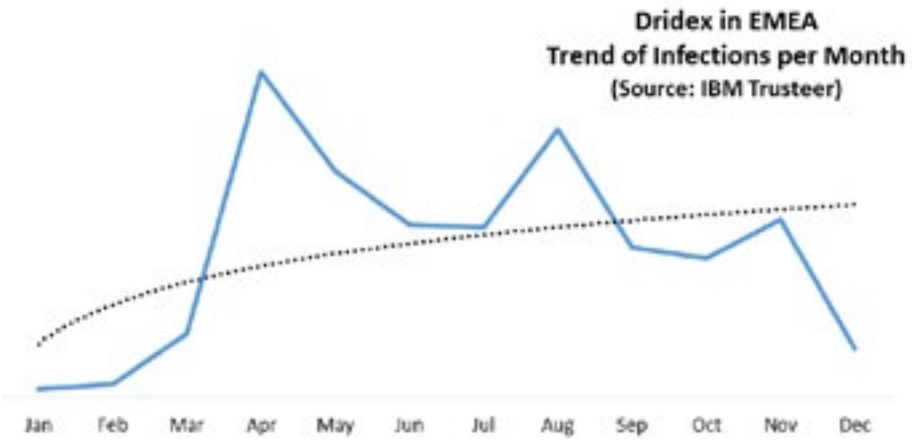
Questa campagna si contraddistingue anche per la ricerca di credenziali di accesso a siti online di ricerca impiego. Questo comportamento si riscontra anche da parte di altri malware durante l'anno. Una possibile spiegazione è nella necessità di arruolare continuamente money mules, gli spalloni digitali disposti a far transitare sui loro conti bancari le somme frodate in cambio di una percentuale, ma a rischio di essere individuati come favoreggiatori delle organizzazioni di cyber criminali.

A **Febbraio**, i ricercatori di IBM Security Trusteer individuano aggiornamenti dei configuration file per il malware **GootKit v2**, con definizioni per oltre venti diverse banche del **Regno Unito**. Una nuova campagna di attacco è alle porte.

Individuato per la prima volta nel 2014, GootKit è considerato uno dei più avanzati banking trojan attivi ed è stato usato principalmente in Europa. Di Gootkit avevamo già parlato nel rapporto CLUSIT del 2017 [1], in quanto era stato uno dei quattro banking trojan a dominare lo scenario del 2016, con il 10% delle infezioni. GootKit infetta il browser della macchina, e funziona con i browser più diffusi, Internet Explorer, Firefox e Chrome.

Novità di questa campagna sono gli aggiornamenti di codice con nuove tecniche di evasione e persistenza, nascondendo copie del malware nel folder dati di Internet Explorer e sfruttando il meccanismo delle Group Policy per girare come task schedulato e reinstallarsi dopo ogni rimozione operata dall'antimalware.
Ancora nel mese di Febbraio, la nuova versione del banking Trojan **Dridex v4** (Dridex conserva il numero di build dentro il codice binario) è la prima a implementare un metodo innovativo di code injection, studiato dai ricercatori della enSilo [2], e battezzato AtomBombing, in quanto sfrutta le atom tables interne di Windows.

I metodi tradizionali per effettuare code injection sono ormai ben conosciuti ai produttori di antimalware e per questo rischiano di perdere di efficacia. AtomBombing sfrutta un meccanismo innovativo che permette a Dridex di propagarsi all'interno del sistema infetto con un ricorso minimo alle API solitamente usate dai malware ed e quindi di più difficile individuazione. [3]
Oltre all'AtomBombing per il code injection, Dridex implementa migliorie nella encryption dei configuration file, nuove tecniche per proteggersi dall'analisi degli eseguibili e altrettanto nuove tecniche di evasione dagli antimalware. [4]
Le campagne analizzate miravano a utenti di istituzioni bancarie in **Francia**, **Regno Unito**, **Irlanda**, e settimane più tardi anche **Germania**. Analizzando l'intero anno 2017, Dridex risulterà il malware per frodi finanziare più presente in Europa, con circa il 28% di tutte le infezioni.

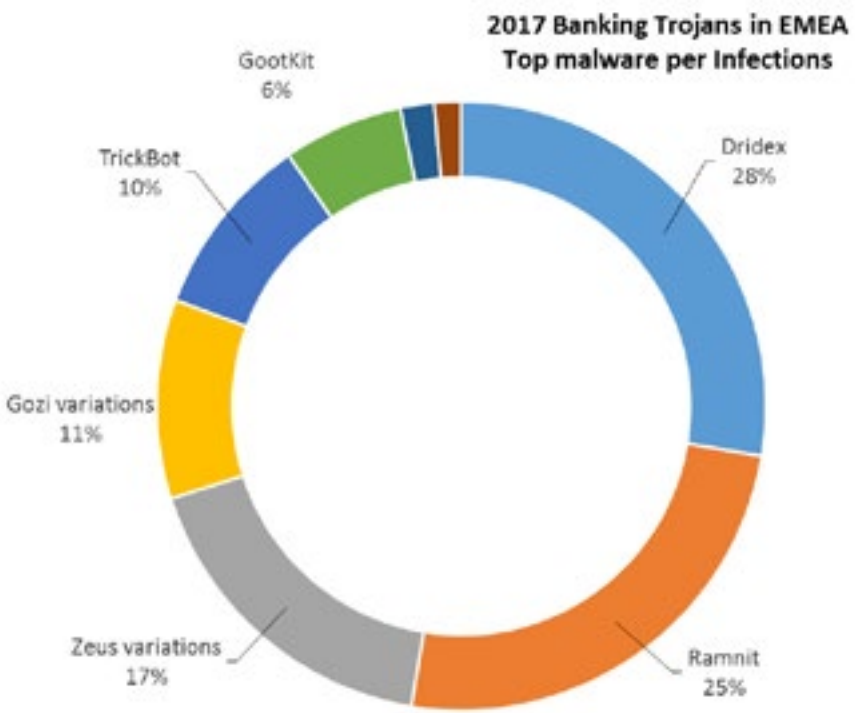


Dridex cresce nel corso del 2017, e durante l'anno implementa sofisticate tattiche di redirection attack.
L'idea alla base dei redirection attack è di dirottare il traffico della vittima verso siti replica, attraverso questi catturare tutte le credenziali di accesso e poi riutilizzare le credenziali per

accedere al vero sito di banking, attraverso un'altra sessione parallela controllata dai cyber criminali. In questo secondo accesso, da parte dei cyber criminali, la precisione è chirurgica, con una percentuale di successo molto alta.
Durante l'intera sessione la vittima è tenuta appositamente lontana dal sito della banca, per portare la vittima a rivelare tutte le informazioni critiche per il log in senza che la banca si accorga che l'account del suo cliente sta per essere compromesso.
Per preparare un tale attacco i cyber criminali creano dapprima un sito replica, molto fedele, della banca. Quanto il sito replica è pronto, il trojan dirotta tutte le richieste HTTP al nuovo indirizzo, senza che l'utente noti nulla di anomalo all'interno del suo browser. L'indirizzo che compare sulla barra del browser è quello corretto del sito di eBanking, ma la connessione sta avvenendo con il sito replica, non quello originale.

Dridex usa la tecnica del DNS poisoning sulla macchina dell'utente per dirottare il traffico di rete verso il sito replica. Nel DNS poisoning l'attaccante inserisce falsi indirizzi nella cache del DNS. Come risultato, tutte le richieste verso gli indirizzi della banca vengono dirottate verso il sito replica e questo per tutte le tipologie di traffico.
Non sospettando nulla, la vittima procede con il log in, che avviene di fatto sul sito replica. Il server della banca non vede nessun log in, non ha informazioni sulla sessione e non può segnalare nulla al proprio cliente.
Dopo l'iniziale autenticazione sul sito replica, i cyber criminali effettuano parallelamente log in sul sito vero della banca, in un'altra sessione contemporanea e distinta dalla prima. Da questo punto in poi, la vittima riceve injection nel suo browser per sollecitare l'inserimento dei secondi fattori di autenticazione (one-time password, PIN dispositivi), sulla base di quanto richiesto dalla reale sessione con la banca. L'Account TakeOver (ATO), o impossessamento dell'account, ha avuto successo, e in assenza di soluzioni specifiche, nulla può fare la banca.

Nuove campagne **GootKit v2** prendono di mira banche del **Regno Unito**, e questa volta in maniera più importante anche siti in **Francia**. Nel primo quadrimestre dell'anno, GootKit è il malware più importante nelle frodi finanziarie francesi, con il 38% di tutte le infezioni.
A Maggio i ricercatori di IBM Trusteer isolano una campagna basata sul **Ramnit**, con obiettivi nel **Regno Unito** e in **Italia**. Questa volta gli operatori di Ramnit usano il RIG Exploit Kit per infettare le macchine degli utenti attraverso campagne di malvertising su siti web compromessi. Il RIG Exploit Kit è considerato l'exploit kit più prolifico in quel momento.
Quasi in contemporanea parte il primo grande attacco con la tecnica dei redirection attacks in **Italia**, basato su **GootKit** distribuito attraverso malvertising. Sei banche italiane sono tra gli obiettivi. [5]
Gli sviluppatori di GootKit usano le tecnica dei redirection attacks quanto più possibile, prima che il mondo bancario e i produttori di soluzioni antimalware riescano a trovare un rimedio. Tra Maggio e Giugno vi sono numerose campagne di attacco e IBM Trusteer ne arriverà a isolare oltre dieci.



A Giugno una campagna basata su **Dridex** colpisce numerose nazioni a livello globale e, seppur marginalmente, anche l'**Italia**.
Ancora una volta, incredibile a dirlo, il malware è veicolato da una mail di phishing, che avvisa l'utente di una fattura non pagata e contenente un PDF infetto. Malgrado questo vettore d'infezione sia ben noto, l'Italia registra circa il 4% delle infezioni. Una percentuale relativamente esigua, ma che la fa risultare comunque la nazione non anglofona con il più alto numero di infezioni. La barriera linguistica che ci ha protetto fino a questo punto, sta per cadere. La campagna di phishing si esaurisce nel giro di circa due settimane, e con essa l'effetto del malware

Anche **TrickBot** implementa il meccanismo dei redirection attacks, ed esordisce con una campagna di attacco in **Spagna**. Le campagne di TrickBot sono quasi sempre molto mirate, e si orientano tutte verso aziende e singoli individui ad alto reddito.
Si sono contate banche colpite in oltre 24 nazioni al mondo, e TrickBot sale velocemente la lista dei malware più efficaci, sin dalla sua creazione nel 2016.

Nel corso del 2017 si piazza come il quinto malware per frodi finanziarie più diffuso in Europa, con poco meno del 10% di tutte le infezioni osservate.
Ad Agosto, una ventina di applicazioni di largo utilizzo, come finti giochi, torce, salva schermo, in apparenza innocue sono in realtà infettate con il banking trojan **BankBot**. [6] E questo dopo che alcune altre centinaia di applicazioni infette dallo stesso malware BankBot erano state individuate e rimosse dal Google Play all'inizio dell'anno. [7] Il trojan BankBot entra sul dispositivo mobile attraverso una applicazione apparentemente innocua, che rimane in esecuzione silenziosa pronta a interferire con il funzionamento delle altre applicazioni installate sullo stesso dispositivo, come le applicazioni per accedere alla banca, catturando le credenziali di accesso, all'insaputa dell'utente e senza alcun segno sul display del dispositivo.

D'improvviso si scopre che uno dei princìpi fin qui adottato, installare solo software da sorgenti autorevoli come appunto il Google Play, potrebbe da solo non essere più sufficiente.

A Settembre una nuova campagna di attacco incentrata sul malware **Sphinx**, una variante di Zeus v2, ha obiettivi principali in **Italia** (con circa il 70% dei target) e in **Spagna**.
Oltre a siti di e-banking, questa campagna ha come target le piattaforme di scambio delle criptomonete. La nuova campagna implementa importanti novità nel codice di Sphinx. Supporto Tor e comunicazione con i server di C&C più robusta e resiliente, offuscamento dell'eseguibile, e tecniche anti-VM per evadere dalle piattaforme di analisi automatica.

Panda Banker irrompe in **Italia** alla fine di Settembre, con una massiccia attività di spamming che raccoglie migliaia di vittime su tutto il territorio nazionale. [8] Panda è un malware di derivazione Zeus che cattura codici di accesso a siti bancari, oltre che webmail e social network.
Anche in questo caso, la campagna di spamming avviene attraverso l'invio di email apparentemente originate da aziende di recapito, contenenti allegati compromessi, aperti ed eseguiti dalle vittime, incuranti delle più elementari norme di precauzione che da più parti vengono ormai sistematicamente raccomandate. Nella parte finale della campagna, gli operatori di Panda sfruttano anche il RIG Exploit Kit per distribuire il malware.

L'anno si chiude con altre due importanti campagne. La prima, a Ottobre, costruita attorno al **GootKit v2**, verso banche di **Francia**, **Italia** e **Regno Unito**. La campagna sfrutta web injection verso le banche francesi, e redirection attack nella componente Italiana e Britannica.
La seconda campagna è invece costruita attorno al malware Ramnit e con obiettivo un esiguo numero di banche in Italia e Regno Unito, oltre che in altri paesi extra europei.
Malgrado il numero limitato di obiettivi, la nuova campagna di Ramnit mostra importanti migliorie di codice. Un dropper scarica sull'endpoint il package criptato contenente all'interno l'eseguibile di Ramnit. Il dropper decripta il Ramnit in memoria e lo inietta all'interno

del Media Player, come tecnica di evasione. Da questo guscio protettivo, Ramnit scarica i suoi plug-in dal server di Command and Control, esegue i moduli delegati al meccanismo di web-injection, web filtering, dirottamento delle richieste al DNS, gestione dei cookie, e altre componenti di supporto.
Ramnit concluderà il 2017 come il malware con il maggior numero di singole configurazioni distribuite agli endpoint compromessi nel corso dell'anno. Da solo Ramnit totalizza il triplo delle configurazioni dei 3 malware finanziari che lo seguono. Malgrado questa prolificità, Ramnit sarà uno dei malware che perderà costantemente di efficacia durante l'anno, grazie al lavoro dei team di analisi e all'efficacia delle soluzioni di advanced fraud protection che bene sono riusciti a identificare e prevenire le frodi.

Cosa aspettarci per il prossimo futuro

Da qualche anno il terreno delle frodi finanziare è uscito dal raggio d'azione dell'hacker solitario per diventare territorio di gruppi criminali ben organizzati e strutturati. Affinché una frode produca un ritorno economico servono una serie di elementi. Anzitutto la capacità tecnologica di costruire e mantenere un malware di alto livello, poi servono le competenze tecniche per aggiornarlo ogni qualvolta il malware viene identificato dai prodotti di advanced fraud protection già esistenti. Anche la rete di Command and Control (C&C) richiede mantenimento, assieme alle componenti di anonimizzazione del traffico e di encryption. Gli attacchi richiedono poi la conoscenza accurata dell'interfaccia o della applicazione di eBanking e una localizzazione perfetta nelle lingue del soggetto attaccato. Infine, per ogni attacco che ha successo, occorre una rete di spalloni digitali o money mules che facciano fluire la somma frodata di conto in conto, fino a farne perdere le tracce.

Sulla scorta di quanto fin qui delineato, e quanto osservato negli ultimi mesi del 2017, l'anno 2018 vedrà un'ulteriore polarizzazione verso malware controllati da gruppi di cyber criminali di élite, con collegamenti internazionali, continuo incremento della complessità, componentizzazione e riuso del codice e ulteriore spostamento del malware verso i dispositivi mobili.
Le tattiche di redirection attack, implementate fin'ora solo da alcuni malware, saranno gradualmente adottate da tutti i principali malware, sulla scorta di una percentuale di successo molto alta e della difficoltà intrinseca da parte dalla banca di proteggere l'accesso all'account del proprio cliente, con la banca totalmente all'oscuro della transazione compromessa. Promettenti sono le soluzioni per la protezione dell'Account TakeOver (ATO) che combinano diversi indicatori di rischio, come il rilevamento dello spoofing del dispositivo, gli elenchi di dispositivi noti per essere stati usati da gang cyber criminali, e la User Behaviour Analysis, riuscendo a identificare la sessione sospetta prima che avvenga la transazione.

È indubbio che qualsiasi sia la soluzione messa in campo dalla banca, questa deve essere supportata da continua osservazione e ricerca dell'evoluzione delle tattiche di attacco.

In un contesto mutevole come quello descritto, una soluzione non supportata da team di ricerca specializzati nell'analisi del malware, rischia di divenire presto obsoleta e inefficacie. La crescente importanza del ruolo dei money mules è suggerita proprio dai malware analizzati, molti dei quali combinano la cattura di credenziali di accesso a siti di ricerca lavoro, alla frode finanziaria informatica. La campagna Ramnit di Gennaio 2017 mira, in parallelo, anche a credenziali di accesso a siti online di ricerca impiego.

Chi cerca lavoro, e lo fa attraverso i canali digitali, è al tempo stesso tecnologicamente evoluto e interessato al denaro, quindi un buon candidato per essere assoldato nel grande esercito di coloro che contribuiscono, più o meno consapevolmente, a far perdere le tracce di quanto sottratto, dietro ricompensa. A Novembre 2016, Europol, Eurojust, Federazione Bancaria Europea (EBF), e 106 banche, collaborano ad un'operazione che porta all'arresto di 178 persone [9] e all'identificazione di 580 money mules in tutta Europa. Si stima che il volume di affari delle persone coinvolte nell'operazione sia stato di 23 milioni di Euro, il 95% del quale direttamente collegato a qualche forma di cybercrime.
Anche la campagna Ramnit che colpisce l'Italia nell'Ottobre 2017 ha come obiettivo secondario l'individuazione di candidati money mules. Oltre alle banche, gli operatori di Ramnit inseriscono come target nei configuration file le URL di accesso a siti di ricerca lavoro in Gran Bretagna, Australia e Francia.

Ramnit non è l'unico malware a fare scouting di money mules. La campagna TrickBot di Ottobre prende di mira banche in oltre 40 nazioni diverse, ma anche credenziali di accesso a Salesforce e alcuni tra i più autorevoli siti di ricerca personale di Stati Uniti e Canada.
A Novembre 2017 la Polizia di Stato contribuisce per l'Italia a una campagna coordinata da Europol [10], per l'individuazione dei money mules destinatari di somme provenienti da frodi informatiche e campagne di phishing. Durante l'operazione vengono identificati 37 mules operanti in Italia, di questi 32 sono arrestati e 5 denunciati. Sul territorio nazionale le transazioni fraudolente sono state 32, per oltre 150.000 euro, e una media di oltre 4000 euro a soggetto identificato.

La crescita di valore del bitcoin che nella fine del 2017 ha toccato il suo picco massimo in oltre 19000 dollari e una rivalutazione nel corso dell'anno di oltre il 1000%, non è passata inosservata alle bande di cyber criminali.
A Settembre 2017, una campagna basata sul malware Gozi colpisce molte banche a livello mondiale. La campagna ha come target anche alcune piattaforme di scambio di criptovalute operanti in Asia, come BitFlyer, Blockchain.info, CoinCheck, e GMO-Z.
Nello stesso mese, il team di ricerca IBM Trusteer riporta di una campagna di attacco contro Italia (con circa il 70% dei target), e Spagna. Questa volta il malware utilizzato è Sphinx, una variante di Zeus v2.
Parallelamente ai classici obiettivi bancari, questa campagna associa la ricerca di credenziali di accesso a piattaforme di scambio di criptovalute.

In termini assoluti le attività verso le criptovalute è esigua, e conta solo per il 3%, ma è indubbiamente il segno di un cambiamento, anche in Italia.
Le notizie che arrivano dall'inizio 2018 non fanno che confermare questo fenomeno, come uno dei trend che ci accompagnerà nel corso dell'anno.

Indubbiamente l'intelligenza artificiale e le capacità cognitive delle singole soluzioni saranno leve importanti nel campo della lotta al cybercrime nel settore finanziario.
L'uso dell'intelligenza artificiale nelle soluzioni di sicurezza offerte sul mercato si sta orientando su tre macro aree. Anzitutto nell'analisi predittiva con sistemi in grado di identificare autonomamente nuove frodi, e che individuano i falsi positivi.
C'à poi l'area della intelligence consolidation, che sfrutta le capacità di interpretazione del linguaggio naturale, analizzando e apprendendo dall'enorme quantità di informazioni, per lo più in forma non strutturata e prodotte continuamente nel campo della sicurezza. Security bulletins, report, grafici, conferenze, notizie di agenzia, tweet, advisories e altre fonti, che altrimenti rischierebbero di finire ignorate in quanto non fruibili dalle soluzioni di sicurezza finora usate.

Infine, l'intelligenza artificiale si pone come trusted advisor a supporto del lavoro degli analisti umani, per una più veloce risposta alle minacce e agli attacchi. Non quindi una tecnologia che sostituisce il security analyst, ma piuttosto una tecnologia a supporto del security analyst, di cui incrementa sensibilmente la produttività.
La chiave di tutto è che capacità di intelligenza artificiale e capacità cognitive siano infuse all'interno delle soluzioni, uscendo dai laboratori e dai centri di ricerca per divenire fruibili e alla portata di tutti gli utilizzatori.
Molte frodi qui discusse mirano a impossessarsi della nostra identità digitale. Un'auspicabile evoluzione dei meccanismi di accesso ai servizi finanziari, deve avvalersi delle costanti migliorie nei meccanismi per autenticare la nostre identità online.
Un recente studio sul futuro dell'identità [11] delinea l'evoluzione dei metodi per validare le identità online.
L'autenticazione biometrica è sicuramente il futuro prossimo, ma non senza qualche preoccupazione relativamente alla sicurezza. Nello studio si evidenzia come l'impronta digitale sia la forma di autenticazione percepita come più sicura (44% dei rispondenti), decisamente più avanti di tutti i metodi non biometrici, e molto avanti anche al riconoscimento facciale sul quale si sono sfidati i produttori di dispositivi mobili.
L'autenticazione biometrica è già usata dal 67% dei partecipanti al survey, con un 87% che ne considera l'adozione nel futuro. Permangono tuttavia riserve su come i dati biometrici sono conservati e usati. Siccome la biometria può essere usata per identificare un individuo al di sopra di ogni dubbio, e i fattori biometrici sono impossibili da revocare se compromessi, le principali preoccupazioni sono sulla conservazione e l'uso dei fattori biometrici (55%), e l'uso di fattori biometrici artefatti per l'accesso fraudolento alle informazioni personali (50%).

Relativamente alla fiducia dei differenti erogatori di servizio nell'uso della biometria come parte del processo di autenticazione, le istituzioni finanziarie primarie sono quelle considerate più affidabili, mentre i social media sono quelli considerati meno affidabili. Questo stride con la tendenza corrente che vede molti servizi poggiarsi proprio sui social media per l'autenticazione e l'accesso alle applicazioni. Sono poi gli stessi utenti a confessare che nell'accesso ai social media il fattore più importante è la convenienza o comodità, seguito da sicurezza e privacy.

L'autenticazione biometrica è spesso offerta come un'opzione dal fornitore di servizi, la cui adozione è lasciata alla scelta dell'utente finale. Solitamente gli utenti scelgono il metodo di autenticazione che li mette più a proprio agio. Offrire una scelta tra metodi di autenticazione alternativi può essere una delle chiavi all'adozione, e può rispondere alle diverse percezioni generazionali, culturali e geografiche degli utenti.
La ricerca e le soluzioni di User Behavior Analytics (UBA) [12] identificano le attività potenzialmente fraudolente e realizzate da sistemi di hacking automatico, analizzando sequenze di attività anomale che un umano non potrebbe realizzare e sfruttando informazioni che la rete già contiene ma che venivano finora ignorate.

In un contesto così variegato, saranno di ausilio le soluzioni di risk-based authentication, le quali valutano dati contestuali e comportamentali per attribuire un livello di rischio a ciascuna transazione, sia essa un semplice log in piuttosto che un'operazione dispositiva. Quando il livello di rischio è elevato, il fornitore di servizi può richiedere all'utente fattori addizionali di autenticazione a verifica della reale identità.
La ricerca futura sui pattern di adozione e di abuso dei meccanismi di autenticazione rappresenta un punto sostanziale per la costruzione di tecnologia pragmatica e costruita attorno all'utente.

Bibliografia

[1] AA. VV. *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia* - CLUSIT, Marzo 2017
[2] T. Liberman *AtomBombing: A Code Injection that Bypasses Current Security Solutions* - enSilo, Ottobre 2016
[3] M. Baz, O. Safran *Dridex's Cold War: Enter AtomBombing* - SecurityIntelligence.com, Febbraio 2017 - https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
[4] *Dridex v4 - Major version upgrade released* – IBM X-Force Exchange, Febbraio 2017 - https://exchange.xforce.ibmcloud.com/collection/26fdea1e8cc69f52a551e8d451f80aa1
[5] L. Kessem *GootKit Malvertising Brings Redirection Attacks to Italian Banks* - SecurityIntelligence.com, Maggio 2017 - https://securityintelligence.com/gootkit-malvertising- brings-redirection-attacks-to-italian-banks/
[6] L. Kessem, S. Gritzman *After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play* - SecurityIntelligence.com, Maggio 2017 - https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/
[7] E. Tara *Hundreds of Google Play Apps Infected with the BankBot Trojan* – Infosecurity Magazine, Aprile 2017
[8] *Panda Banker collection* - IBM X-Force Exchange, Ottobre 2017 - https://exchange.xforce.ibmcloud.com
[9] *Internet Organized Crime Threat Assessment - IOCTA 2017* - European Union Agency for Law Enforcement Cooperation (Europol), 2017
[10] *Operazione EMMA*3 - Commissariato di P.S. online, Novembre 2017 - http://www.commissariatodips.it/notizie/articolo/operazione-emma3.html
[11] *IBM Future of Identity Study IBM Security, January 2018* - ibm.biz/FutureOfIdentity
[12] T. Obremski *Deep Network Insights for Deeper Analytics* SecurityIntelligence.com, December 2017 - https://securityintelligence.com/take-a-dive-deep-network-insights-for-deeper-analytics/
[13] S. Morgan *Cyber Crime Costs Projected To Reach $2 Trillion by 2019* Forbes, Gennaio 2016 - https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2- trillion-by-2019/
[14] C. Barlow *New Year, New Threats: Five Security Predictions That Will Take Hold in 2018* SecurityIntelligence.com, December 2017 - https://securityintelligence.com/new-year-new-threats- five-security-predictions-that-will-take-hold-in-2018/
[15] L. Kessem *New Discoveries in Cybercrime: 2017 Year in Review* SecurityIntelligence.com, Dicembre 2017 - https://securityintelligence.com/events/new-discoveries-in-cybercrime-2017-a- year-in-review/

Analisi del cyber-crime in Italia in ambito finanziario nel 2017

[A cura di Andrea Granata, Communication Valley Reply]

Nell'anno 2017, confermando il trend già registrato nel 2016, le attività legate al Cyber Crime in ambito finanziario si sono rivelate in espansione sia per quanto riguarda l'ambito globale che per quello italiano. I dati che seguono sono il frutto del monitoraggio, da parte del Cyber Security Command Center (CSCC) di Communication Valley Reply, dei fenomeni fraudolenti che abbiamo dovuto gestire per conto di alcune delle principali realtà bancarie italiane.

Gli attacchi osservati possono essere suddivisi nelle seguenti macro categorie:
- Attacchi di Ingegneria Sociale (Phishing)
- Attacchi tramite malware

Il vettore principale che i cyber-criminali utilizzano per compromettere gli utenti è quello della posta elettronica, confermando anche in questo aspetto la tendenza rilevata nei precedenti anni. Benché la tecnica in sé rimanga sempre la stessa, a diventare più sofisticate sono però le strategie di evasione di filtri antispam e antivirus, tramite le quali i cyber-attacchi riescono ad essere veicolati attraverso e-mail con messaggi che, in alcuni casi, risultano perfettamente identici a messaggi leciti che l'utente si aspetta di ricevere.

Attacchi di ingegneria sociale (Phishing)

Analisi e diffusione del fenomeno

Il Phishing [1] è un fenomeno che attraverso tecniche di Ingegneria Sociale (Social Engineering), quindi imitando per aspetto e contenuti messaggi legittimi di fornitori di servizi, richiede di fornire informazioni riservate come il numero della carta di credito o le credenziali d'accesso. Il livello di verosimiglianza dei messaggi che vengono inviati è così elevato che sta diventando sempre più difficile per l'utente medio notare la differenza tra le mail mandate in una campagna di Phishing e le e-mail inviate legittimamente dai comuni servizi on-line.

Dagli studi condotti durante l'anno 2017 [2] è stato possibile ricavare quali sono stati i principali Paesi d'origine dei flussi di spam attraverso l'analisi degli header SMTP. La distribuzione statistica dei dati riscontrati è delineata in Figura 1.

Presentiamo anche un andamento per quanto riguarda uno degli argomenti di maggiore rilievo anche dal punto di vista mediatico per quanto riguarda il 2017: il tema è quello del ransomware e di due delle famiglie di maggiore impatto durante il 2017, ovvero Wannacry e Locky. In particolare Wannacry ha avuto forte impatto perché insieme

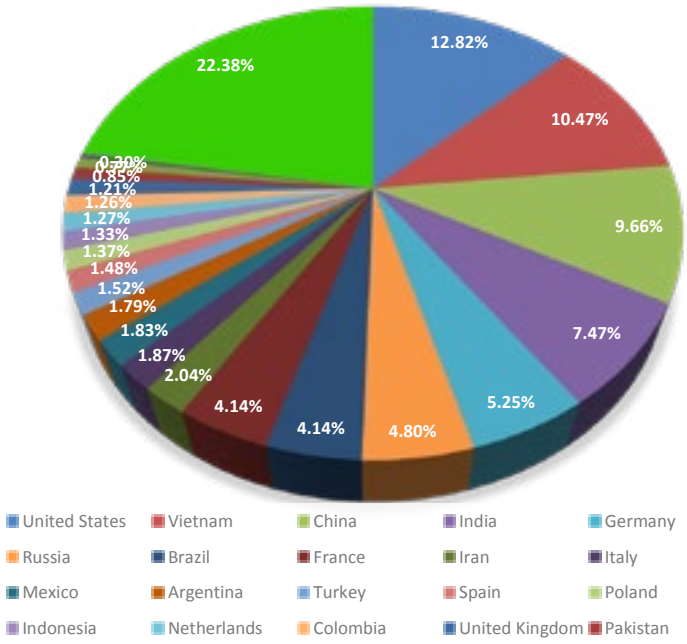


Figura 1 - *Distribuzione dei flussi di spam, suddivisi per Paese di origine*

Dalle statistiche emerge che gli Stati Uniti risultano come prima fonte delle mail di spam, con un 12.82%, seguiti da vicino da tre Paesi orientali: Vietnam (10.47%), Cina (9.66%) e India (7.47%). La Germania è il primo Paese nell'Unione Europea per numero di mail sospette e si attesta al quinto posto con un 5.25%.
Questa distribuzione evidenzia come, rispetto al 2016, ci sia stata una netta diminuzione del traffico proveniente sia dagli Stati Uniti che dalla Cina: in entrambi i casi il traffico risulta infatti praticamente dimezzato. Al contrario, il Vietnam, che il precedente anno non presentava dati significativi, nel 2017 è balzato al secondo posto, mentre l'India è passata da 4% a 9.66%. È anche interessante notare che i Paesi che si trovano nella Top 10 sono responsabili dell'invio di poco più del 60% delle mail malevole.

Per quanto riguarda il panorama italiano, il nostro Paese si trova all'ultimo posto nella Top 10, totalizzando l'1.87% del traffico totale.

Se si prende in considerazione invece il contesto che l'e-mail intende sfruttare per aggirare il malcapitato utente, la distribuzione risultante è quella in Figura 2. Essendo il campo potenzialmente più remunerativo, quello finanziario continua ad essere il principale target con un quarto del totale delle mail inviate; tuttavia stanno emergendo altri settori che vedono

la relativa percentuale di attacchi salire di anno in anno, in particolare si segnalano quelli relativi all'Hosting, ai servizi di pagamento con carte di credito e ai servizi di e-commerce. Più marginali invece sono le percentuali per quelli a tema Social Network, probabilmente perché meno interessanti dal punto di vista lucrativo, e per quelli mirati a colpire entità governative. In quest'ultimo caso i temi dell'attivismo politico sono solitamente prevalenti rispetto agli aspetti economici, in controtendenza rispetto alla maggioranza delle mail di Phishing che vedono nel guadagno economico uno dei principali moventi.

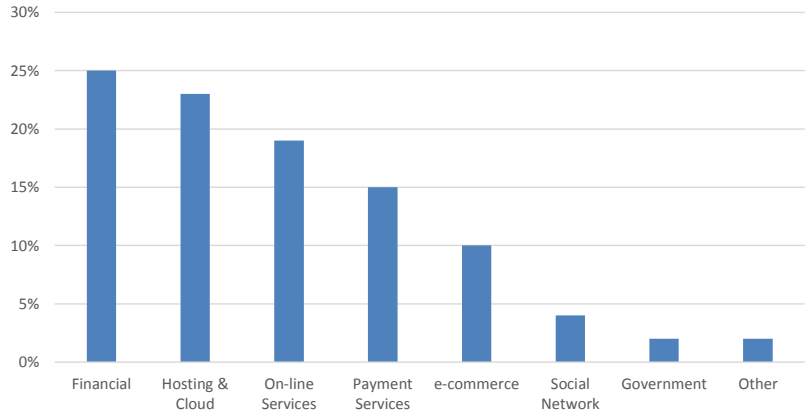


Figura 2 - *Distribuzione delle mail di Phishing, suddivise per tematica trattata*

Le principali campagne di Phishing rilevate

Gli esempi pratici di analisi di campagne di Phishing che sono presentati in questa sezione illustrano le due strategie maggiormente utilizzate nel corso del 2017 e riguardano campagne ancora in corso al momento della stesura del presente documento. L'ampia diffusione e gli effetti decisamente negativi che si ripercuotono sull'utente che ne cade vittima, rendono queste campagne particolarmente aggressive ed insidiose.

Nei casi presentati lo scopo finale e quello di prendere il controllo del computer dell'utente vittima attraverso l'uso di un malware, un programma informatico usato dai cyber-criminali solitamente per entrare in possesso di informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata. La compromissione dell'utente inizia con l'arrivo di un'e-mail in cui a seconda delle situazioni:

- si richiede all'utente di cliccare su un link;
- si allega un file che l'utente non rileva come sospetto e viene pertanto scaricato ed esaminato.

Un esempio di mail riconducibile al primo caso è quello rappresentato, opportunamente

anonimizzato, in **Figura 3**. Si può notare che la mail prende di mira utenti italiani e si presenta come un tentativo che ha come obiettivo quello di ingannare l'utente facendo in modo che clicchi su uno degli hyperlink evidenziati nei rettangoli rossi. I pretesti che vengono utilizzati sono i seguenti.

- La mail risulta proveniente da un fantomatico e generico "Gruppo Assicurativo".
- L'oggetto della mail fa riferimento alla copia di un documento.
- Vengono presentati due link che l'utente dovrebbe seguire per scaricare, appunto, la copia di un'assicurazione sulla vita a cui si accenna nel testo della mail.

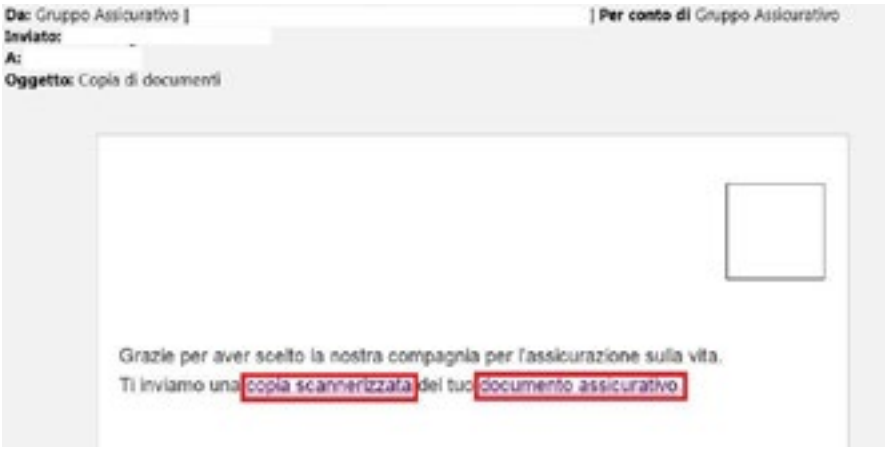


Figura 3 - *Esempio di mail, opportunamente anonimizzata, relativa ad una campagna di Phishing condotta attraverso link malevoli*

Nel momento in cui l'utente procede a cliccare su uno dei link si scatenano le seguenti azioni.

- Il browser che l'utente utilizza per navigare abitualmente su Internet visita le pagine web a cui puntano i link.
- In realtà questi link puntano a risorse su un server compromesso.
- Il browser scarica queste risorse: si tratta di un file JavaScript, contenente istruzioni che il browser è in grado di eseguire.
- Il browser esegue il file che ha scaricato: le istruzioni contenute fanno in modo che il browser si connetta ad un ulteriore sito Internet per scaricare un'altra risorsa.
- La nuova risorsa viene scaricata: il suo nome è "connection.jpg.exe".

A questo punto, sfruttando il fatto che i sistemi Windows per impostazione di default non visualizzano l'estensione del file, in questo caso il ".exe", il nome della risorsa viene visto

come "connection.jpg": pertanto tale risorsa sembrerebbe un comune file immagine. L'utente apre il file, credendo che si tratti della scansione dell'assicurazione, ma invece di visualizzare un'immagine ha appena avviato un malware che permetterà ai criminali informatici di entrare in possesso di informazioni sensibili.

Nel secondo caso la mail di Phishing non contiene link, ma possiede un allegato, come mostrato in **Figura 4**. Si tratta di un documento Excel che, se aperto, ha l'aspetto di una fattura (Figura 5). La peculiarità consiste nella richiesta fatta all'utente di fare clic su "ATTIVA CONTENUTO", ovvero "Enable Content" nel foglio Excel in immagine.

Figura 4 - *Esempio di mail di Phishing, opportunamente anonimizzata, relativa a una campagna di Phishing condotta attraverso file allegato*

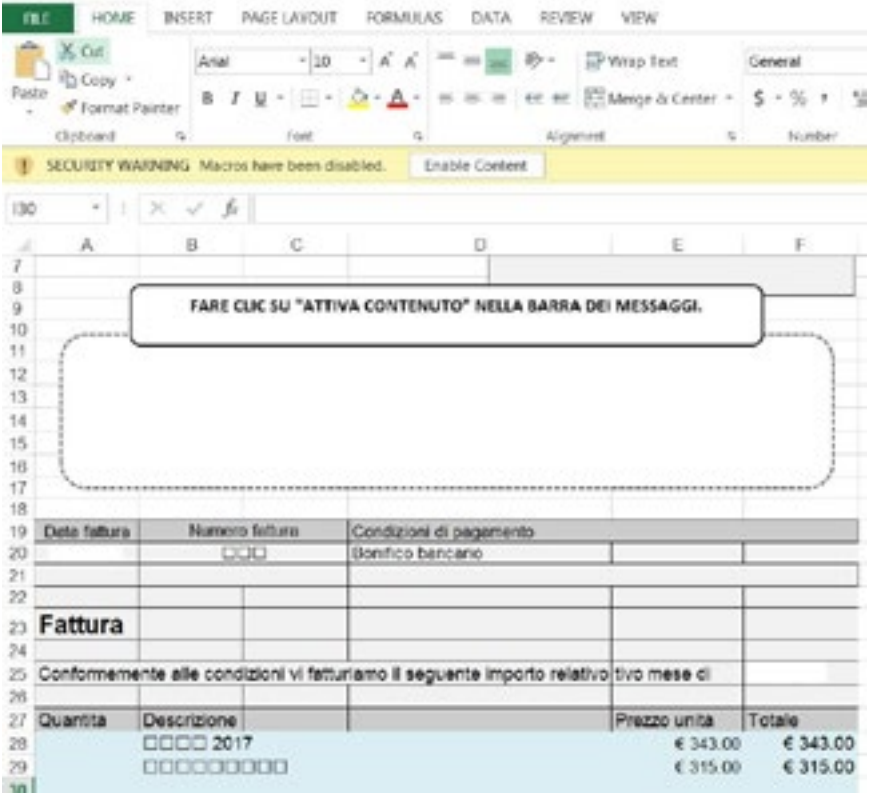


Figura 5 - *File Excel allegato alla mail di Phishing, con invito all'utente per l'abilitazione dei contenuti*

Nel momento in cui l'utente abilita i contenuti si scatenano diverse azioni.

- Vengono abilitate ed immediatamente eseguite le macro di Office configurate nel foglio elettronico. Normalmente, la macro è una metodologia che viene utilizzata per eseguire in modo automatico azioni ripetitive durante la stesura di un documento.
- La macro in questione, tuttavia, effettua una connessione ad un server remoto compromesso o comunque sotto il controllo dei cyber-criminali.
- Durante la connessione viene scaricato un file eseguibile che viene poi lanciato, sempre dalla macro, attraverso l'uso di PowerShell, uno strumento di sistema presente su Windows e che consente l'avvio di file eseguibili.
- Il file scaricato non è altro che un malware, che risulta a questo punto in esecuzione.

Dalle analisi condotte, il malware utilizzato risulta un esemplare della famiglia dei cosiddet-

ti "Panda Banker", anche noto come "Zeus Panda" [3]. Gli utenti che vengono infettati da questa tipologia di malware solitamente non si accorgono di esserlo in quanto non riscontrano alcuna anomalia nel normale funzionamento del proprio PC. In realtà, il malware resta in attesa che l'utente visiti particolari siti Internet (solitamente quelli relativi agli Internet Banking degli istituti bancari) e si attiva solo in questo caso, raccogliendo informazioni sensibili come le credenziali d'accesso per poi inviarle in remoto ai cyber-criminali.

Attacchi tramite malware

Metodi di diffusione e attacco

Come analizzato nella sezione sul Phishing, le e-mail costituiscono il mezzo di diffusione principale dei malware. Questa strategia si spiega con il fatto che è necessario fornire un contesto credibile che riesca a convincere l'utente ad eseguire sul proprio dispositivo software malevolo. Alle tecniche di Phishing e Social Engineering vanno aggiunte quelle di *evasion*: gli autori di malware le utilizzano per fare in modo che il software da loro prodotto non venga considerato sospetto dall'utente e da programmi antivirus possono essere molteplici.

Descriviamo di seguito le strategie di evasion individuate fra i sample analizzati nel corso del 2017 in riferimento all'ambito bancario italiano.

- **Utilizzo di macro** – Una macro è una procedura costituita da un insieme di comandi o istruzioni che si ripetono di frequente durante l'esecuzione di un programma. Sono di uso comune all'interno di elaboratori di testo e fogli di calcolo elettronici, dove servono per automatizzare e rendere più veloci attività che risulterebbero altrimenti ripetitive. Nell'ambito della distribuzione dei malware le macro possono essere utilizzate per scaricare ed eseguire software malevolo sul dispositivo da infettare, senza che l'utente si accorga di quanto sta accadendo.
- **Esecuzione di script** – Ogni script è costituito da un insieme di istruzioni che i comuni computer sono in grado di interpretare. L'esecuzione di script avviene solitamente all'interno di software di grande diffusione, come per esempio i browser per la navigazione in Internet, in cui gli script servono per aggiungere contenuti dinamici all'interno delle pagine web. Gli script, nel panorama del software malevolo, sono fondamentali perché hanno lo scopo di collegarsi ad un sito Internet per scaricare ed eseguire il malware stesso. Questa strategia è in parte legata al punto precedente, perché le macro contengono al proprio interno dei veri e propri script che servono appunto per l'esecuzione di software malevolo.
- **Offuscamento del codice** – Per rendere di difficile comprensione ad un lettore umano il codice sorgente che costituisce script e macro si ricorre a tecniche di offuscamento. Queste eliminano ogni riferimento a parole o strutture all'interno del codice che potrebbero in qualche modo ricondurre alle funzioni che il codice stesso cerca di eseguire. Sempre

di più queste tecniche si stanno specializzando per aggirare i controlli dei comuni software antivirus, che negli ultimi anni hanno sviluppato la capacità di esaminare il codice sorgente. Inoltre, una tendenza che sta sempre di più emergendo è quella di utilizzare degli strumenti automatici, dotati di interfacce grafiche di facile uso, che sono in grado di produrre l'offuscamento, personalizzandolo in base alla configurazione scelta.

- **Packing degli eseguibili** – I file eseguibili sono quelli che contengono il malware vero e proprio. Per non poter essere individuati da software antivirus e per mascherarne il funzionamento in caso di analisi fatta dall'uomo, viene utilizzato un packer. Questo è un programma che modifica l'eseguibile originale, ad esempio attraverso tecniche crittografiche, per poi aggiungergli un loader che una volta eseguito è in grado di ricostruire il programma di partenza.

Oltre alle tecniche solitamente utilizzate per celare software malevolo, vogliamo descrivere una nuova strategia che è comparsa nel corso del 2017 e che prede di mira lo specifico comportamento dei portali di Internet Banking di istituti bancari italiani, sfruttandolo allo scopo di dirottare i pagamenti, eseguiti dagli utenti di questi portali, verso conti gestiti dai cyber-criminali in modo più o meno diretto. Il funzionamento del malware sul dispositivo compromesso avviene secondo i seguenti punti.

- Quando l'utente visita il l'Internet Banking del proprio istituto bancario il malware si attiva e resta in attesa che l'utente si posizioni nella pagina di esecuzione dei bonifici.
- L'utente va sulla pagina di esecuzione dei bonifici e compila il campo che contiene l'IBAN di destinazione della transazione.
- Quando l'utente clicca su un altro punto qualsiasi della pagina, ad esempio perché deve compilare un altro campo, il malware entra in azione e cambia l'IBAN destinatario con uno di quelli che sono sotto il controllo dei criminali informatici.
- L'utente non si accorge di questo cambiamento in quanto il browser continua a visualizzare l'IBAN da lui inserito in origine.
- Ignaro di quanto il malware ha fatto, l'utente porta a termine la transazione, ma l'operazione viene accreditata su un IBAN diverso da quello da lui inserito inizialmente.

Ecco alcune osservazioni da aggiungere riguardo il comportamento osservato.

- Per fare agire il malware in modo così mirato è necessaria un'approfondita conoscenza dello specifico portale: le stesse tecniche, infatti, non funzionerebbero se applicate ad altri Internet Banking.
- Nel caso presentato le tecniche con autenticazione multi-fattore non sono di per sé sufficienti ad evitare la frode perché l'utente non sospetta che qualcosa sia stato cambiato all'interno della pagina.
- I criminali non agiscono più in modo solitario, ma costituiscono vere e proprie associazioni organizzate: lo si capisce sia dalla specificità dell'attacco che dal fatto che non è uno solo il conto destinatario delle transazioni fraudolente.

Trend di distribuzione

Presentiamo in Figura 6 l'andamento del numero delle maggiori tipologie di malware bancari individuati durante il 2017 [4]. Analizzando i trend, emergono le seguenti considerazioni.

- La grande famiglia dei malware derivati da Zeus continua ad essere fortemente rappresentata nel panorama dei malware bancari, anche per quanto riguarda lo scenario italiano.
- Una nuova variante di Gozi, a sua volta un derivato di Zeus, si è aggiunta alle varianti già note e il suo andamento ha avuto un picco nei mesi di settembre-ottobre.
- Panda, che è anch'esso variante della famiglia Zeus, si sta confermando particolarmente presente in Italia ed è facile prevedere che anche nei primi mesi del 2018 sarà protagonista di campagne di infezione.
- Dridex si è dimostrato attivo nell'ambito bancario italiano in più campagne di infezione durante l'arco dell'anno e si prevede che continuerà ad esserlo anche per una prima parte del 2018, data la sua capacità di mutare e il numero di campagne attualmente in corso.
- Abbiamo voluto aggiungere anche le tipologie Emotet (già noto dal 2014) e Trickbot che, pur non essendo stati individuati in ambito italiano nel corso del 2017, potrebbero presto colpire anche in Italia. Seguendo ciò che spesso in passato si è già verificato, gli andamenti delle infezioni si ripetono uguali, sebbene spostati in avanti di qualche settimana, anche nel nostro Paese.

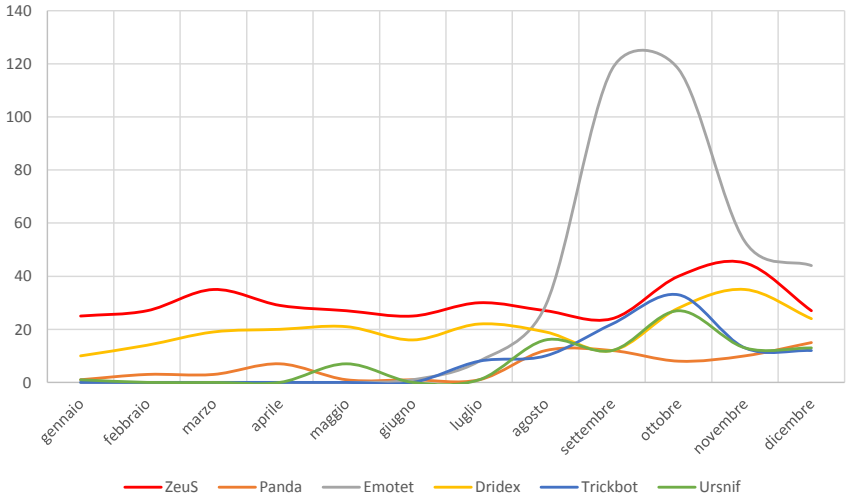


Figura 6 - *Andamenti delle principali famiglie di malware bancario rilevate nel 2017*

Presentiamo anche un andamento per quanto riguarda uno degli argomenti di maggiore rilievo anche dal punto di vista mediatico per quanto riguarda il 2017: il tema è quello del ransomware e di due delle famiglie di maggiore impatto durante il 2017, ovvero Wannacry

e Locky. In particolare Wannacry ha avuto forte impatto perché insieme alle classiche funzioni di cifratura dei dati tipiche dei ransomware ha applicato con successo le capacità tipiche dei worm che sono in grado di propagare l'infezione a tutti i dispositivi vulnerabili connessi in una stessa rete.

Come si evince dal grafico in Figura 7, Wannacry ha avuto un picco di diffusione come numero di sample fra agosto e novembre, dopo essere inizialmente stato notato in un attacco nel mese di maggio. Questo è dovuto al fatto che, una volta che si è diffusa la notizia, il sample originale è stato riutilizzato per produrre nuove varianti appartenenti alla stessa famiglia.

Locky, invece, è ritornato a colpire anche nel 2017, dopo essere stato protagonista nel 2016. Il suo metodo di diffusione è però quello classico: sfrutta mail di Phishing con dei documenti di testo in allegato che, una volta aperti, tramite l'uso di macro sono in grado di scaricare ed eseguire il ransomware, cifrando i dati della vittima.

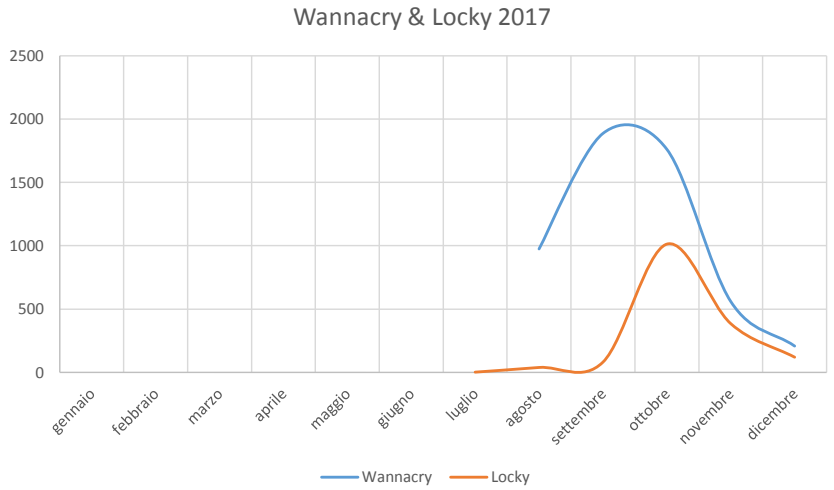


Figura 7 - *Andamenti dei ransomware Wannacry e Locky nel 2017*

Conclusioni

Come abbiamo evidenziato negli esempi a descrizione dei fenomeni presentati, la tendenza a cui stiamo assistendo negli ultimi anni ci porta ad una complessità negli attacchi via via crescente. In particolare, non è più il fattore tecnologico ad aumentare in difficoltà, come succedeva nei primi anni in cui i crimini informatici iniziavano ad essere noti alle cronache. Quindi non sono più solo le vulnerabilità dei sistemi informatici ad essere sfruttate per portare a compimento una frode.
Da qualche anno a questa parte vengono sempre di più utilizzate complesse strategie dietro le quali agiscono articolate organizzazioni criminali, che spesso acquistano i software malevoli, con configurazioni personalizzate per un istituto bancario piuttosto che un altro. Ciò alimenta un vero e proprio mercato di *Malware As a Service*, che va ad unirsi a quello già florido costituito dalla compravendita di credenziali digitali sottratte ai legittimi proprietari.

Questa complessità produce anche un aumento della difficoltà quando si tratta di individuare le frodi stesse: non è più sufficiente l'ispezione manuale dei singoli eventi da parte di un analista umano. Per combattere questi fenomeni la componente umana sarà sempre di più affiancata da strategie che, implementando tecniche di *Machine Learning*, permettono già oggi di esaminare le transazioni che l'utente esegue quando naviga nelle pagine del proprio Internet Banking.
Non è più quindi il singolo evento ad essere giudicato come fraudolento o legittimo, ma è la transazione, come insieme di eventi correlati, ad essere vagliata.

Questo approccio automatico consente, ed è questa la sua vera forza, di definire ed adeguare in modalità dinamica le regole attraverso cui le transazioni vengono valutate perché, sulla base delle richieste passate, riesce a delineare un modello di comportamento, segnalando in tempo reale azioni che non rientrano nel modello standard come tentativo di frode. In un mondo di dati la cui mole diventa ogni giorno più grande, questa modalità risulta al momento la più promettente per l'individuazione di potenziali frodi.

Riferimenti

[1] Phishing, https://en.wikipedia.org/wiki/Phishing
[2] Fonte Cyber Security Command Center (CSCC) di Communication Valley Reply
[3] Zeus Panda Prominent in Italian-Language Phishing Throughout 2017 (https://phishme.com/zeus-panda-prominent-italian-language-phishing-throughout-2017/)
[4] Fonte CERTFin Finanziario Italiano, a cura di Communication Valley Reply, Bollettino Mensile sugli Attacchi Informatici, novembre 2017

Carding - Tecniche di vendita: evoluzioni recenti e future - Periodo 2017

[A cura di Luca Sangalli, Luca Dinardo e Francesco Faenzi, Lutech]

Introduzione

Il presente report redatto dal Team di **Cyber Threat Intelligence di Lutech**, ha lo scopo di presentare lo scenario attuale relativo alla compravendita illegale di carte di credito su internet, fenomeno noto come *Carding*.

Attraverso i nostri sistemi proprietari di ricerca, attivi su fonti pubbliche e private, presenti sia nel deepweb che nel darkweb, sono stati raccolti e analizzati dati riconducibili al tema del carding, trattato su diversi canali:

Nelle successive sezioni viene descritto il fenomeno del carding in generale ("***Il fenomeno del Carding***"), vengono presentati altri canali di vendita ("***Canali di vendita alternativi***"), un impiego della tecnologia della Blockchain ("***Blackmarket e Blockchain"***) e viene riportato un caso di analisi di blackmarket che ha portato all'identificazione di una compromissione ai danni di una catena di ristoranti statunitensi ("***Blackmarket – Analisi di un data breach***").

Il fenomeno del Carding

Con il termine *Carding* si identifica principalmente lo scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari. Il carding è una delle attività più diffusa e popolare nell'underground; è possibile trovare numerosi market specializzati nella sola vendita di dati di carte di credito così come interi forum e thread dedicati all'argomento, con annunci di compravendita, guide e metodi sempre più aggiornati per riuscire a portare a termine questo tipo di truffe.

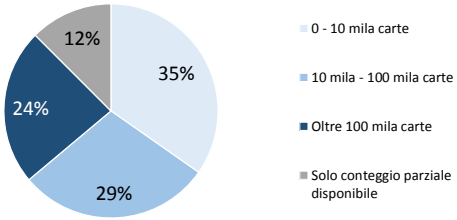
La maggior parte della compravendita di carte di credito avviene tramite i blackmarket, questo perché come per il normale e-commerce legale, è il canale più comodo sia per i

compratori alla ricerca di questo prodotto che per i venditori che lo offrono. In questo modo i contatti fra le due parti vengono ridotte al minimo e la gestione della trattativa è affidata al market. Questo sistema si è evoluto negli anni da semplici siti web a veri e propri marketplace di informazioni illegali, completi di filtri di ricerca, news sui prodotti aggiunti, servizi di feedback e customer care, rimborsi e altro ancora.

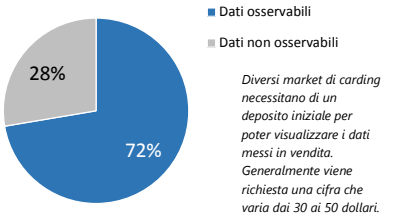
Aggiornamento sui dati dei blackmarket - 2017

In questa sezione viene riportato un aggiornamento sulle statistiche relative ai dati delle carte di credito estratti dai market di carding, su cui è stato possibile verificarne l'effettiva presenza. Vengono riportati diversi indicatori sulla distribuzione di vendita di tali informazioni. I dati numerici relativi ad ogni blackmarket sono stati estratti durante la fase di raccolta delle informazioni.

Distribuzione quantità di carte per market



Distribuzione vendita di carte



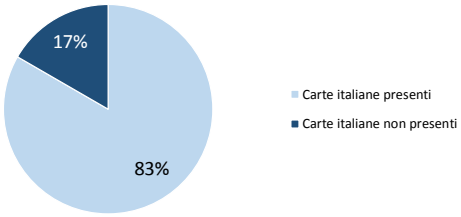
Diversi market di carding necessitano di un deposito iniziale per poter visualizzare i dati messi in vendita. Generalmente viene richiesta una cifra che varia dai 30 ai 50 dollari.

Il conteggio di tali quantità è stato estratto dai market tuttavia è necessario precisare che **non è indicativo dell'effettivo volume di vendita dei market** in quanto può riferirsi al numero di carte di credito in vendita in quel momento, a quelle non scadute oppure all'intero storico di informazioni che sono state presenti sui market stessi.

La maggior parte dei blackmarket presenti in rete ha a disposizione dati prevalentemente Statunitensi, poiché le carte di pagamento non integrano i chip elettronici ma sono dotati solo di banda magnetica, tuttavia sono presenti numeri significativi anche per quanto riguarda le carte emesse da istituiti di paesi europei, fra cui l'Italia.

Distribuzione vendita di carte italiane

(*Totale: 68*)



Confermando la situazione degli anni precedenti, il prezzo delle carte di pagamento messe in vendita sui market si attesta intorno ai 20 dollari, dipendentemente dalla quantità di informazioni disponibili, quali:

- Solo dati della carta (Numero, scadenza e CVV)
- Nome intestatario
- Indirizzo
- Numero di telefono
- PIN

Canali di vendita alternativi

I blackmarket rappresentano sicuramente il canale più utilizzato per la compravendita di dati di carte di credito, tuttavia la loro necessità di essere esposti e raggiungibili li ha resi sempre più oggetto di interesse da parte delle forze dell'ordine e ciò ha inevitabilmente portato al controllo ed alla chiusura di molti di essi (Figura 1) e, più in generale, alla riduzione della durata media della loro vita, come già presentato nel report Clusit 2017 ("*Analisi blackmarket – Scenario e focus sul carding in Italia*").

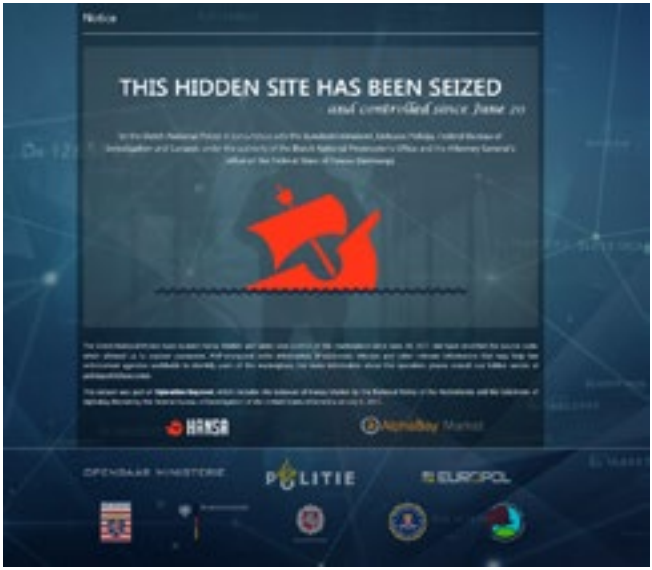


Figura 1 - *Blackmarket chiuso dalle forze dell'ordine*

Per questi motivi, negli ultimi anni si è osservato un trend che ha portato i cyber criminali a spostare la loro attenzione su canali di vendita alternativi. In base alle analisi effettuate per

la redazione di questo ed altri report, tra i principali canali utilizzati per la compravendita di dati di carte di credito e di altro materiale illecito troviamo sicuramente i vari servizi di chat (Telegram, Whatsapp, IRC, ICQ, Jabber, etc.), i forum, sia quelli in clear web che nel dark/deep web, fino all'utilizzo dei classici social network come punto di contatto per la vendita diretta.
Tradizionalmente, uno degli altri principali canali di compravendita sono i forum. I forum sono da sempre uno dei canali più utilizzati nell'ambiente underground per discutere e diffondere attività illegali. Relativamente al carding, possiamo definirli come dei mezzi complementari ai blackmarket, spesso utilizzati dai gestori e da venditori per far pubblicità ai marketplace stessi, come farne conoscere gli indirizzi al quale raggiungerli, presentare feedback dei compratori per ottenere la fiducia dei nuovi utenti, annunciare nuove liste di dati a disposizione dei venditori e altro ancora.

Oltre a questo, molto spesso i venditori pubblicano degli annunci di vendita di dati relativi a carte di credito in loro possesso direttamente sui forum (**Figura 2**), in modo da raggiungere un bacino di potenziali compratori il più ampio possibile.

Figura 2 - *Raccolta thread su vari forum di Carding*

Analizzando numerosi forum dedicati al carding è possibile avere una panoramica di quanto questo strumento sia utilizzato dagli attori specializzati in questo tipo di commercio; in particolare sui forum più popolari sono presenti all'anno mediamente circa 30 thread di venditori "PRO" (seller verificati, che spesso pagano una quota ai proprietari dei forum per una posizione nell'home page del proprio thread) e numerosi di altri venditori.
Non solo, questi canali spesso vengono utilizzati da utenti che sono alla ricerca di collaborazioni per portare a termine le proprie attività illecite. Un esempio è riportato nella figura seguente, dove un utente presumibilmente italiano cerca collaborazione annunciando la possibilità di prelevare soldi da conti frodati (**Figura 3**).

Figura 3 - *Richiesta di un utente italiano su un forum di Carding*

Alcuni di questi shop poi, con l'intento di raggiungere un sempre maggiore pubblico interessato, hanno espanso il loro raggio di azione postando gli annunci anche sui più popolari Social Network e/o creando pagine e gruppi, come ad esempio riportato nella seguente immagine (**Figura 4**).

Figura 4 - *Pagina Facebook relativa a gruppo di Carding*

Oltre ai canali di vendita già descritti, uno degli esempi più significativi è il popolare servizio di messaggistica Telegram, su cui ad oggi è facilmente possibile accedere a numerosi gruppi dedicati alla compravendita di carte di credito; in particolare, per l'analisi in oggetto, sono stati presi in considerazione esclusivamente quelli con linguaggio in italiano.

Analizzando i canali con visibilità pubblica è possibile trovare decine di gruppi dedicati al carding, che hanno una media superiore a circa cento partecipanti iscritti al gruppo e, talvolta, una attività estremamente intensa. Estendendo invece il perimetro alle chat di tutto il mondo, è facile trovare numerosi canali con diverse migliaia di partecipanti, a dimostrazione dell'interesse delle persone e della popolarità del carding.

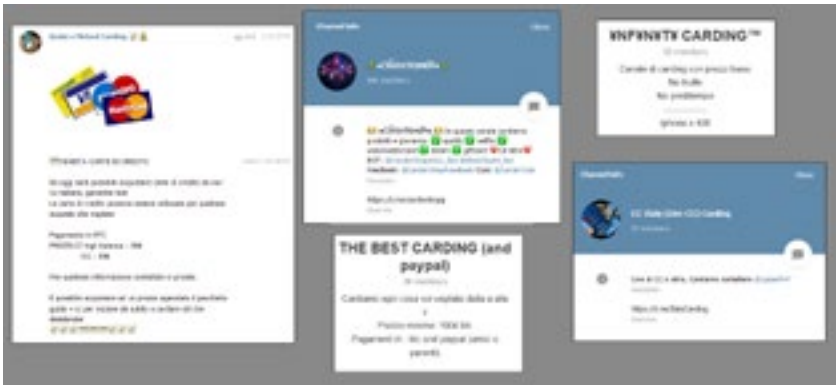


Figura 5 - *Diversi canali Telegram dedicati al carding, in italiano*

Figura 6 - *Feedback degli utenti*

Come è possibile notare dalla **Figura 6**, alcuni di questi venditori hanno addirittura creato appositi canali per raccogliere i feedback degli utenti sulla qualità del servizio.

Blackmarket e Blockchain

Conseguentemente al rapido diffondersi della tecnologia Blockchain, anche i cyber criminali hanno iniziato a sfruttarne a proprio vantaggio i pregi per creare e utilizzare dei nuovi canali di vendita di dati di carte di credito che possano risultare più "sicuri" per il loro scopo.

Ad oggi, semplificando e senza voler scendere nei dettagli dell'attuale tecnologia, gli utenti che visitano un sito web effettuano una query DNS verso uno dei 13 "root server", gestiti da un totale di 12 organizzazioni a livello mondiale, per ottenere l'indirizzo IP del sito web, ospitato su un server centralizzato (fisico o virtuale) di un qualsiasi service provider, ed accedere ai contenuti offerti, tramite l'utilizzo del proprio browser.

Questo meccanismo, inevitabilmente, permette ai gestori di questi "root server" e ai service provider che offrono il servizio di hosting di poter oscurare, censurare e tracciare qualunque contenuto e/o sito web esposto sulla rete internet.

Tramite l'utilizzo della blockchain, invece, oggi è possibile decentralizzare totalmente questo processo.

Ad oggi è infatti possibile registrare dei domini senza la necessità di dover utilizzare un ente centralizzato per la creazione e la gestione degli stessi. Una rete di nodi indipendenti, installati e messi in funzione da chiunque voglia partecipare al progetto in modo attivo, permette ad un utente di registrare dei domini utilizzando una serie di TLD (.bit, .lib, .emc, .coin, .bazar, oltre ai TLD offerti da OpenNIC) in maniera totalmente libera ed anonima.

Dall'altra parte, gli utenti che vogliono accedere a queste tipologie di domini, devono necessariamente interrogare la rete blockchain su cui essi si basano. A tal scopo, sono state create, con la collaborazione di una vasta community di sviluppatori, delle piattaforme di servizi blockchain (ad esempio: blockchain-dns.info, emercoin.com, namecoin.org) che tramite l'utilizzo di software ad hoc e/o plugin, disponibili per i browser più comuni, permettono agli utenti di accedere a questi domini in maniera totalmente trasparente ed efficiente.

Viene riportato di seguito un esempio di un marketplace che sfrutta la blockchain per la traduzione del nome del dominio avente TLD ".bazar".

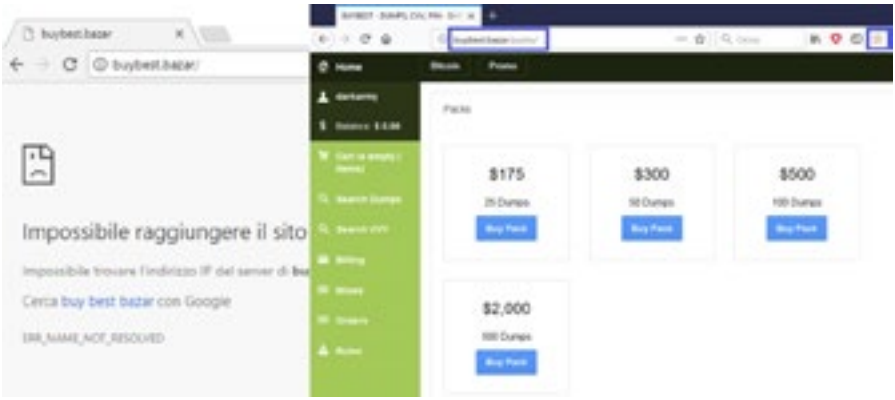


Figura 7 - *A sinistra accesso tramite browser classico, a destra accesso con plugin per BlockChain installato*

Com'è possibile notare dalla **Figura 7**, senza l'installazione del plugin del browser non è possibile accedere al marketplace. Viceversa, attivando il plugin, è possibile accedere a tutti i suoi servizi, disponibili previa registrazione.
Ma non è finita qui; per dare un'idea più puntuale dell'attuale diffusione del fenomeno, ulteriori analisi sul blackmarket precedentemente riportato hanno condotto alla scoperta di ben 42 marketplace differenti (ma molto simili tra loro), registrati su domini ".bazar", incentrati sulla compravendita di dati di carte di credito e di materiale illecito ospitati sul medesimo server localizzato in Russia.

Figura 8 - *Marketplace con domini .bazar ospitati su un server localizzato in Russia*

L'utilizzo della blockchain, come già detto, non si limita alla possibilità di eseguire la registrazione di domini in modo decentralizzato.

Esistono e sono già funzionanti una serie di progetti che tramite la tecnologia blockchain permettono di distribuire totalmente anche i contenuti offerti dagli utenti. Uno di questi è ZeroNet:

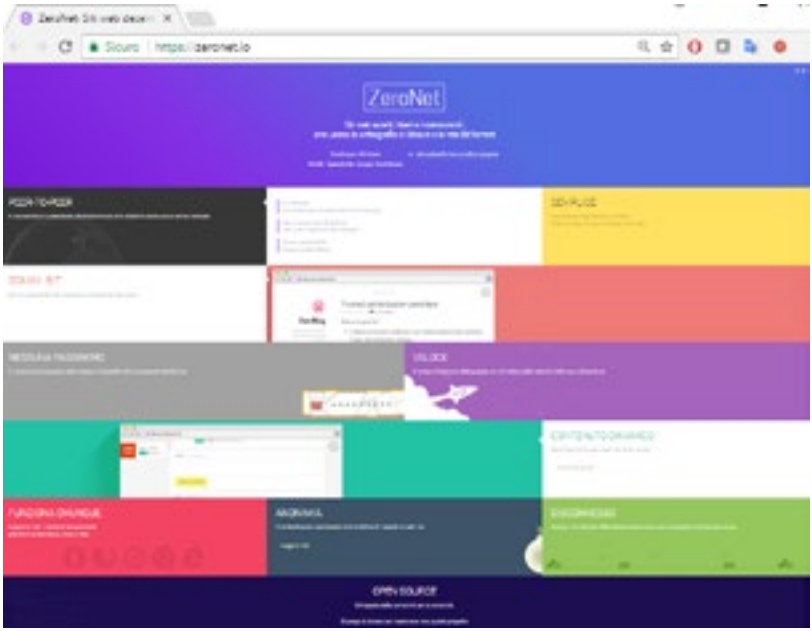


Figura 9 - *Servizio BlockChain per la decentralizzazione di contenuti web*

Sostanzialmente, è stata creata una rete P2P tra i nodi che spontaneamente (ed anzi, incentivati da guadagni dovuti al loro impiego) entrano a far parte della community. Questa rete di client permette la diffusione e distribuzione di un contenuto web sui vari nodi facenti parte della rete stessa. Semplicemente visitando e scaricando un contenuto, in modo automatizzato tramite l'utilizzo di software open source sviluppato ad hoc dalla community di riferimento, un utente mette a disposizione di altri lo stesso contenuto.
Il risultato di tale processo è che ogni utente facente parte della rete, può autonomamente offrire agli altri utenti una versione aggiornata di un contenuto web in maniera totalmente decentralizzata.

E non è tutto, perché questi servizi permettono di integrare un ulteriore layer di anonimizzazione dei client collegati al network, sfruttando la rete TOR e rendendo ancora più difficile poter risalire alle identità degli utenti durante un eventuale processo di "takedown" da parte di enti preposti al controllo che abbiano rilevato la presenza di contenuti non leciti. Proprio per queste caratteristiche, ci si aspetta che sempre più cyber criminali in futuro utilizzeranno queste tecnologie per i propri scopi lucrativi legati al carding (e non solo).

Blackmarket - Analisi di un data breach

I dati delle carte di pagamento messe in vendita sui vari canali precedentemente descritti sono spesso raccolti dai cyber criminali tramite diversi metodi, fra cui l'installazione di dispositivi su sportelli ATM e PoS (skimmer), accessi abusivi a sistemi che memorizzano tali dati (ad esempio negozi e sistemi di e-commerce), malware diffusi e attivi su sistemi degli utenti e altro ancora. Determinare la provenienza esatta dei dati che si trovano in vendita su internet è quasi sempre impossibile per via dell'eterogeneità delle fonti a disposizione dei venditori, tuttavia il monitoraggio dei canali di vendita permette talvolta di riuscire a scoprire sistemi infetti e non ancora noti.

Uno di questi casi è quello avvenuto ai danni di "Jason's Deli", una catena di ristoranti attiva in 29 stati degli USA. Analizzando l'annuncio di un popolare market di carding (**Figura 10**), alcuni ricercatori hanno ricondotto parte dei dati messi in vendita alle posizioni dei ristoranti di Jason's Deli .
(*fonte: https://krebsonsecurity.com/2017/12/4-years-after-target-the-little-guy-is-the-target/*)

Figura 10 - *Annuncio dei nuovi dati in vendita. Si può notare come sia dichiarata la fonte "fonte: High-end restaurant chain"*

La società ha subito avviato un'investigazione e avvisato i propri clienti dell'accaduto, mettendo anche a disposizione un numero di telefono per chiarimenti. Al momento della stesura di tale report, però, non si hanno aggiornamenti in merito alla vicenda.

Conclusioni

Il carding rimane una delle attività di compravendita illegale più popolare, tuttavia, il crescente interesse da parte delle forze dell'ordine nell'affrontare il problema, ha portato ad una sua evoluzione rappresentata da nuovi canali di vendita alternativi ai semplici black-market, e che in particolare sono: servizi di messaggistica diretta, social network e forums. Ad oggi la maggior parte di questi canali e servizi utilizzano dei sistemi per mantenere l'anonimato dei venditori, quali il pagamento in bitcoin e le registrazioni anonime (per i servizi di chat spesso è necessario solo un numero di telefono, che in alcuni stati può non essere associato a nessuna persona fisica).

Inoltre, per rendere sempre più difficoltosa l'attività degli enti preposti al controllo ed evitare il più possibile la sospensione, la chiusura o il tracciamento dei vari marketplace, i cyber criminali hanno iniziato ad adottare dei sistemi decentralizzati per la registrazione dei propri servizi, ad esempio sfruttando il protocollo DNS basato su tecnologia Blockchain. In questo modo i cyber criminali possono registrare e gestire domini in maniera anonima, che vengono poi utilizzati per ospitare siti di compravendita di materiale illecito e che quindi risultano essere difficilmente contrastabili.

Ciononostante, l'impegno ed il monitoraggio costante di tutti questi canali può dare dei risultati di valore che possono andare oltre il semplice blocco delle carte rubate: come nel caso di Jason's Deli può essere possibile risalire ad una compromissione di sistemi reali non ancora scoperta.

GDPR ai blocchi di partenza

[A cura di Sergio Fumagalli]

Nel momento in cui sta andando in stampa il Rapporto Clusit, mancano solo novanta giorni alla scadenza del 25 maggio ma tutto il 2018 sarà l'anno di avvio dell'era del GDPR.
In maggio il Regolamento UE 2016-679 (GDPR) sarà pienamente in vigore in tutta la UE, portando a compimento il disegno iniziato con la direttiva del 95, volto a garantire la libera circolazione dei dati personali in tutta la UE, allargata allo Spazio Economico Europeo (SEE).
I ventuno mesi trascorsi dalla pubblicazione in Gazzetta del GDPR hanno consentito di chiarire alcuni aspetti della nuova normativa e lasciato alcune incertezze che saranno chiarite o con interventi di indirizzo delle Autorità, sulla scia delle diverse linee guida pubblicate fin qui, o con interventi legislativi nazionali o dai tribunali dopo il 25 maggio.

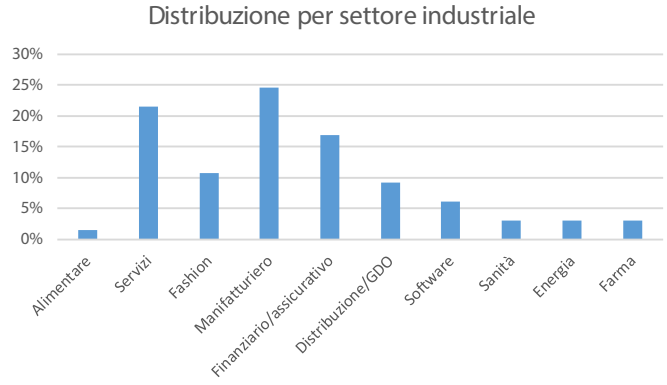


Figura 1

Nel seguito proviamo ad affrontare alcuni punti, sulla base di una esperienza significativa maturata in oltre 60 progetti di adeguamento al GDPR in settori diversi e per aziende di dimensione e complessità assai variabili (vedi **Figura 1** e **Figura 2**).
Non si tratta di un campione statisticamente significativo perché non rappresentativo, nella sua composizione, del contesto nazionale ma comunque interessante per numero e varietà.
L'obiettivo dell'intervento non è dare indicazioni puntuali su specifici articoli del GDPR ma di approfondire, senza alcuna pretesa di esaustività, alcuni temi che spesso, nell'urgenza di raggiungere gli obiettivi di conformità desiderati, vengono trascurati o sottovalutati.

Il quadro normativo

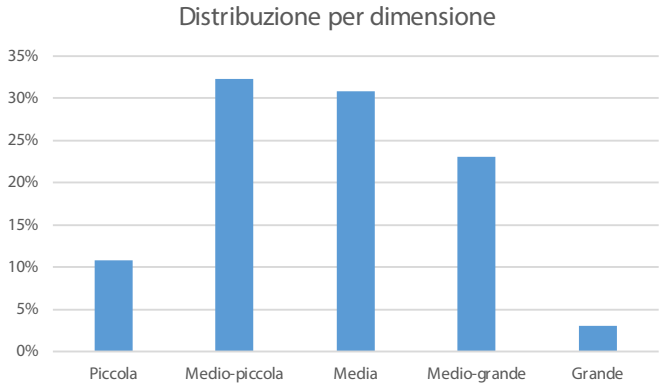


Figura 2

Il contesto legislativo in cui le organizzazioni – aziende, amministrazioni pubbliche, enti – devono operare non è stabile e consolidato ma in progressivo completamento, sia sul piano legislativo che su quello interpretativo. Questo può comportare la necessità di rivedere scelte progettuali già consolidate, alla luce di fatti nuovi ed espone, inevitabilmente, ogni progetto di adeguamento a una certa instabilità.
Le aree grigie non riguardano l'intero corpo normativo ma semmai temi al contorno o all'intersezione con normative applicabili che regolano aspetti diversi: dal diritto del lavoro, alla sicurezza pubblica.
L'incertezza però genera incertezza e alcuni interventi recenti anche del legislatore italiano hanno contribuito ad alimentarla.

A fare il punto della situazione aiuta la COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL del 24 gennaio 2018 che riafferma con forza che il Regolamento è direttamente applicabile in tutti gli Stati membri e autoconsistente. Ai legislatori nazionali sono lasciati alcuni ambiti specifici, identificati e delimitati dal testo del Regolamento come ricorda la Comunicazione citata:
"Member States have to take the necessary steps to adapt their legislation by repealing and amending existing laws, and setting up national data protection authorities, choosing an accreditation body and laying down the rules for the reconciliation of freedom of expression and data protection.
Also, the Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields: public sector, employment and social security, preventive and occupational medicine, public health, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, national identification number, public access to official documents, and obligations of secrecy.

In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations."
Per dare una risposta su questi punti il Parlamento Italiano ha inserito nella Finanziaria 2107 la delega al Governo per la redazione e l'approvazione di uno o più Decreti Legislativi che, al momento di scrivere questo intervento, sono in corso di predisposizione e che sono attesi prima della scadenza del 25 maggio. In una ottica europea, simili interventi sono in corso anche in altri Stati dell'UE(in alcuni Paesi sono già completati).

Come si accennava, altri interventi puntuali del Legislatore italiano, che sono stati approvati nello stesso periodo, sono assai meno comprensibili e lasciano perplessi: per come sono stati approvati, per i loro contenuti, puntuali e non organici, infine, per la contestuale presenza della delega al Governo di cui sopra, che lascia presagire un intervento organico sull'intera materia che sperabilmente assorbirà per intero la competenza del legislatore nazionale di cui, peraltro, la Commissione chiarisce con grande precisione e fermezza i limiti:
"When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct applicability of the Regulation and of jeopardising its simultaneous and uniform application in the whole of the EU are contrary to the Treaties39 […] The national legislator can therefore neither copy the text of the Regulation when it is not necessary in the light of the criteria provided by the case law, nor interpret it or add additional conditions to the rules directly applicable under the Regulation. If they did, operators throughout the Union would again be faced with fragmentation and would not know which rules they have to obey."

L'instaurarsi di normative nazionali in conflitto tra loro o anche solo diverse, vanificherebbe, infatti, uno dei principali obiettivi del Regolamento che consiste proprio nella semplificazione derivante dal passaggio dalla situazione attuale in cui sono presenti, di fatto, 28 legislazioni diverse, seppur derivanti da un'unica Direttiva madre, al nuovo contesto post 25 maggio 2018 in cui il quadro legislativo è determinato dal GDPR in tutta la UE.
A tutela di questo obiettivo la Comunicazione citata non esita ad affermare in modo perentorio quanto segue:
"Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure."

L'aspettativa di un intervento legislativo nazionale in grado di modificare aspetti significativi del GDPR sembrerebbe, dunque, sbagliata.
Detto questo, per le organizzazioni che operano in diversi stati dell'UE, rimane la necessità di fare fronte a un quadro legislativo al contorno del GDPR che rimane frammentato, seppur meno che in passato. Ciò è, in parte dovuto alla difficoltà di cancellare in un colpo solo vent'anni di legislazione nazionale in 28 stati, dall'altro ai limiti stessi

della costruzione europea per quanto riguarda il rapporto con gli Stati nazionali, in molti ambiti contigui alla protezione dei dati personali.
Sul piano dell'interpretazione degli articoli del GDPR, nei mesi intercorsi dalla pubblicazione in Gazzetta del GDPR, sono state emanate diverse linee guida da parte del Gruppo ex articolo 29 e altre sono in corso di elaborazione, come riportato nella **Tabella** 1, contenuta nella Comunicazione di cui sopra.

Guidelines/working documents by the Article 29 Working Party in view of the entry into application of the Regulation[20]	
Right to data portability	Adopted on 4-5 April 2017
Data protection officers	
Designation of the lead Supervisory Authority	
Data protection impact assessment	Adopted on 3-4 October 2017
Administrative fines	Adopted on 3-4 October 2017
Profiling	Work ongoing
Data breach	Work ongoing
Consent	Work ongoing
Transparency	Work ongoing
Certification and accreditation	Work ongoing
Adequacy referential	Work ongoing
Binding corporate rules for controllers	Work ongoing
Binding corporate rules for processors	Work ongoing

Tabella 1 - *Linee Guida e strumenti*

Tutti i testi sono recuperabili dal sito ufficiale del Garante italiano.

Come si vede il quadro complessivo presenta luci ed ombre e lo sforzo di adeguamento delle organizzazioni si è sviluppato e si sta sviluppando in un contesto normativo che è sì unitario per tutto il continente ma che, contemporaneamente, per alcuni aspetti non secondari, viene a precisarsi, con tutte le incertezze che questo può comportare.
Tenerne conto significa minimizzarne l'impatto sui progetti di adeguamento che inevitabilmente devono essere posti in essere.

Il progetto di adeguamento al GDPR

Il GDPR non riguarda una singola funzione: riguarda il Titolare cioè l'organizzazione nel suo complesso.
Nelle realtà meno strutturate e molto focalizzate sull'operatività, spesso l'IT svolge un ruolo trasversale che supplisce alla mancanza di funzioni dedicate all'organizzazione, alla sicurezza, al controllo. In questi casi non è raro che proprio all'IT sia assegnato il compito di gestire il progetto di adeguamento al GDPR.

Nelle organizzazioni più strutturate, operanti in mercati molto regolamentati, invece, spesso la protezione dei dati personali è vista come un problema legale e il progetto di adeguamento viene assegnato di conseguenza all'ufficio competente.
Qualunque sia la scelta, chiunque lo guidi, il progetto deve essere trasversale e multidisciplinare, evitando di privilegiare la dimensione IT, di limitarsi alla revisione delle informative o delle modalità di raccolta del consenso o di concepire i vari aspetti come argomenti separati l'uno dall'altro.
Ad esempio, è ormai evidente a tutti la profondità della trasformazione digitale del business e della società con la sua capacità di creare e trattare intere categorie di nuovi dati spesso riferiti a persone: dipendenti, collaboratori, fornitori, clienti, prospect, consumatori.
Altrettanto evidente è l'impossibilità di ricondurre questo fenomeno alla sola dimensione dei sistemi informativi che spesso sono lontani dal luogo dove la trasformazione viene generata e non hanno, né per ruolo né per competenza, gli strumenti per valutare le conseguenze di queste innovazioni sulle libertà e i diritti degli interessati, cioè delle persone fisiche a cui i nuovi dati e i nuovi trattamenti si riferiscono.
Eppure, sono proprio queste innovazioni a mettere a rischio i diritti e le libertà e, dunque, proprio questi casi dovranno essere valutati attentamente per non esporre l'organizzazione a sanzioni o contenziosi rilevanti.
Affrontare correttamente la compliance al GDPR richiede, dunque, la capacità di coinvolgere tutte le funzioni aziendali, cosa che non sempre un singolo reparto è in grado di fare, senza il supporto di vertici aziendali consapevoli.
Concretamente, trascurare questo aspetto comporta il rischio di spendere un mucchio di soldi per gestire gli aspetti burocratici della Data protection senza davvero individuare e ridurre i rischi più rilevanti.
Un esempio evidente della necessità di un approccio multidisciplinare alla compliance al GDPR riguarda la sicurezza delle informazioni, che è uno dei principi a cui il trattamento dei dati personali deve attenersi, e che viene facilmente considerata una questione "tecnica", anche se il GDPR nell'articolo 32 rimanda esplicitamente a misure tecniche e organizzative per garantire una sicurezza adeguata al rischio.
Le funzioni tecniche sono impossibilitate ad esprimere una valutazione almeno su una delle componenti fondamentali del rischio: l'impatto di una determinata violazione di sicurezza, cioè il danno che ne può derivare. Questo è presidio di chi determina le finalità del trattamento, cioè del management aziendale ai diversi livelli: dai responsabili delle funzioni fino ai vertici aziendali in caso di gravi violazioni di sicurezza con ricadute su milioni di clienti.
I costi che è ragionevole sostenere per adottare adeguate misure di sicurezza dipendono, quindi, da una valutazione che solo in parte è tecnica. Considerare la sicurezza una questione solo "tecnica" e porta a privilegiare investimenti volti a ridurre la probabilità di alcune tipologie di eventi dannosi, sottovalutandone altre e non agendo per ridurne le conseguenze. Il rischio è di effettuare grandi investimenti senza che il rischio ne sia davvero ridotto.
Peraltro, se si guarda ai tre articoli che trattano la sicurezza - 32, 33, 34 - appare evidente come il legislatore abbia cercato di indurre un approccio meno settoriale: l'obbligo di noti-

fica al Garante dei data breach scatta "*a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Può un tecnico esprimersi in merito alla probabilità di un simile rischio?
Anche per la corretta gestione della sicurezza servono dunque, oltre ai tecnici, competenze legali, procedure efficaci, metodologie documentate per assumere e sostenere le scelte discrezionali affidate dal GDPR al Titolare secondo il principio di accountability.

La gestione del dato personale

Si può essere portati ad individuare nella sicurezza il principale impatto del GDPR sui sistemi informativi e sull'uso di tecnologie digitali da parte delle aziende ma questa prospettiva non è corretta.
Una delle più rilevanti novità introdotte dal GDPR riguarda la necessità di determinare il tempo di conservazione del data personale - o un criterio per determinarlo - e di comunicarlo all'interessato nell'informativa, al momento di raccogliere i suoi dati. Al termine del periodo individuato i dati dovranno essere cancellati o essere resi inutilizzabili per quella finalità, se la loro conservazione è richiesta per altre finalità.
La gestione di questo requisito normativo comporta impatti non marginali sulla gestione dei dati da parte delle applicazioni e dei sistemi informativi nel loro complesso.
Il diritto alla portabilità, il diritto all'oblio e alla limitazione del trattamento unito al diritto all'accesso comportano anch'essi una attenzione specifica al ciclo di vita del dato personale, il quale può entrare nei sistemi informativi del Titolare a certe condizioni, è soggetto a regole particolari per tutta la durata della sua permanenza e alla fine deve essere rimosso.
A questa dimensione che riguarda il dato se ne sovrappone, poi, un'altra che riguarda l'interessato a cui il dato appartiene e, in particolare, relativamente alla gestione del consenso concesso a determinati trattamenti o, più in generale, alla base legale che li consente.
La rilevanza dei dati personali per il business aziendale e i rischi connessi ad un trattamento non conforme indurranno progressivamente ad affrontare queste tematiche con strumenti più evoluti di quelli attuali.
Soluzioni strutturali non sono probabilmente compatibili con i tempi dei progetti di adeguamento che hanno nel 25 maggio un riferimento non eludibile. Compito di questi progetti è, però, almeno di evidenziare il problema in modo che progressivamente venga affrontato, sia sul fronte della domanda che su quello dell'offerta in modo efficace e al contempo sostenibile.

La gestione dell'innovazione

Il successo o l'insuccesso del GDPR si misurerà, negli anni, dalla capacità che dimostrerà di tutelare i diritti e le libertà degli interessati senza costituire un ostacolo sproporzionato e insormontabile per l'innovazione e la trasformazione digitale.
Per raggiungere questo obiettivo il legislatore ha delineato una strategia che si regge da un lato sul principio di accountability e dall'altro introducendo alcuni obblighi specifici a carico del Titolare:

- Data Protection by Design e by Default (art. 25)
- Data protection impact assessment e consultazione preventive (artt. 35 e 36)

La gestione dell'innovazione non riguarda tanto il progetto di adeguamento quanto la gestione a regime della conformità, rispetto alla quale il progetto di adeguamento deve limitarsi a dotare il Titolare degli strumenti necessari, cioè procedure e metodologie aziendali, anche semplici, da attivare ogni volta che si introduce un'innovazione significativa.
La Data Protection by Design e by default è una procedura che deve essere applicata ad ogni progetto di innovazione. Deve pertanto diventare una prassi ordinaria: come di un nuovo progetto si valutano sempre gli aspetti economici, così dal 25 maggio bisognerà valutare anche la rispondenza alle regole del GDPR.
La DPIA viceversa è una procedura straordinaria: è richiesta quando l'innovazione può comportare rischi elevati per i diritti e le libertà degli interessati. In questa valutazione, le tecnologie utilizzate e la loro combinazione giocano un ruolo determinante.
La preoccupazione del Legislatore è evidentemente connessa alla impossibilità di sapere a priori dove ci porteranno le tecnologie digitali e la loro combinazione, unita alla consapevolezza dell'impatto profondo che possono avere sulla vita delle persone, spesso al di là della finalità immediata per cui sono introdotte. Ne derivano l'inutilità di dettare regole precise a priori e la necessità di affidarsi in prima istanza al principio di accountability per delegare la valutazione al Titolare.
Anche per il Titolare il rischio di sottovalutare le implicazioni dell'innovazione è, forse, più grave di quello di rischiare qualche sanzione per una conformità zoppicante: le implicazioni dell'innovazione per la protezione dei Dati Personali – ma anche per la sicurezza degli asset aziendali – possono essere rilevantissime, fino al punto di suggerire la cancellazione del progetto e non sono necessariamente proporzionali all'investimento necessario: piccoli progetti, attivati con budget ridotti per raggiungere gli obiettivi di un piccolo reparto, possono comportare il trattamento di dati di milioni di persone ed esporre il Titolare a rischi di compliance o a contenziosi molto onerosi.
Non si tratta, dunque, solo di predisporre delle procedure e delle metodologie ma anche di creare, con una formazione specifica, una consapevolezza adeguata e diffusa in tutta l'organizzazione.
In questi mesi, la DPIA ha colpito l'immaginario delle imprese e dei consulenti in modo particolare.
Quello che deve attirare la massima attenzione è, invece, il complesso di norme poste a presidio dell'innovazione: la procedura obbligatoria di Data Protection by design che al proprio interno deve contenere una verifica sulla necessità di procedere anche al DPIA.
La responsabilità di questo presidio non è in capo al DPO o agli esperti di data protection ma al responsabile del progetto di innovazione: è lui, o lei, ad innescarla e a condurla, come una parte delle proprie responsabilità ordinarie. Questo è il punto di controllo che il Titolare deve presidiare per evitare di scoprire solo a posteriori di essere esposto a rischi di sanzioni o di contenziosi rilevanti.

Conclusioni

Il progetto di adeguamento al GDPR è un passaggio importante a causa delle rilevanti innovazioni introdotte dal GDPR. Si tratta, comunque, di una fase necessaria ma transitoria che non porta ad una conformità statica, definita una volta per tutte ma ad un modello di gestione di una componente strutturale del business che fino a ieri non era tale: i dati personali.
L'osservare da vicino questa fase transitoria porta certamente a rilevare la preoccupazione delle aziende per l'entità delle sanzioni ma anche un livello di consapevolezza dell'esistenza del problema che fino a qualche anno fa non c'era.
Come per la sicurezza, la società e il sistema delle imprese sta lentamente prendendo coscienza della rilevanza assoluta di questioni fino ad oggi trascurate. Non è detto che questo basti, perché il problema cresce ad una velocità maggiore della consapevolezza ma è un inizio che consente di pensare ad una prospettiva positiva.

Il percorso verso il GDPR

[Survey a cura dell'Osservatorio Information Security & Privacy del Politecnico di Milano]

L'avvento del nuovo Regolamento europeo sulla Protezione dei Dati Personali (GDPR) ha letteralmente sconvolto il mercato digitale nel corso dell'ultimo anno. L'attenzione alle modalità con cui raccogliere ed utilizzare i dati dei clienti e la scelta delle tecnologie da mettere in campo per garantirne la sicurezza sono sempre più un punto cruciale nel percorso di introduzione di nuovi progetti di innovazione digitale. Accanto a ciò, la crescente minaccia derivante da attacchi sempre più sofisticati ha smosso l'interesse del mercato delle soluzioni tecnologiche legate alla sicurezza dei dati, che riscuotono sempre maggior successo.

In questo scenario si è mosso l'Osservatorio Information Security & Privacy – promosso dalla School of Management del Politecnico di Milano – in collaborazione con CEFRIEL e DEIB e con il patrocinio di CLUSIT.

L'Osservatorio, al suo terzo anno di Ricerca, si è posto l'obiettivo di rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security & privacy e di monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.

La Ricerca 2017 dell'Osservatorio ha proposto una Survey di rilevazione che ha coinvolto 1107 CISO, CSO e CIO di imprese italiane. In particolare sono state coinvolte 160 organizzazioni grandi (>249 addetti) e 947 PMI (tra 2 e 249 addetti).

L'indagine sulle grandi imprese, oltre a monitorare il mercato dell'information security e le scelte delle diverse realtà rispetto agli aspetti organizzativi, si è soffermata a indagare il percorso di adeguamento delle aziende ai requisiti imposti dal GDPR. La rilevazione ha esplorato cinque aspetti in particolare: l'awareness, il budget dedicato, le azioni implementate, la figura del DPO.[1]
In questo contesto, per il rapporto Clusit è stata svolta un'indagine in esclusiva sulla maturità dei singoli settori (GDO, Finance e Manufacturing) e sulle criticità riscontrate nel percorso di adeguamento al GDPR.

Dalla rilevazione emergono alcune peculiarità tipiche dei diversi settori di business analizzati, alcuni dei quali verranno approfonditi successivamente. Giova anticipare il dato secondo cui le imprese appartenenti ai settori della Grande Distribuzione Organizzata (GDO), bancario e assicurativo, dove il trattamento del dato personale appare essere core-business, hanno avviato ormai da mesi importanti e complessi progetti di adeguamento al GDPR.

[1] La rilevazione è stata condotta tra ottobre e dicembre 2017.

L'indagine ha evidenziato un sensibile incremento dell'awareness delle aziende rispetto all'anno precedente. Sono infatti diminuite le aziende che dichiarano una scarsa conoscenza delle implicazioni del GDPR, passando dal 23% del campione dell'anno scorso all'8% di quest'anno. Coerentemente è emerso come nell'85% dei casi l'intera tematica sia ormai posta all'attenzione del vertice e non solo delle funzioni specialistiche (Security, Legal, Compliance, ecc.). A sostegno di tali dati va rilevato come nel 2016 solamente il 9% del campione dichiarava che fosse già in corso un vero e proprio progetto strutturato di adeguamento alla normativa; nel 2017 tale percentuale si attesta invece sul 51%, mentre il 34% afferma che è in corso un'analisi di dettaglio dei requisiti richiesti e dei piani di attuazione possibili (**Figura 1**).

Figura 1 - *L'awareness e le misure di adeguamento (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

Per quanto riguarda il settore del GDO, il percorso verso l'adeguamento al GDPR risulta essere, come sopra accennato, ben tracciato: il 71% delle aziende dichiara infatti che è in corso un progetto strutturato in materia. Volgendo lo sguardo al settore bancario, il 67% delle aziende ha già messo in atto un progetto di adeguamento e la stessa percentuale si registra tra le organizzazioni rientranti nel settore assicurativo. Tra le aziende manifatturiere, poco più della metà (51%) afferma l'esistenza di un processo di analisi dettagliata dei requisiti richiesti dalla normativa e dei piani di attuazione possibili (**Figura 2**).

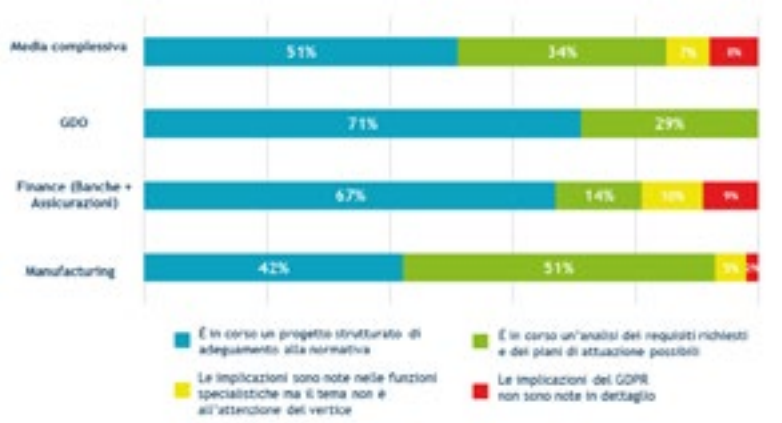


Figura 2 - *L'awareness per settore di mercato (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

Parallelamente alla crescita dell'awareness, si è registrato un notevole incremento del budget dedicato a misure di adeguamento e risposta al GDPR. Mentre nel 2016 solamente nel 15% dei casi esisteva un budget dedicato (nel 7% pluriennale e nell'8% annuale), nell'ultimo anno la percentuale ha raggiunto il 58%: il 35% del campione dichiara l'esistenza di un budget con orizzonte annuale, il 23% con orizzonte pluriennale. È tuttavia ancora alta la percentuale di aziende che afferma che attualmente non esiste un budget: nel 23% dei casi sarà stanziato nel corso dei prossimi 6 mesi e nel restante 19% non è previsto del tutto (**Figura 3**).

Figura 3 - *L'orizzonte di pianificazione (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

La percentuale di organizzazioni operanti nel mondo del GDO che ha stanziato un budget dedicato a misure di risposta al GDPR si attesta sul 53% (35% con orizzonte annuale, 18% pluriennale). Nel settore bancario la percentuale sale al 65% (29% annuale, 36% pluriennale), mentre in campo assicurativo un budget dedicato è stanziato addirittura nell'80% dei casi. Tra le aziende manifatturiere il 47% ha stanziato un budget dedicato a misure di risposta al GDPR con orizzonte annuale (**Figura 4**).

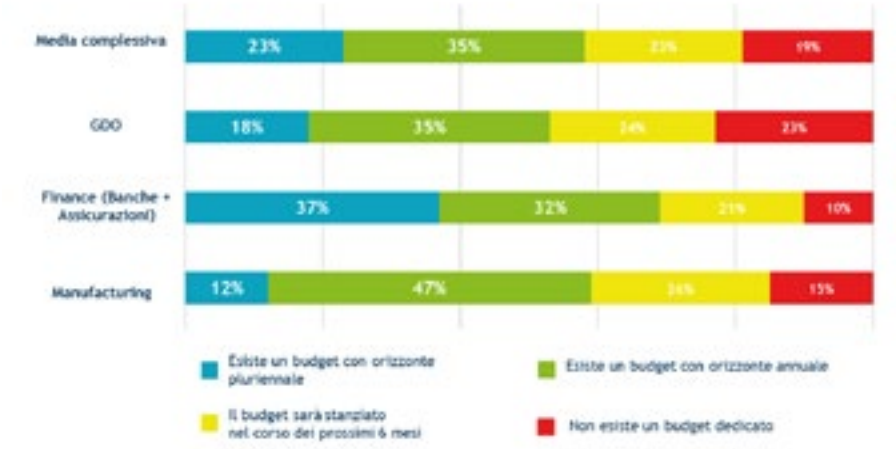


Figura 4 - *L'orizzonte di pianificazione per settore di mercato (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

Entrando nello specifico nelle fasi che compongono il processo di adeguamento al GDPR intrapreso dalle organizzazioni (**Figura 5**), le principali azioni in corso o che sono già state implementate riguardano la valutazione della compliance (87%), l'individuazione dei ruoli e delle responsabilità (80%), la stesura o la modifica della documentazione (77%), la definizione delle politiche di sicurezza e valutazione dei rischi (77%), la creazione e l'aggiornamento del registro dei trattamenti (74%), la valutazione di impatto sulla protezione dei dati personali (57%), la procedura di data breach (53%), il servizio di Data Protection Officer (50%) e l'implementazione dei processi per l'esercizio dei diritti dell'interessato (49%). Analizzando i singoli settori di mercato emerge come l'88% delle aziende del mondo della Grande Distribuzione Organizzata si sta dedicando alla stesura o alla modifica della documentazione, l'80% delle aziende appartenenti al mondo bancario ha iniziato a stendere politiche di sicurezza e analisi dei rischi, mentre il 67% delle organizzazioni manifatturiere ha intrapreso un processo di valutazione della compliance normativa.

Figura 5 - *Le fasi del percorso di adeguamento (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

La Ricerca ha indagato anche la presenza del Data Protection Officer (DPO) all'interno delle aziende. L'introduzione di tale figura, in alcuni casi obbligatoria, è di fondamentale importanza in quanto è volta a facilitare il rispetto, da parte delle singole organizzazioni, delle disposizioni dettate dalla nuova normativa europea. Analizzando il campione, nel 15% delle aziende la figura del DPO risulta formalizzata, nell'10% è una presenza di tipo informale e nel 3% dei casi la responsabilità è delegata a una figura esterna all'azienda. Rispetto alla rilevazione compiuta l'anno precedente, negli ultimi 12 mesi è aumentata la percentuale di aziende che ha dichiarato di voler introdurre la figura del DPO nel prossimo futuro (57%, laddove nel 2016 era il 31%); conseguentemente è diminuita la percentuale di imprese che ha affermato di non prevederne l'introduzione (attualmente pari al 15%). Per quanto riguarda le attività affidate al DPO all'interno dell'azienda, le principali sono: assicurare il rispetto dei requisiti previsti dal GDPR (93%), sorvegliare l'osservanza del Regolamento (76%), fornire pareri al Titolare o al Responsabile del trattamento (59%) e curare i rapporti con gli interessati e con l'Autorità di controllo (55%). (**Figura 6**)

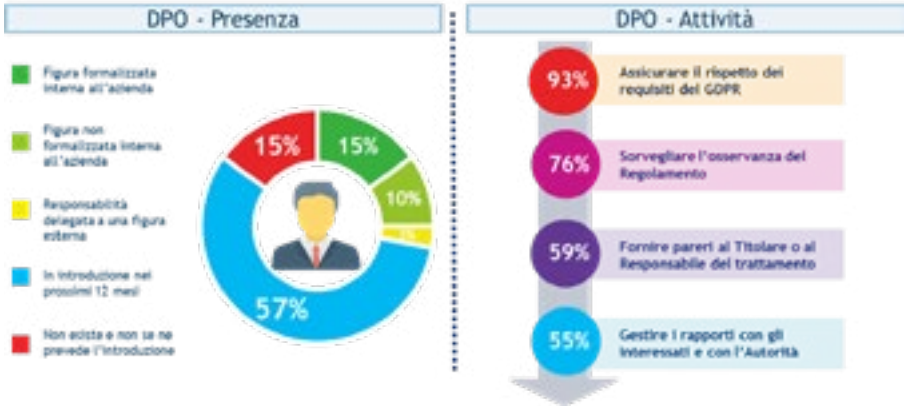


Figura 6 - *Il Data Protection Officer (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

La figura del DPO è presente formalmente solo nel 6% delle organizzazioni operanti nel settore della Grande Distribuzione Organizzata, ma il 76% ne prevede l'introduzione entro 12 mesi. Una percentuale più bassa ma comunque interessante si registra tra le imprese manifatturiere, dove il 54% delle aziende dichiara di voler introdurre nel proprio organico la figura del DPO nel prossimo anno. Passando al settore bancario, il 67% ha dichiarato di avere intenzione di introdurre il servizio di Data Protection Officer entro un anno (**Figura 7**).

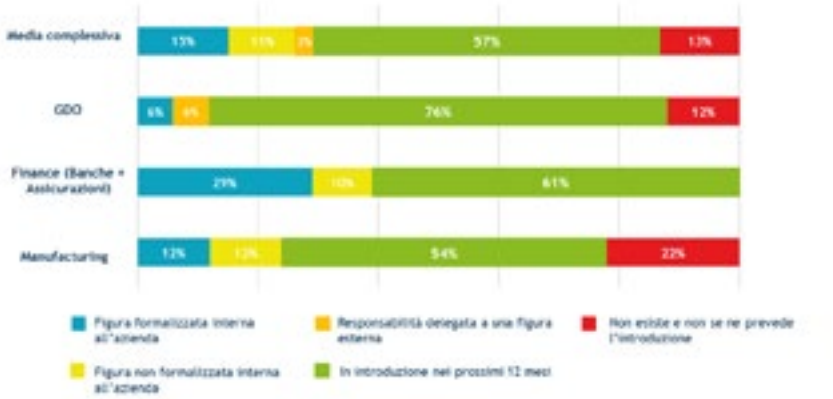


Figura 7 - *Il Data Protection Officer per settore di mercato (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

La rilevazione ha indagato infine quali sono gli ambiti legati al GDPR su cui le organizzazioni si sentono meno preparate e che rappresentano quindi una maggiore criticità nel percorso di adeguamento ai requisiti imposti dalla normativa. Gli aspetti che le aziende ritengono dovrebbero essere maggiormente precisati (ad esempio mediante la formulazione di linee guida) riguardano il principio della privacy by design e la pseudonimizzazione dei dati personali (55%), la valutazione d'impatto sulla protezione dei dati personali (42%), il tema della comunicazione della violazione dei dati personali all'interessato (40%), la figura del Data Protection Officer (32%), la notifica del data breach all'autorità di controllo (27%), il diritto alla portabilità dei dati personali (26%) e i legittimi interessi perseguiti dal responsabile del trattamento (24%). In particolare, l'applicazione del principio della privacy by design e il tema della pseudonimizzazione dei dati personali rappresentano la principale criticità per tutti i settori di mercato (GDO, bancario, assicurativo e manifatturiero) fino a qui esaminati (**Figura 8**).

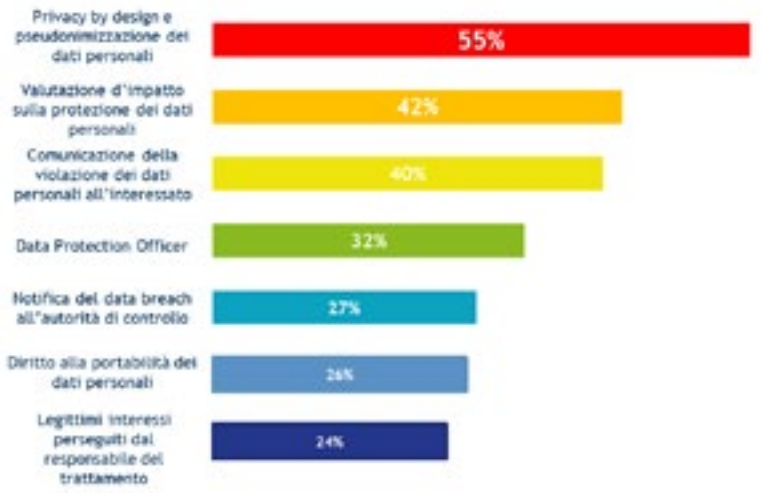


Figura 8 - *Le principali criticità riscontrate (Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano)*

La Ricerca rende comunque evidente che è in corso un sostanziale cambio di marcia.
Il fatto stesso che quasi tutte le aziende che hanno partecipato alla rilevazione dichiarino di aver intrapreso processi di valutazione della compliance normativa e di aver iniziato a individuare ruoli e responsabilità interne alle organizzazioni significa che lo scopo normativo, perlomeno sulle aziende di più alto livello, è stato raggiunto. Il dato probabilmente più significativo è quello per il quale oltre tre quarti delle organizzazioni ha dichiarato di aver steso o iniziato a stendere politiche di sicurezza e valutazione dei rischi: significa aver

coinvolto le giuste competenze, aver avviato un processo di valutazione interna, di analisi dei rischi e quindi, in definitiva, di coscienza della problematica.

Nei prossimi mesi assisteremo al completamento dei progetti di adeguamento al GDPR: saranno finiti gli assessment, saranno stesi i registri dei trattamenti, saranno state adottate le procedure interne a garanzia dei diritti degli interessati e saranno state effettuate le analisi dei rischi. Perlomeno dalle società più attente al tema.
In seguito è presumibile che l'attenzione al tema cominci a permeare anche le PMI per le quali i dati personali non rappresentano il core-business. È probabile inoltre che si assista a una progressiva esternalizzazione dei servizi verso soggetti che, potendo contare su economie di scala, possano proteggere meglio le infrastrutture e le applicazioni e, in ultimo, i dati dei clienti.

Infine, ci si può attendere un'ulteriore crescita degli investimenti in sicurezza informatica e uno spostamento delle attività consulenziali dai progetti di adeguamento al GDPR alle attività sottese al mantenimento della compliance: analisi dei rischi su nuovi trattamenti, Data Protection Impact Assessment e impostazione legale e tecnologica sotto il profilo della privacy by design.

La notifica del Data breach: opportunità o adempimento burocratico?

[A cura di Giuseppe Vaciago]

Introduzione

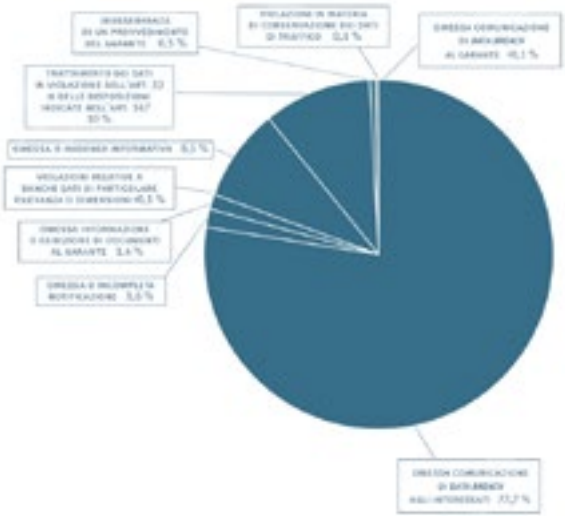
L'art. 4 del Regolamento Europeo sulla Privacy 679 ("GDPR") definisce i *Data breach* come "violazione dei dati personali", ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dal maggio del 2018 tutte le imprese italiane dovranno notificare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza al Garante della Privacy ("Garante"), ogni violazione di dati personali subita all'interno del proprio sistema informatico.

Quest'obbligo era in vigore fin dal 2013 (cfr. provv. del Garante del 4 aprile 2013, n. 161, docweb n. 2388260), anche se limitato alle società telefoniche e agli *Internet Service Provider*.

I dati statistici ci dicono che il trend di segnalazioni di data breach al Garante anche se limitato ad un settore specifico, è in crescita:

Anno	2014	2015	2016
Violazioni	22	49	46



Interessante notare che tra le procedure sanzionatorie del Garante della Privacy del 2016, la percentuale più significativa ha riguardato un importante data breach non correttamente segnalato da una nota Telco.

In definitiva, con l'avvento del GDPR, la procedura di notifica di *Data breach* garantirà, *in primis*, di avere una più corretta percezione del fenomeno e, inoltre, obbligherà le società a investire direttamente o indirettamente, sui processi di gestione degli incidenti informatici che sono alla base della sicurezza informatica.
Questa è una delle tante sfide che questa normativa ci permette di raccogliere se guardiamo al data breach non come mero adempimento burocratico, ma come un'opportunità per aumentare il livello di awareness a livello Europeo sul trend degli attacchi. Tuttavia, per ottenere questo risultato è necessaria una cooperazione non soltanto a livello nazionale, ma anche a livello internazionale al fine di avere in tempo reale dei dati realmente fruibili e in grado di consentire un'adeguata strategia di prevenzione.

La notifica del data breach e la cooperazione internazionale

Partiamo da questo presupposto: ogni data breach ha, sempre con maggiore frequenza, rilevanza transazionale. Basti pensare ai casi in cui i target di attacco sono dei gruppi multinazionali o dei cloud provider che operano su più Stati Membri dell'Unione Europea.
Per comprendere la complessità della procedura di segnalazione di un data breach in grado di compromettere i dati personali relativi a cittadini appartenenti a più giurisdizioni europee, non si può prescindere dalla lettura del paper[1] redatto dai rappresentanti dei Garanti per la Protezione dei dati personali di cinque Stati Membri (Italia, Spagna, Francia, Germania, Grecia) che hanno tratto alcune prime considerazioni in tema di data breach alla luce di uno studio condotto alla fine del 2015 dal Joint Research Centre della Commissione Europea (DG-JRC) in collaborazione con DG-JUST (Direzione Generale della Giustizia e dei Consumatori).
Lo studio si è tradotto in una simulazione o "cyber exercise" che ha visto coinvolti sette Stati Membri (Francia, Germania, Grecia, Irlanda, Italia, Polonia e Spagna) mirata a promuovere la collaborazione tra Stati Membri in caso di attacchi informatici transnazionali. Questo tipo di "esercizio" è di grande utilità soprattutto alla luce della prossima entrata in vigore del GDPR a maggio 2018.
L'obiettivo è stato quello di valutare il livello di preparazione dei vari Stati Membri al fine di prevenire o, comunque, limitare i danni di un attacco informatico, qualora lo stesso colpisca più Stati Membri. I risultati hanno evidenziato, come era ipotizzabile, i seguenti limiti: manca una lista di referenti ("point of contact") dei vari Stati Membri che genera non pochi problemi in termini logistici e comunicativi in caso di situazioni di urgenza, è assente

[1] A. Malatrasa, I. Sanchez, L. Beslaya, I. Coisel, I. Vakalis, G. D'Acquisto, M. Garcia Sanchez, M. Grall, M. Hansen, V. Zorkadis, *Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities,* Computer Law & Security Review, Agosto 2017.

una procedura che consenta uno scambio di informazioni sicuro e, per quanto possibile, anonimo e, da ultimo, non è stata ancora trovata una soluzione ai ben noti problemi di legge applicabile e giurisdizione che vengono amplificati dalle 24 lingue ufficiali dell'Unione Europea utilizzate in caso di segnalazione dai singoli Garanti dei vari Stati Membri.
Il GDPR, tuttavia, oltre ad estendere l'obbligatorietà della notifica a tutte i data controller stabiliti in Europa (artt. 33 e 34) e non più a determinati categorie di soggetti, come si prevedeva con il Regolamento della Commissione 611/2013, richiede una più ampia cooperazione tra le varie Autorità Garanti Europee (artt. 60, 61 e 62). Ne consegue che l'obiettivo di superare questi limiti diventa una priorità che può e deve essere raggiunta.
Rispondere in modo efficace a un data breach richiede un approccio multidisciplinare dove vengono presi in esame aspetti di natura tecnica, legale, finanziaria e sociale che coinvolgono tanto il singolo data controller quanto le stesse Autorità Garanti di ogni Stato Membro.
Il citato studio del DG-JRC ha preso in esame due tipologie di attacchi: quelli relativi ad un soggetto operante in ambito extra UE (ad esempio un cloud provider statunitense), ma che veda coinvolti cittadini Europei in qualità di interessati o un soggetto che opera in ambito UE (si pensi ad esempio ad un gruppo bancario). Ovviamente solo nel secondo caso possiamo ipotizzare una forma di collaborazione, salva la possibilità di considerare "stabilito" il cloud provider in uno degli Stati Membri.
Le raccomandazioni che emergono dallo studio, oltre ad evidenziare la necessità di formare una lista di referenti suddivisi per ogni Stato Membro deputati alla gestione e al coordinamento delle informazioni rilevanti in caso di data breach e a promuovere l'organizzazione di altri "cyber exercise" prima dell'entrata in vigore del GDPR (anche se, fino ad ora, non sembra sia stato dato seguito alla prima iniziativa), si concentrano sostanzialmente su due aspetti fondamentali:

1. Deve essere sviluppata una piattaforma in grado di supportare lo scambio di informazioni in modo sicuro e rapido che sostituisca l'utilizzo (insicuro) dell'email. La stessa piattaforma, inoltre, potrebbe avere numerose altre funzionalità in grado di consentire il coordinamento tra le varie Autorità Garanti europee.
2. Al netto dell'introduzione della piattaforma, devono essere, comunque, previste delle misure tecniche idonee in grado di garantire la sicurezza del flusso informativo tra i vari Stati Membri. Come aveva già evidenziato un noto ISP fin dal 2010 alla Commissione Europea, questo tipo di notifiche potrebbe diventare un target di attacco molto interessante per i cybercriminali. Sarebbe, infatti, paradossale se vi fosse un leak derivante da un precedente attacco. In questo senso, la creazione di policy condivise diventa quindi un obiettivo non più rinunciabile.

Partendo da questi presupposti, mi permetto alcune riflessioni a margine dell'ottimo lavoro svolto dal gruppo di lavoro.
In primo luogo, la piattaforma raccomandata all'esito dello studio dovrebbe essere dotata di un sistema di data sharing sugli attacchi avvenuti anche solo a livello nazionale: la possibilità, infatti, di consultare una repository costantemente aggiornata in grado di consentire

un'analisi efficace sulle più attuali minacce informatiche agevolerebbe l'adozione tempestiva di adeguati strumenti di difesa soprattutto se tali dati venissero condivisi con le Agenzie Europee competenti in materia (si pensi ad esempio ad un coinvolgimento di ENISA o EUROPOL).

L'approccio Statunitense fornisce, nei quarantotto Stati che hanno adottato una normativa sul data breach, degli spunti che meritano uno studio più approfondito. Ad esempio in Arizona si prevede che, in caso di data breach, la società colpita possa notificare agli interessati tale violazione solo dopo che la polizia giudiziaria ha verificato se tale notifica possa compromettere le indagini. Anche la Federal Trade Commission sollecita l'importanza di una cooperazione tra la società attaccata e l'autorità giudiziaria al fine di avere ogni elemento utili per le investigazioni. Pur essendo estremamente improbabile che la condivisione di questi dati possa portare all'identificazione dell'attaccante, è indubitabile che una loro corretta analisi giochi un ruolo fondamentale per la prevenzione di futuri attacchi.
In secondo luogo, è bene evidenziare che la condivisione di un volume di dati così significativo all'interno della piattaforma si accompagna all'esigenza di adozione di particolari cautele in relazione a tre distinti livelli: il primo è quello di garantire, nel rispetto del principio di data minimization, che non siano condivise informazioni non pertinenti alle finalità di sicurezza per le quali la stessa piattaforma è stata creata. Il secondo è quello di, di rendere omogeneo il modello di segnalazione di data breach (il confronto, ad esempio, del modello francese e di quello italiano attualmente in vigore, evidenzia l'esistenza di significative differenze nel format). È pertanto auspicabile, da un lato, che sia introdotto un modello unico a livello europeo che utilizzi un formato idoneo a garantire un'adeguata interoperabilità; dall'altro, che sia previsto l'obbligo di introdurre, almeno in casi di segnalazione che coinvolgano più giurisdizioni, l'utilizzo obbligatorio della lingua inglese in aggiunta alla lingua ufficiale dello Stato Membro.

Il terzo, e forse scontato, livello di cautela attiene al rispetto, nella realizzazione della piattaforma, dei principi della privacy "by design" e "by default", in forza dei quali il trattamento deve sin dall'inizio essere configurato nel rispetto dei requisiti del GDPR e improntato alla tutela dei diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Un ulteriore profilo da considerare è sicuramente quello del rispetto dei principi della digital forensics. Se fosse possibile integrare la segnalazione del data breach con l'invio, ove possibile, di allegati che -nel rispetto delle best practices consolidate a livello internazionale in tema di acquisizione della prova digitale e, ovviamente, della privacy dei titolari del trattamento- fornissero utili elementi circa l'attacco, avremmo aggiunto un ulteriore tassello di fondamentale importanza per studiare e, quindi, prevenire gli attacchi informatici.

Profili Legali

Requisiti della notifica

In sostanza, l'art. 33 del GDPR impone ad ogni società l'obbligo di notificare al Garante qualsiasi violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata.
Tutto questo in 72 ore. Ne discende che tutte le aziende sono sostanzialmente "costrette" ad adottare una procedura che preveda tale notifica, soprattutto se si considera che la stessa deve essere fatta anche in caso di distruzione o perdita di dati per cause differenti da un attacco informatico, come, ad esempio, il banale furto di un laptop di un dipendente che contenga dati personali di clienti o di dipendenti.
Un aspetto particolarmente rilevante però è che, nel caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il GDPR obbliga il titolare del trattamento a comunicare tale violazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione del *Data breach* all'Interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi dati personali. Tuttavia, si può essere esonerati dalla notifica all'Interessato, ove:

a) Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione;
b) Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati di cui alla lettera a);
c) Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.
d) I contenuti delle comunicazioni violate sono interamente cifrati.

Sappiamo bene che l'ipotesi d) è avveniristica poiché la cifratura completa dei dati personali mette a dura prova l'operatività aziendale e quella c) è demandata alla valutazione *ex post* di un giudice.

Rimane quindi da capire quali siano le misure idonee atte a scongiurare tale rischio. Il GDPR ci viene in supporto stabilendo che "*l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può es-*

sere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (ndr. art. 32 del GDPR)".
Pertanto, l'obiettivo è molto semplice: le aziende, per evitare il rischio di un danno reputazionale, dovranno nel prossimo futuro adottare il codice di condotta che verrà presumibilmente stilato dalle associazioni di categoria e validato dal Garante, oppure affrontare un complesso meccanismo di certificazione (ad es. 27001 ISO/IEC). Vi sono ancora molti interrogativi su quali saranno gli standard che dovranno essere rispettati, ma un dato è certo: sicuramente questo tipo di approccio cambierà l'approccio alla sicurezza inforamtica di molte aziende in Italia.

In cosa consiste un Data breach?

Al netto della definizione di *Data breach* prevista dall'art. 4 del GDPR, è importante cercare di contestualizzare tale "violazione di dati personali" all'interno di un contesto aziendale. Da questo punto di vista è recentemente intervenuto il WP29 con un'opinione[2] contenente delle importanti linee guida che hanno distinto in tre macro-categorie il *Data breach*:

(i) "*Confidentiality Breach*", quando vi è un accesso accidentale o abusivo a dati personali;
(ii) "*Availibility Breach*", quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;
(iii) "*Integrity Breach*", quando vi è un'alterazione accidentale o non autorizzata del dato personale.

Sono stati forniti alcuni esempi significativi di *Data breach* che possono essere di grande utilità per inquadrare il contesto con particolare riferimento al caso di "*Availibility Breach*".

Perdita di un device non cifrato	Anche il semplice smarrimento di un telefonino aziendale può costituire una valida ragione di un Data breach nel caso in cui contenga dati personali e non sia stato opportunamente cifrato.
Un device viene infettato da un Ransomware	Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione
Perdità di disponibilità del dato personale	Un esempio potenziale di perdita di disponibilità del dato è quando un dato personale viene inviato per errore ad un terzo non autorizzato.

72 ore: quando parte il conto alla rovescia?

[2] Data Protection Working party 29, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottata il 3 ottobre 2017.

Uno dei dubbi interpretativi maggiori è relativo alla tempistica molto stretta che viene data alle società per comunicare la violazione. Per questa ragione la norma prevede, infatti, che la comunicazione sia fatta "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*". Tuttavia, questo tipo di formulazione pone dubbi interpretativi cul concetto di ingiustificato ritardo. Per questo motivo il GLA29 ha fornito le seguenti esemplificazioni.

Perdita di un device non cifrato	Il titolare del trattamento deve notificare non appena viene a conoscenza che il device è stato smarrito. Il fatto che il titolare non sia a conoscenza che vi sia stato o meno un accesso al device da soggetto non autorizzato non rileva.
Il titolare del trattamento viene reso edotto di un attacco informatico	Il titolare del trattamento deve tempestivamente verificare se sono stati violati dei dati personali e una volta verificato deve procedere alla verifica nelle 72 ore.
Un cybercriminale contatta la società con una richiesta di riscatto dopo averla attaccata.	Il titolare del trattamento deve notificare al Garante da subito tale violazione.

In definitiva, il nucleo centrale su cui è necessario lavorare nella fase investigativa è quella di capire in tempi brevi, l'impatto che il potenziale attacco ha avuto sui dati personali delle varie categorie di Interessati. Implementare una procedura che consenta di valutare preliminarmente non solo "come" è avvenuto l'attacco, ma "cosa" sia stato oggetto di attacco è di fondamentale importanza.

L'art. 33, co. 3 del GDPR chiarisce inoltre che quando non è possibile fornire tutte le informazioni nello stesso momento si può procedere all'invio delle informazioni mancanti in una fase successiva. Infine, può anche accadere che il titolare del trattamento notifichi la perdita della disponibilità di un determinato supporto al Garante e che in un momento successivo lo ritrovi all'interno dei propri uffici senza che lo stesso sia stato alterato. In questo caso, è sufficiente comunicare all'autorità che il supporto è stato ritrovato e richiedere che la procedura di notifica venga annullata.

Quali sono i fattori che determinano il rischio per i diritti e le libertà delle persone fisiche?

L'art. 33 del GDPR chiarisce che la notifica al Garante può non essere fatta "*ove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Per valutare i fattori che determinano tale rischio, il Gruppo di lavoro *ex* Articolo 29 ha determinato i seguenti parametri che permettono di avere più elementi per valutare o meno la rilevanza e/o la gravità di un Data breach:

Fattori che determinato la presenza del rischio per i diritti e le libertà delle persone fisiche
Il tipo di "breach": è evidente che il tipo di violazione determina un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa da dalla perdita dei dati sanitari di un paziente;
La natura, il numero e il grado di sensibilità dei dati personali violati: l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;
Facilità di associare i dati violati ad una persona fisica: capita spesso, infatti, che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;
Gravità delle conseguenze per gli Interessati: quando il titolare del trattamento percepisce il rischio che i dati peronali, oggetto della violazione, possano essere utilizzati immediatamente contro gli Interessati (si pensi al caso della frode o della sostituzione di persona);
Numero di Interessati esposti al rischio: è evidente che un parametro da tenere in considerazione è quello del numero degli Interessati potenzialmente coinvolti.
Caratteritiche del titolare del trattamento: la graduazione del rischio deve essere diversa in base alla tipologia di soggetto colpito. Ad esempio, un conto è l'attacco ad una struttura ospedaliera, un altro è l'attacco al server di un monolocale adibito dall'azienda ad uso foresteria.

Il registro dei Data breach

Ai sensi dell'art. 33 del GDPR è obbligatorio per il titolare del trattamento conservare la documentazione attestante tutti i *Data breach* avvenuti.
I titolari sono, quindi, tenuti a conservare un registro dei *Data breach* che deve contenere le seguenti informazioni:

- i dettagli relativi al *Data breach* (e cioè la causa, il luogo dove è avvenuto e la tipologia di dati personali violati);
- gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal titolare.

Oltre a questi aspetti, il titolare dovrebbe anche motivare la ragione delle decisioni assunte a seguito del *Data breach* con particolare riferimento ai seguenti casi:

(i) il titolare ha deciso di non procedere alla notifica;
(ii) il titolare ha ritardato nella procedura di notifica;
(iii) il titolare ha deciso di non notificare il Data breach agli Interessati.

Rischi sanzionatori

I rischi sanzionatori in caso di mancato rispetto della procedura di notifica del *Data breach* sono, ai sensi dell'art. 83 del GPDR, la sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società (cioè, del titolare). È importante ricordare che in caso di mancata notifica di un *Data breach*, il Garante ha la possibilità di sanzionare la medesima società per l'assenza di adeguate misure di sicurezza ai sensi dell'art. 32 del GDPR, generando così il cumulo di due distinte sanzioni.

Conclusioni

Pur non ignorando la difficoltà d'implementazione del GDPR, si deve rilevare come diventi necessario "tenere l'asticella alta". Solo in questo modo si può sperare di poter sfruttare l'occasione fornita dalla nuova normativa privacy per poter implementare a livello Europeo un efficace sistema di protezione dalle minacce informatiche.

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC

Nel 2017 il NIST ha evidenziato una crescita particolarmente significativa nel numero dei CVEs: le vulnerabilità pubblicate nel 2016 erano circa 6300, mentre nel 2017 lo stesso dato è arrivato ad oltre 14600 segnalazioni. A circa il 15% di tali vulnerabilità i ricercatori attribuiscono un Common Vulnerability Scoring System (CVSS) superiore a 7,5 punti su 10, ovvero vengono riconosciute come vulnerabilità particolarmente gravi che possono avere un impatto critico sulla sicurezza complessiva delle infrastrutture IT di qualsiasi azienda. Nel 2017 sono emerse quasi 2200 vulnerabilità con un livello di gravità elevato e/o critico, evidenziando una acme sostanziale nelle statistiche rilevate dal NIST nell'ultimo decennio. Oltre al susseguirsi dei titoli dei giornali, che contribuiscono ad alimentare un clima di allarme sempre maggiore sulle nuove forme di spionaggio industriale e di criminalità elettronica, nel 2017 alcuni stimoli esogeni, come gli indirizzi di politica industriale su IoT/Industry 4.0 e le nuove normative a tutela della privacy dei dati (GDPR), hanno contribuito a formare una consapevolezza sempre maggiore sul problema del rischio IT, evidenziando le fondamentali fragilità che si nascondono dietro tecnologie che sono diventate in pochissimi anni le infrastrutture fondamentali non soltanto per il modello di business di molte imprese ma per le stesse istituzioni che stanno alla base della società.
Ogni anno IDC propone una breve panoramica che guarda alle tendenze internazionali più significative che andranno a incidere sull'orizzonte di breve-medio termine del settore della Sicurezza IT.

Nel 2018 alcune tendenze tecnologiche proseguiranno nel loro processo di rinnovamento dei paradigmi tecnologici più consolidati: in questa sede, tra le principali tendenze individuate da IDC nel FutureScape 2018, è possibile evidenziare l'attestazione di piattaforme sempre più integrate per il consolidamento del parco applicativo, la diffusione di nuovi strumenti per la gestione degli attacchi automatici e persistenti (i cosidetti *deception programs*), l'affermazione dei programmi di tracciamento della filiera e di certificazione in termini di sicurezza delle componenti hardware (esigenza che si sta rivelando una *conditio sine qua non* per la realizzazione di paradigmi IoT e Industry 4.0).
Secondo IDC, entro il 2020 un terzo della spesa globale in Sicurezza IT si indirizzerà verso quegli operatori che avranno saputo proporre al mercato delle piattaforme di sicurezza complete. Sia a causa dei limiti di budget sia per ridurre la complessità di gestione, un numero sempre maggiore di CIO si orienterà verso piattaforme realmente integrate a discapito delle soluzioni puntuali. Con la diffusione del Cloud negli ambienti Enterprise e la progressiva attestazione di ambienti IT ibridi che combinano elementi cloud, edge e on-premise, sono andate moltiplicandosi le soluzioni di Security specializzate nella gestione di singole sezioni della rete aziendale. Talvolta le infrastrutture IT delle imprese ospitano fino a 50 diverse soluzioni di Sicurezza nei propri ambienti, con un sostanziale incremento nella complessità

di aggiornamento, gestione delle patch e monitoraggio delle potenziali minacce che si nascondono in rete.
Nei prossimi due anni il 60% delle imprese del Global Ranking 2000 di Forbes metterà in campo veri e propri *deception tools* per ingannare gli attaccanti, incrementando il costo delle operazioni di *hacking* automatico e migliorando la resilienza delle reti. L'automazione sempre più intelligente nell'ambito della Sicurezza IT, i cosiddetti *cyber-reasoning systems*, sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi, sono stati ampiamente dimostrati negli ultimi anni (basti pensare al sistema Mayhem sviluppato dalla Carnegie Mellon University e presentato durante il cyber Grand Challenge del 2016, per citare soltanto il nome più famoso). Sebbene da alcuni siano ancora considerati degli esercizi accademici che richiedono elevati investimenti e di tempo e di risorse, le nuove *deception technologies* possono contribuire a rendere le operazioni di infiltrazioni più "rumorose", semplificando gli esercizi di identificazione da parte degli analisti. Negli ultimi anni si è assistito a una vera e propria "corsa agli armamenti" dell'automazione, sia per la difesa che per l'attacco alle reti informatiche, e nei prossimi anni diventeranno sempre più comuni.

Entro il 2020 un settimo dei dispositivi IoT saranno certificati per garantire che durante il processo di produzione e distribuzione non siano stati compromessi dal punto di vista della Sicurezza IT, certificando il livello di rischio sia a livello di firmware che di hardware. Dai primi strumenti di cyberwarfare come Stuxnet, Duqu, Flame fino agli exploit condotti dall'Equation Group, di anno in anno ormai vengono rivelate vulnerabilità sempre più clamorose di infrastrutture tecnologiche che si ritenevano perfettamente consolidate. Tali vulnerabilità, che passano attraversano livelli sempre più profondi dello stack ISO/OSI, dal firmware degli hard-disk (come nel caso di GrayFish/ EquationDrug) fino ai meccanismi di esecuzione dei processori (come nel caso dei recentissimi MeltDown e Spectre), lasciano spazio a una crescente sofisticazione degli attacchi che deve essere affrontata a livello di filiera produttiva dei componenti affinché l'IoT diventi una concreta prospettiva per il futuro. Soltanto un sistema di relazioni industriali basato su un'autorità di certificazione del tutto terza e indipendente potrebbe consentire di risolvere tale problema, certificando l'integrità dei componenti dalla produzione fino all'assemblaggio finale attraverso l'ecosistema frammentato e variegato dei fornitori di dispositivi IoT.
A pochi mesi dalla scadenza del periodo transitorio di adeguamento al GDPR (25 maggio 2018), una parte sempre più ampia del mercato italiano ha intrapreso una valutazione più approfondita in merito ai temi della privacy, della gestione dei dati sensibili e della prevenzione dei data breaches. Il GDPR pone l'accento sulla necessità di concepire la Sicurezza non soltanto come un accessorio superficiale, ma come una componente essenziale nel disegno di qualsiasi processo produttivo e distributivo, contemplando una visione del futuro dove le tecnologie ICT saranno infrastrutture sempre più pervasive anche a livello industriale. Introducendo principi come la *data protection by default*, la progettazione di qualsiasi processo aziendale, non solo dei processi IT, richiederà una specifica attenzione

rispetto allo stato dell'arte delle tecnologie per la Sicurezza IT, evidenziando i razionali delle scelte tecnologiche e qualificando l'appropriatezza di qualsiasi decisione di implementazione. Una sfida lanciata non soltanto alle imprese italiane ed europee, ma a qualsiasi impresa internazionale che intenda lavorare con i dati dei cittadini europei, attraverso l'inclusione di specifiche clausole di extraterritorialità nel testo della nuova normativa.

La Sicurezza IT in Italia: le previsioni di spesa aggregata

Nei paragrafi che seguono viene proposta una sintetica rappresentazione quantitativa dei principali segmenti della Sicurezza IT con riferimento al mercato italiano, in base alle tassonomie standard impiegate da IDC a livello internazionale. Le informazioni derivano dalla stima dei risultati dei principali operatori con riferimento ai ricavi di licenze, rinnovi, manutenzioni e sottoscrizioni a consumo di servizi rispetto al territorio nazionale. Le stime derivano sia dalla *knowledge base* accumulata da IDC a livello internazionale sia dalla ricerca condotta a livello locale, dai contatti diretti con gli operatori e dall'analisi delle comunicazioni economico-finanziarie. IDC impiega tassonomie standard, neutrali rispetto alle denominazioni commerciali impiegate dagli operatori; per facilitare i processi di conciliazione dei dati, le informazioni raccolte durante le indagini vengono ricondotte nell'ambito di tali tassonomie standard, rispetto le quali vengono categorizzare e comparate le informazioni raccolte nelle varie geografie.

Il Software per la Sicurezza IT, segmentato nelle aree della Web Security, del Security & Vulnerability Management, della Network Security, dell'Identity & Access Management e dell'Endpoint Security, rappresenta in Italia un valore complessivo di circa 360 milioni di euro nel 2017 (***Fig. 1***). Con un $CAGR_{2017\text{-}2020}$ di otto punti percentuali, con una prospettiva al rialzo rispetto alle stime dello scorso anno, a trainare la crescita del comparto sono essenzialmente le applicazioni legate a Security & Vulnerability Management e Identity Access Management, in alcuni casi con tassi di crescita anche a due cifre, mentre le altre aree esprimono tendenziali di crescita inferiore. Nel momento in cui le strategie di difesa si spostano da una logica perimetrale/ network a una prospettiva centrata su dato/ identità, si assiste a un progressivo spostamento dei razionali di spesa verso nuove aree tecnologiche.

Figura 1– *La Sicurezza IT, i principali segmenti del mercato italiano (Software, Appliance e Servizi). Fonte: IDC Italia, 2018*

In merito alla categoria delle Appliances per la Sicurezza IT, IDC segmenta il mercato in cinque aree principali (VPN, Firewall, IDP, Unified Threat Management, Content) che nel 2017 hanno espresso un valore complessivo di poco sopra i 200 milioni di euro (***Fig. 1***). Con un $CAGR_{2017\text{-}2020}$ stimato in circa cinque punti percentuali, IDC propone un maggiore ottimismo nelle sue stime di medio termine, sebbene la maggior parte della crescita sia riconducibile essenzialmente alle soluzioni di Unified Threat Management, mentre rispetto alle altre aree tecnologiche contemplate osserva un tasso di crescita estremamente contenuto e quasi flat nel medio termine.

I Servizi per la Sicurezza IT rappresentano il comparto caratterizzato dalla maggiore dinamicità in termini di continuo rinnovamento delle proposizioni dei principali operatori, con una articolazione sempre più profonda dei servizi proposti al mercato. Proponendo una tassonomia generale e neutrale rispetto alle proposte dei diversi operatori, IDC stima la dimensione del comparto in base alla ripartizione tra servizi di IT Consulting e servizi di System Integration/ Implementation. Con un $CAGR_{2017\text{-}2020}$ sopra ai tre punti percentuali, in moderato rialzo rispetto alle previsioni dello scorso anno, i servizi hanno un valore superiore ai 500 milioni di euro nel 2017.

Opportunità e sfide secondo le imprese italiane

Nella sezione seguente verranno evidenziati i principali risultati di una indagine condotta da IDC sul mercato italiano che ha coinvolto circa 400 imprese nel segmento sopra i 10 addetti, includendo gran parte della struttura imprenditoriale del Paese (dal manifatturiero ai servizi, dal commercio alla pubblica amministrazione, dalle utilities fino ai trasporti e alle comunicazioni).

Lo strumento di indagine, composto da circa una ventina di quesiti di approfondimento con domande a risposta chiusa e a risposta multipla, ha indagato i fattori che indirizzano la spesa in Sicurezza, le priorità principali dell'impresa, sia lato business che technology, la rilevanza della Sicurezza rispetto a diversi paradigmi tecnologico-organizzativi (dalla Trasformazione Digitale all'Internet delle Cose, senza dimenticare la rilevanza del GDPR nel 2018). Il questionario è stato somministrato a un campione che comprende sia le figure apicali dell'IT aziendale (CIO/ Directors/ etc.), sia figure più specializzate che danno una centralità di rappresentanza al tema della Sicurezza IT (Chief Information Security Officer/ IT Security Manager/ etc.), sia figure di middle management più generaliste per cui la Sicurezza IT rappresenta un compito comunque imprescindibile (IT Manager/ Responsabili IT/ etc.).
Il dato campionario è stato estrapolato all'universo delle imprese in base a elaborazioni IDC dei dati ISTAT così da dare una puntuale rappresentazione del fenomeno della Sicurezza IT rispetto al segmento delle Imprese con oltre 10 addetti in Italia.

Tendenze di spesa e investimento del mercato italiano

Dalle ultime indagini condotto sul segmento sopra i 10 addetti, emerge una valutazione della congiuntura economica 2018 improntata a un moderato ottimismo: circa il 72% delle imprese evidenzia previsioni di fatturato stabile per l'anno a venire, circa il 24% attende una crescita dei risultati rispetto all'anno precedente, mentre soltanto il 4% segnala una potenziale riduzione. Si vanno rafforzando le aspettative di una ripresa più generale dell'economia: i segnali ancora deboli rilevati nell'edizione dello scorso anno cedono il passo a un maggiore ottimismo, che si riflette nella spesa potenzialmente allocabile per i budget ICT e nel budget rate della Sicurezza IT. A guidare le previsioni di crescita per il 2018 sono le medie e le grandi Imprese, dove quasi due imprese su tre prevedono un anno di espansione dei risultati aziendali e quasi una su dieci attende una crescita a doppia cifra. I settori al cardine della crescita sono i servizi alla persona, il comparto bancario e il commercio al dettaglio.
Oltrepassati i momenti più difficili della crisi globale dell'economia, uno scenario improntato sulla ripresa non può che riflettersi positivamente sulle prospettive di evoluzione della spesa ICT per il 2018: circa il 78% delle imprese prevede un budget ICT sostanzialmente stabile, il 16% intravede una crescita credibile, mentre soltanto il 6% segnala una ulteriore razionalizzazione della capacità di spesa. Da notare come le aspettative di fatturato abbiano un impatto esteso nel determinare le prospettive del budget ICT (***fig. 2***): laddove il fatturato è in espansione, il 46% delle imprese indica una conseguente espansione del budget ICT; viceversa, dove il fatturato è dato come stabile, oppure in riduzione, soltanto il 7% delle imprese apre qualche spazio a una crescita potenziale della spesa ICT. Le previsioni di crescita dei budget ICT sono ampiamente eterogenee rispetto ai comparti industriali, ma a differenza degli ultimi anni le maggiori aspettative di crescita anno su anno cominciano a care capolino anche in comparti *material-intensive* come il manifatturiero e il commercio al dettaglio (a guidare la ripresa degli investimenti non sono più e soltanto i settori *information-intensive* come le banche e i servizi).

Figura 2 - *Fattori congiunturali che influenzano le prospettive di spesa in Sicurezza IT. Fonte: IDC, 2018 (rispondenti n=398, imprese con oltre 10 addetti; estrapolazione all'universo basata su modello di analisi territoriale)*

Il passo successivo, il movimento dalla formazione del budget ICT alla definizione di un budget per la Sicurezza IT, non è assolutamente scontato, soprattutto se si considera la posizione radicalmente dicotomica che assume il mercato italiano: circa il 47% delle imprese spendono in modo del tutto saltuario, mentre circa il 48% spende esclusivamente nel budget generale dell'IT, mentre meno del 5% delle imprese considera la Sicurezza IT una spesa strategica a cui riservare un budget specifico e dedicato nel 2018. In considerazione di tali premesse, non sorprende che tra le varie voci che formano il budget IT la Sicurezza molto spesso assume un peso marginale: infatti, circa il 30% delle imprese italiane assegna meno dell'1% del budget IT complessivo alla Sicurezza, il 24% si spinge fino al 3% e meno del 5% delle imprese supera tale soglia. A tale marginale attribuzione di valore, si aggiunge la grande elasticità di tale spesa rispetto all'andamento di variabili fondamentali come il fatturato e il budget ICT: come si osserva in fig. 2, dove il fatturato o il budget ICT risultano stabili o in riduzione, oltre il 70% delle imprese alloca meno dell'1% del budget alla Sicurezza IT; viceversa, quando le previsioni sono positive, il 45% delle imprese spende ben oltre tale soglia, quasi il doppio rispetto agli altri casi.

Nel corso dell'indagine sono state approfondite le specifiche aree di investimento previste dalle imprese italiane nel 2018 (***fig.*** 3). Nell'ambito di tale rappresentazione, in parte riconducibile alla tassonomia IDC delle tecnologie per la Sicurezza, si è segmentato il dato rispetto alle categorie di spesa, distinguendo il gruppo delle imprese che spende in Sicurezza meno dell'1% del budget IT (*Low Spender*) da quello che spende al di sopra dell'1% (*High Spender*). Tale ripartizione consente di dare ulteriore sostanza a quella dicotomica suddivisione del mercato italiano tra imprese che investono in modo del tutto contingente nella Sicurezza e imprese che considerano la Sicurezza una infrastruttura essenziale per abilitare nuovi modelli, processi, paradigmi. Emerge un quadro di notevoli differenze tra i due raggruppamenti.

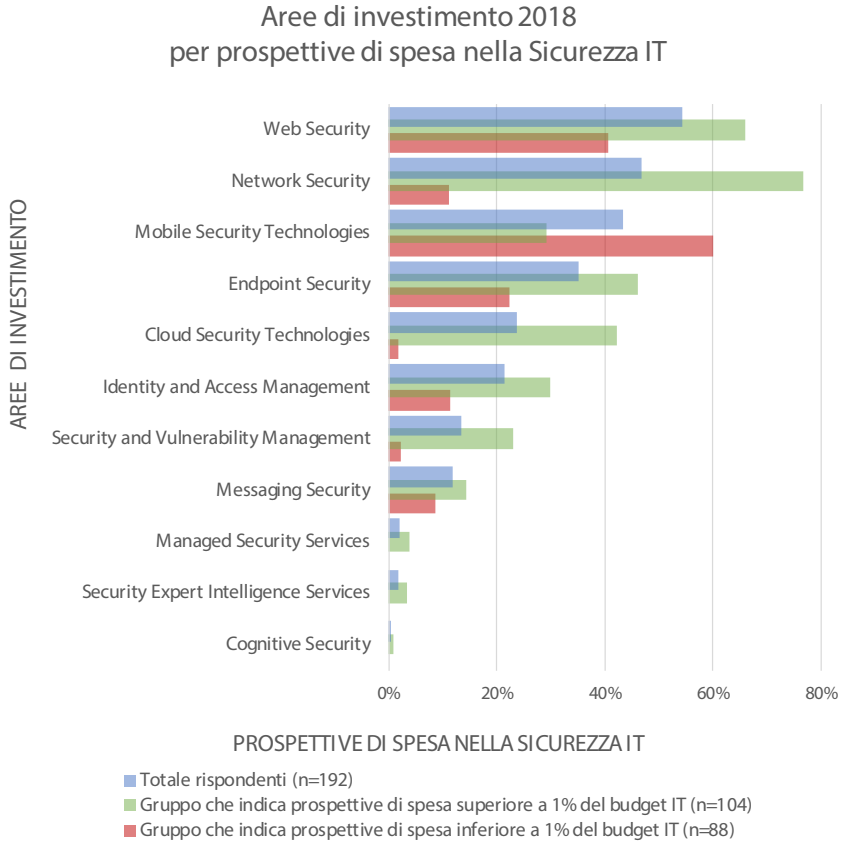


Figura 3 - *Aree di investimento 2018 nella Sicurezza IT. Fonte: IDC Italia, 2018 (rispondenti n=192, imprese con oltre 10 addetti; estrapolazione all'universo basata su modello di analisi territoriale)*

Nel 2018 gli *High Spenders* si distribuiscono in media su tre distinte aree di investimento, mentre i *Low Spenders* sulla metà, circa una e mezzo. Mentre la Web Security rimane un'area di investimento centrale per entrambi i raggruppamenti, gli *High Spenders* si polarizzano in modo particolare sulla Network Security, mentre i *Low Spenders* mettono in evidenza le tecnologie per il Mobile. È possibile immaginare che in alcuni contesti organizzativi di medie e grandi dimensioni, i sistemi informativi siano basati su una infrastruttura IT piuttosto sviluppata e articolata, che richiede interventi su diversi fronti, mentre in contesti organizzativi di più modeste dimensioni, di fatto la rete aziendale molto spesse assume una forma piuttosto elementare, e i dispositivi mobili rappresentano molto spesso la principale appendice a rischio.
Il raggruppamento degli *High Spender* si estende sull'intero spettro delle opzioni disponibili, senza trascurare i servizi più sofisticati, come ad esempio i Managed Security Services, la Security Intelligence e la Cognitive Security: si tratta senza dubbio di un ristretto gruppo di *early adopters* che sperimenta i primi passi nella terra incognita delle nuove proposte degli operatori. Viceversa, è immediato osservare come i *Low Spender* praticamente scompaiano in diverse aree tecnologiche, neanche quelle più sofisticate e innovative in assoluto: ad esempio, sono minimamente rappresentati nelle aree della Cloud Security e della Vulnerability Management, mentre sono del tutto assenti nelle aree di servizio più sofisticate. Questa parte del mercato italiano è ampiamente rappresentata da imprese di piccola e media dimensione, con un approccio piuttosto tradizionale, prevalentemente *signature-based*, rispetto alla gestione della Sicurezza IT

La Sicurezza IT tra priorità tecnologiche e di mercato

Nella sezione seguente si affronta l'impatto della Sicurezza IT rispetto alla pianificazione strategica delle imprese, con riferimento sia alle priorità tecnologiche, riconducibili alla progettualità del dipartimento IT, che alle priorità di mercato, riconducibili alla progettualità dell'impresa nella sua globalità. Dall'indagine emerge con particolare evidenza come le imprese che nel 2018 intendono indirizzare il proprio impegno verso un miglioramento della Sicurezza IT esprimono una agenda strategica sistematicamente differente dalle altre imprese italiane.
Come già osservato negli anni scorsi, la Sicurezza IT si posiziona sempre all'apice delle priorità tecnologiche delle imprese italiane, sebbene tale rilevanza talvolta si traduca in una dichiarazione di principio più che in una effettiva prerogativa di spesa, come ampiamente evidenziato nei paragrafi precedenti. La necessità di preservare la rilevanza dell'IT aziendale, in un momento di trasformazione molto significativo della società, delle filiere industriali e degli stessi paradigmi tecnologici, induce molto spesso ad attribuire alla Sicurezza quasi un ruolo di governance dei sistemi informativi, travalicando di molto le aspettative che sarebbe ragionevole attribuire a un ambito così specifico. Pur senza arrivare a tali estremi, anche quest'anno l'indagine mette in evidenza la natura intrinseca della Sicurezza IT come abilitatore tecnologico indispensabile per esprimere una parta importante delle progettualità aziendali, come si avrà modo di mostrare nei prossimi paragrafi.

La Sicurezza IT viene indicata come priorità per il 2018 da circa il 28% delle imprese italiane sopra i 10 addetti. Sebbene il dato dello scorso anno facesse riferimento a un perimetro di indagine assai più ristretto, che comprendeva soltanto le imprese sopra i 50 addetti, comunque si osserva un certo ridimensionamento rispetto ad altri indirizzi strategici rispetto allo scorso anno, in modo particolare rispetto ad obiettivi di automazione e di consolidamento dei sistemi, molto spesso riconducibili alle prime sperimentazioni su nuovi paradigmi, come ad esempio l'Internet delle Cose, che comunque hanno un impatto positivo sul budget rate complessivo destinato alla Sicurezza, come si avrà modo di osservare nei paragrafi successivi.
Conviene soffermarsi qualche ulteriore istante per commentare le differenze in termini di progettualità tra le imprese che appartengono a questo raggruppamento e le altre imprese italiane rappresentate nel campione (***fig. 4***). Da tale confronto emergono sostanziali difformità nell'orizzonte strategico per il 2018: le imprese con obiettivi legati alla Sicurezza IT sono ampiamente più orientate sull'automazione e sull'ottimizzazione dei processi (55% nel gruppo Sicurezza IT rispetto a un dato del 32% sul totale campione). La differenza è ancora più marcata in merito al miglioramento dei servizi IT e dei tempi di delivery (39% contro il 13% del campione generale) e rimane comunque molto elevata nella dimensione relativa all'innovazione e al rinnovamento delle infrastrutture IT/ datacenter (26% versus 9%). Sono questi gli indizi che inducono a ritenere che l'investimento in Sicurezza IT sia prodromo rispetto a processi di trasformazione più generali, legati sia alla Trasformazione Digitale nelle sue multiforme sfaccettature sia all'Internet delle Cose e all'Industria 4.0 sia ad appuntamenti normativi importanti, come la fine del periodo transitorio di adeguamento al GDPR.

Figura 4 - *Influenza della Sicurezza IT nell'orientamento delle priorità tecnologiche delle imprese italiane. Fonte: IDC, 2018 (campione n=398, imprese con oltre 10 addetti; estrapolazione all'universo basata su modello di analisi territoriale)*

Allo stesso modo, seguendo il medesimo approccio nella suddivisione del campione, stavolta per evidenziare le differenze nelle priorità di mercato anziché in quelle tecnologiche (***fig.* 5**), emergono distinzioni consistenti fra le imprese che indicano la Sicurezza IT e le altre imprese rappresentate nel perimetro dell'indagine. In particolare, priorità come la conformità normativa, l'ingresso in nuovi mercati e la necessità di migliorare la produttività del lavoro sono le dimensioni che più spesso si stagliano nel confronto tra i raggruppamenti (rispettivamente, 39% nel gruppo Sicurezza IT rispetto al 22% del gruppo generale, 27% rispetto al 9%, e 42% contro 21%). Questi elementi vanno ulteriormente ad aggiungersi al quadro che si tratteggiava nel paragrafo precedente, ovvero quello di un gruppo di imprese che stanno attraversando una fase di trasformazione non soltanto tecnologica, ma una vero e proprio riposizionamento sul mercato, molto spesso accompagnato anche dallo sviluppo di nuovi prodotti e servizi (36% delle imprese del gruppo Sicurezza IT).

Figura 5 - *Influenza della Sicurezza IT nell'orientamento delle priorità di mercato delle imprese italiane. Fonte: IDC, 2018 (campione n=398, imprese con oltre 10 addetti; estrapolazione all'universo basata su modello di analisi territoriale)*

La Sicurezza IT come fattore abilitante per i nuovi paradigmi tecnologici e regolamentari

Nelle scorse edizioni si era evidenziato il grado di associazione tra spending in Sicurezza IT, da un parte, e progettualità relative alle tecnologie della Terza Piattaforma oppure ai modelli di Digital Transformation, dall'altra. Nell'edizione di quest'anno, oltre alle tendenze della spesa e al valore specifico nella pianificazione strategica delle imprese italiane, IDC ha approfondito quali sono i fattori esogeni che stanno esercitando una influenza determinante sulla Sicurezza IT soffermandosi in modo particolare su due argomenti centrali per il 2018: IoT e GDPR.

Come evidenziato nei paragrafi iniziali, spingendosi a un livello logico sempre più basso, le nuove strategie di attacco assumono una portata ancora più generale, influenzando potenzialmente qualsiasi impresa in qualsiasi settore. Se a tale macroscopica espansione dell'impatto potenziale, aggiungiamo gli innumerevoli sforzi che le imprese europee stanno portan-

do avanti per muovere concretamente i primi passi su paradigmi come l'Internet delle Cose e l'Industria 4.0, è facile comprendere come il rischio IT stia assumendo una dimensione che sta diventando via via gigantesca, soprattutto nel momento in cui l'IoT diventasse davvero l'infrastruttura più comune nei sistemi industriali occidentali, prefigurando scenari in cui uno zero-day potrebbe avere sostanziali ripercussioni sul PIL di una nazione. I nuovi indirizzi di politica industriale per l'Industria 4.0 proseguiranno il proprio corso anche nel 2018, aprendo diverse opportunità di investimento IT in Italia.
Esaminando il dato delle prospettive di spesa 2018 all'interno del gruppo di imprese che evidenziano una progettualità specifica sui paradigmi IoT e/o Industry 4.0 (***fig. 6***), è possibile formulare alcune valutazioni sull'impatto che questi nuovi modelli di gestione della produzione potrebbero avere sul mercato della Sicurezza IT in Italia. Quanto emerge dai dati raccolti conferma una influenza potenzialmente positiva, soprattutto nel segmento di imprese che prevedono di investire nella Sicurezza un budget rate compreso tra l'1 e il 3% del budget IT: infatti, se tale dato è pari al 24% nel campione generale, nel gruppo delle imprese con orientamento progettuale su IoT e/o Industry 4.0 lo stesso dato raggiunge il 38%, mentre è significativamente inferiore nel segmento di quanti spendono assai meno, fino all'1% del budget IT (30% nel campione, soltanto 14% nel gruppo). Lo sparuto gruppo di imprese che guarda verso l'IoT e/o l'Industry 4.0 sono perfettamente consapevoli delle sfide da affrontare per muovere concretamente i primi passi in quella direzione e comprendono il ruolo strategico della Sicurezza IT nella realizzazione dei nuovi modelli.

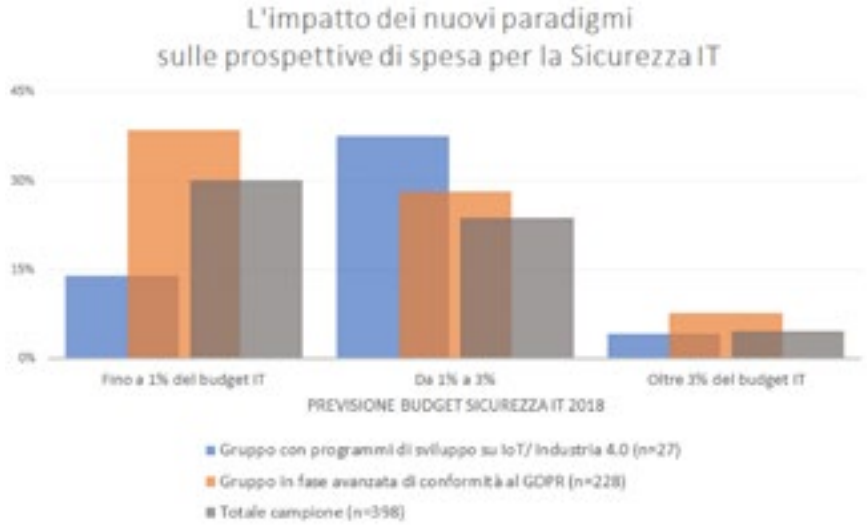


Figura 6 - *Impatto di IoT e GDPR nelle prospettive di spesa per la Sicurezza IT nel 2018. Fonte: IDC, 2018 (campione n=398, imprese con oltre 10 addetti; estrapolazione all'universo basata su modello di analisi territoriale)*

Un ulteriore fattore che inciderà in misura potenzialmente significativa sul mercato della Sicurezza IT è dato dalla conclusione del periodo transitorio per la conformità al GDPR: a partire dal 25 maggio 2018, tutte le imprese che gestiscono dati di cittadini europei dovranno dimostrare di avere implementato nel miglior modo possibile i nuovi principi di tutela previsti dal regolamento europeo, altrimenti rischieranno di incorrere nelle onerose sanzioni previste dalle norme. Si tratterà di un momento di transizione importante, non soltanto a livello tecnologico e organizzativo, laddove sarà necessario realizzare investimenti appositi per rispondere ai dettami del regolamento, ma soprattutto a livello culturale, perché la sicurezza aziendale, da questione prettamente tecnica che difficilmente emergeva al di fuori del dipartimento IT, diventerà a tutti effetti un rischio aziendale, e in alcuni contesti uno dei più importanti.

Il GDPR potrebbe rappresentare un fattore essenziale per aprire nuove prerogative di spesa e dare maggiore spazio alla Sicurezza nell'ambito del budget IT delle imprese italiane. Sempre in ***fig. 6*** viene rappresentato il budget rate delle imprese italiane destinato alla Sicurezza IT tra le imprese italiane che dichiarano di trovarsi in uno stato avanzato di adeguamento al GDPR. Quale che sia il segmento di intensità di spesa, le imprese che hanno intrapreso un percorso di conformità al nuovo regolamento esprimono prospettive di spesa tendenzialmente superiori rispetto al dato generale del mercato italiano (nel segmento di spesa fino all'1% del budget IT sono pari al 39% contro un dato generale del 30%; nel segmento di spesa tra 1 e 3% la percentuale raggiunge il 28% contro un 24% in generale; nel terzo segmento dove la spesa supera il 3% quasi si doppia il dato generale del mercato, 8% contro 5%). Dai dati emerge un quadro di evidenze positive: la necessità improrogabile di rispondere al GDPR potrebbe indurre molte imprese italiane a investire con rinnovato vigore nel 2018.

INDUSTRY 4.0: La nuova frontiera dei cyber criminali nell'anno del GDPR.

[A cura di Michele Onorato, Hitachi Systems CBT]

Il mercato industriale è in forte evoluzione: gli impianti produttivi sono sempre più digitali e interconnessi, si avvalgono dei big data per analizzare i dati e avere una visione da diverse prospettive: ciò permette al top management delle aziende di definire le strategie in modo più rapido, agile e appropriato. Si parla, a tal proposito, di quarta rivoluzione industriale, sostenuta da un piano Industry 4.0, che porterà a una produzione industriale sempre più automatizzata ed efficiente, grazie all'interconnessione dei sistemi produttivi e dei prodotti stessi.
Secondo un rapporto della multinazionale di consulenza McKinsey le nuove tecnologie digitali avranno un impatto profondo su quattro direttrici principali:

- disponibilità di potenza di calcolo e connettività per la centralizzazione delle informazioni;
- sviluppo di soluzioni di machine learning per "apprendere" dai dati raccolti nel tempo;
- miglioramento delle prestazioni lavorative superando le barriere tra uomo e macchine, tramite interfacce "touch" o realtà aumentata;
- interazione machine-to-machine (robotica) che permetterà di razionalizzare i costi e migliorare le prestazioni.

Essendo l'Italia il secondo paese manifatturiero in Europa, ciò provocherà un profondo cambiamento nel nostro paese, sia per quanto riguarda le infrastrutture cosiddette critiche sia per quelle di produzione.
Pensare di affrontare tutti i temi di sicurezza dei sistemi industriali con lo stesso approccio e la stessa metodologia utilizzata fino a oggi in ambito IT (Information Technology) sarebbe un errore imperdonabile. In questo contesto, i principi fondamentali della cyber security forniscono un dato sicuro quando sono rispettati (nell'ordine) i criteri di Riservatezza, Integrità e Disponibilità. Viceversa, in ambiente OT (Operation Technology) l'ordine di importanza di questi tre fattori è esattamente l'opposto: le caratteristiche "irrinunciabili" sono la Disponibilità e l'Integrità, mentre la Riservatezza ha un ruolo, di solito, meno rilevante.
In un'azienda industriale, infatti, un sistema deve essere considerato "sempre acceso" e, a seconda dell'utilizzo più o meno critico, deve prevedere sistemi ridondati a caldo e tempi di ripartenza ridottissimi, come confermano autorevoli report internazionali[1].
L'integrità del dato può poi essere ottenuta solo adottando soluzioni pensate, disegnate e

[1] Survey Securing Industrial Control Systems-2017, Sans Institute. Link di riferimento https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

sviluppate tenendo in considerazione l'intero suo ciclo di vita. Inoltre, sono indispensabili la tracciabilità degli accessi e una precisa registrazione in caso di correzione o variazione dei dati stessi.
Infine, è ormai dimostrato che il semplice utilizzo di sistemi di sicurezza perimetrali pensati per le applicazioni web e IT tradizionali sia inefficace se portato nel mondo OT, in quanto non è agevole definire regole per le connessioni e il filtraggio dei dati che possano essere valide per i sistemi industriali: porte, protocolli e regole sono diverse e specifiche a seconda che si tratti di dispositivi collegati alla rete di impianto o di sistemi di controllo e telecontrollo.
Ne consegue quindi che per "fare security" in ambito industriale devono essere previste soluzioni e approcci mirati, da integrare a quanto già previsto per la cyber security aziendale. Specifiche devono essere anche le competenze richieste, per capire e quindi proteggere in modo adeguato le applicazioni OT in reti di automazione, controllo e telecontrollo dai rischi informatici nell'industria e nelle Infrastrutture Critiche.
L'Italia sta cercando oggi di contrastare il fenomeno dei cyber attacchi attraverso la creazione di nuove entità istituzionali che ostacolino i cyber-criminali anche attraverso alcuni strumenti quali il Piano Nazionale per la protezione cibernetica e la sicurezza informatica, pubblicato sulla Gazzetta Ufficiale del 31 Maggio 2017, che stabilisce la roadmap per l'adozione da parte dei soggetti pubblici e privati delle misure prioritarie per l'implementazione del Quadro Strategico Nazionale (QSN).

Situazione attuale

Il mondo industriale è sempre più colpito da attaccanti che intendono appropriarsi di informazioni strategiche e nel contempo creare problemi a infrastrutture critiche e impianti di produzione. Si leggono sempre più spesso notizie riferite ad attacchi industriali come quello subito da Renault e Nissan che, a maggio dello scorso anno, hanno visto fermarsi ben cinque impianti di produzione.

Figura 1 - *Notizia Evento Malevolo*

Attacchi di questo tipo non sono solo mirati al recupero di informazioni preziose, ma anche a creare disagi a infrastrutture critiche e, non ultimo, a minare l'incolumità dei cittadini. È molto interessante lo studio realizzato da alcuni ricercatori del Georgia Institute of Technology (GIT), i quali hanno creato un ransomware in un ambiente di laboratorio in grado di prendere il controllo di un impianto per il trattamento delle acque e di chiudere l'intera fornitura d'acqua di una città o avvelenare l'acqua stessa aumentando la quantità di cloro in essa contenuta.

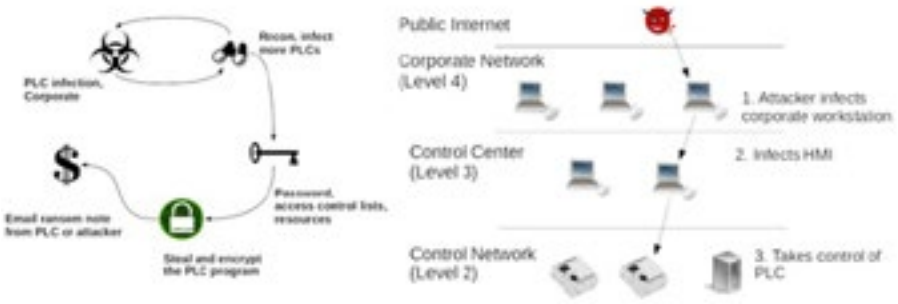


Figura 2 - *Simulazione Attacco (Fonte: Georgia Institute of Technology*[2]*)*

È sempre più evidente la necessità di utilizzare un approccio unico per la gestione dei propri impianti IT e OT anche perché molto spesso il mondo ICS (Industrial Control Systems) è colpito da attacchi che hanno sfruttato una vulnerabilità IT e che successivamente hanno impattato i sistemi SCADA (Supervisory Control And Data Acquisition).
Abbiamo chiesto a Talos, il gruppo di ricercatori in ambito sicurezza di Cisco Systems, di esprimere una loro opinione sui pericoli che oggi il mondo industriale deve affrontare. Secondo loro gli attacchi a sistemi ICS più facili da perpetrare sono quelli indirizzati contro una rete IT. Tali attacchi permettono di guadagnare l'accesso a una rete OT che solitamente non ha sistemi di sicurezza integrati e quindi di compiere delle azioni "lecite", quali l'invio di comandi legittimi, sui sistemi SCADA. Talos inoltre ci rammenta l'ultimo incidente in ambito ICS, denominato Crashoverride, che a fine 2016 in Ucraina ha permesso di inviare comandi per la disattivazione dell'elettricità per circa due ore in una grande città.
Oggi il mondo industriale sottovaluta il pericolo in cui incorre rispetto alla portata delle minacce a cui gli impianti sono sottoposti. Inoltre, le aziende molto spesso non sono a conoscenza di aver subito attacchi, per due motivi fondamentali:

- la mancanza di consapevolezza che i propri impianti industriali possano essere oggetto di attacchi informatici;

[2] Georgia Institute of Technology. http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls

- la mancanza di processi e soluzioni di sicurezza in ambito industriale.

Una ricerca del Sans Institute ha evidenziato che, nonostante la pubblicazione di un numero di incidenti sempre più alto in ambito OT, il livello di minaccia critico o moderato percepito dalle aziende nel 2017 è aumentato di poco rispetto al 2016.
La maggior parte degli intervistati non pensa che i propri sistemi siano stati sottoposti ad attacchi, specificando di non esserne a conoscenza. Ciò conferma che esiste una mancanza di consapevolezza dei rischi a cui gli asset aziendali sono sottoposti e che manca un approccio strutturato per valutare i rischi informatici o di altre categorie e la individuazione di misure di sicurezza da inserire all'interno della propria infrastruttura IT e degli impianti industriali in base alla criticità e al valore degli asset aziendali.
Aspetto non meno preoccupante è la dichiarazione del numero di incidenti che si sono verificati all'interno delle aziende. Una azienda su due ha avuto almeno un attacco durante l'ultimo anno e il 25% delle aziende colpite ne ha registrati dai tre ai cinque. È necessario quindi provvedere all'implementazione di soluzioni integrate che ci permettano di prevenire eventuali attacchi informatici, ma anche studiare nuovi strumenti che ci permettano di monitorare tutti i nostri asset.

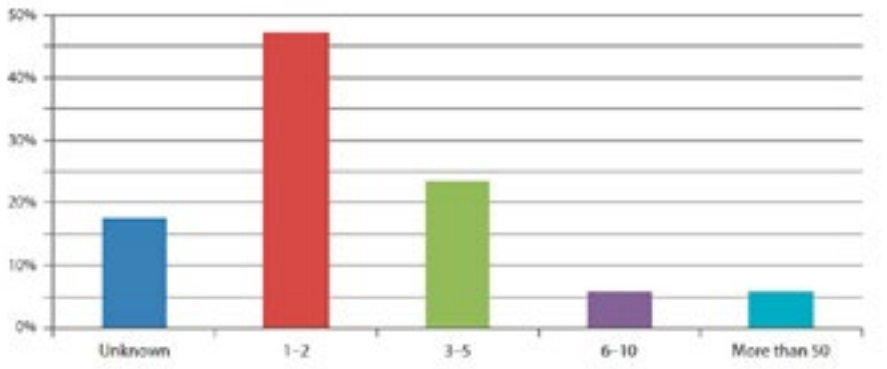


Figura 3 - *Numero di incidenti rilevati (Fonte: Sans Institute)*

Restano comunque ancora i dispositivi IT quelli considerati più a rischio e con maggiore impatto in termini di vulnerabilità anche se sta crescendo la consapevolezza che tutti i sistemi ICS corrono comunque un rischio importante con un impatto notevole, come mostrato nel grafico di **Figura 4**.

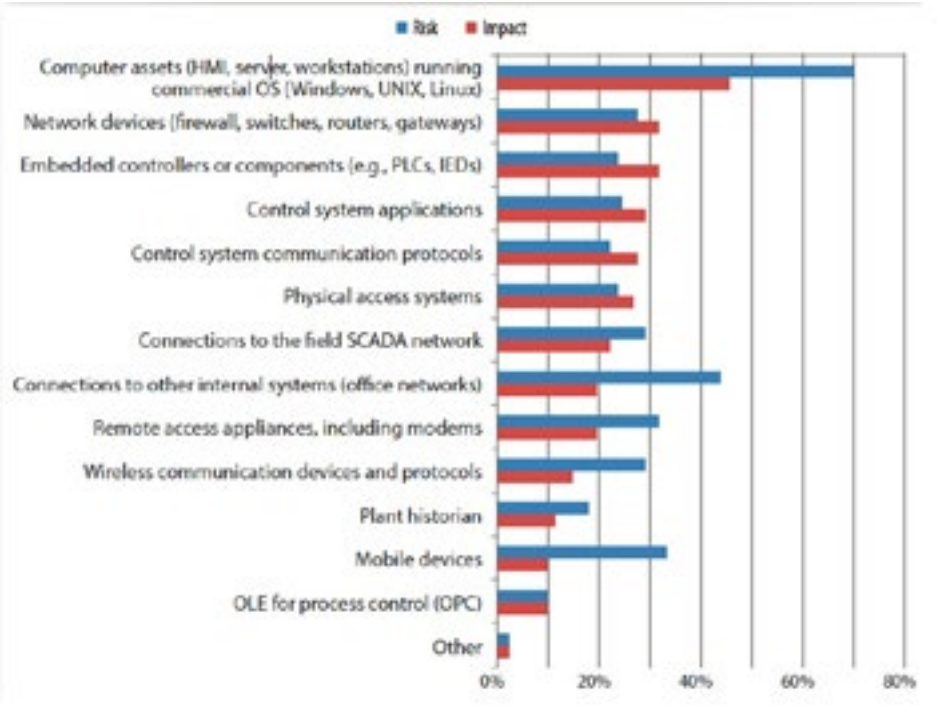


Figura 4 - *Percezione del rischio e dell'impatto sui propri asset (Fonte: Sans Institute)*

Ultimo aspetto interessante della ricerca effettuata dal Sans Institute è che il 46% degli intervistati dichiara di raccogliere informazioni sia dalla rete IT che da quella OT: perciò l'integrazione tra i due mondi sarà sempre più frequente e di conseguenza sempre più soggetta a nuove minacce e nuovi attacchi. Questo deve far riflettere le aziende sui rischi a cui sono soggette: bisogna lavorare su un approccio alla sicurezza strutturato e integrato che permetta di avere una visione globale della propria azienda e sapere quali siano le informazioni strategiche da proteggere e come tali informazioni fluiscano all'interno dei propri sistemi IT e OT. È fondamentale avere un approccio strutturato che coinvolga tutte le aree aziendali che vanno dal business all'IT a chi si occupa della gestione degli impianti industriali grazie all'utilizzo di un processo di Risk Management.

Le Minacce

Oggi c'è una ricerca sempre più attenta nel cercare vulnerabilità in ambito ICS: la criminalità ha infatti compreso che il recupero di informazioni e la creazione di disagi ad aziende industriali può essere molto fruttuoso. Tale attenzione, che è possibile riscontrare da numerosi report internazionali, riguarda anche i singoli elementi delle infrastrutture industriali, in quanto la ricerca delle vulnerabilità è ormai focalizzata anche al tipo di impatto che si intende apportare.

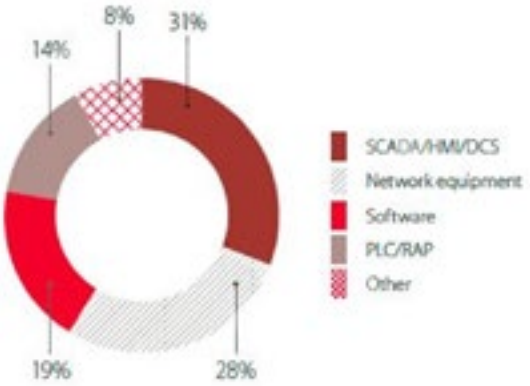


Figura 5 - *Vulnerabilità scoperte rispetto ai componenti (Fonte: Positive Technologies)*

Il dato più preoccupante è che, basandosi sul Common Vulnerability Scoring System (CVSS) versione 3 (first.org/cvss), la maggior parte delle vulnerabilità oggi note e maggiormente diffuse possono essere sfruttate senza disporre di competenze particolari e soprattutto che più della metà di tali vulnerabilità hanno un livello di rischio critico o alto, come mostrato nella figura successiva.

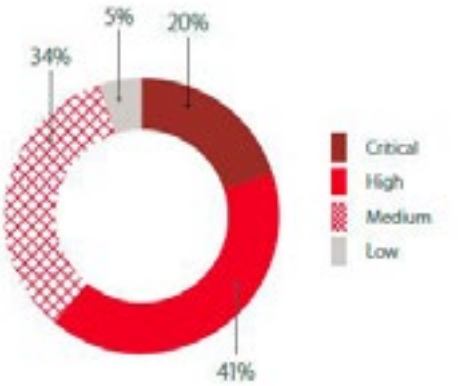


Figura 6 - *Livello di criticità delle vulnerabilità (Fonte: Positive Technologies)*

Una ricerca di Positive Technologies[3] ha rilevato 175.632 componenti ICS online utilizzando prevalentemente metodi passivi per raccogliere informazioni da fonti pubbliche quali Google, Shodan ecc. Ne risulta che il protocollo più utilizzato è HTTP e l'accesso a tali componenti può essere ottenuto attraverso l'utilizzo di password molto semplici.
Di seguito presentiamo la distribuzione geografica dei componenti rilevati: l'Italia risulta quinta, in linea con la diffusione delle tecnologie intelligenti in ambienti di produzione. Pertanto, è ragionevole sostenere che tale posizione crescerà con l'utilizzo del piano governativo Industry 4.0.

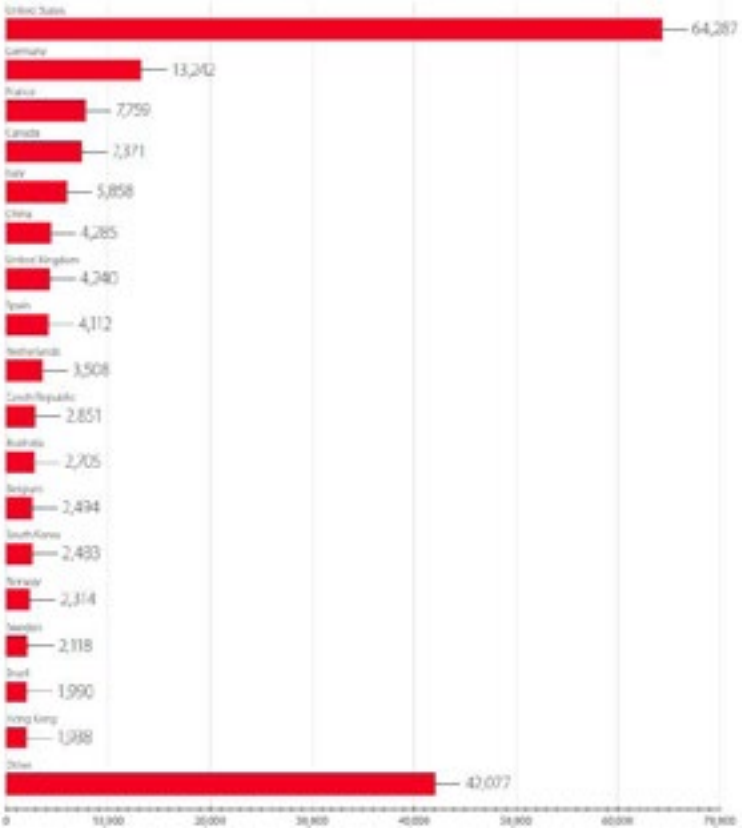


Figura 7 - *Distribuzione geografica degli elementi rilevati (Fonte: Positive Technologies)*

[3] ICS Security: 2017 in review, Positive Technologies
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-Security-2017-eng.pdf

E quindi?

Il settore industriale si sta concentrando sulla integrazione delle proprie reti IT e OT, ma ad oggi non è ancora sufficientemente percepito il rischio di tale integrazione e soprattutto non si è abbastanza consapevoli del fatto che la superficie degli attacchi informatici si stia ampliando.
È necessario pertanto intervenire ridefinendo l'approccio alla problematica, che vada oltre le competenze specifiche dei due mondi IT e OT, che ormai non viaggiano più su binari paralleli.

Ma la convergenza non è l'unica risposta da mettere in campo: vi sono tutta una serie di azioni per la sicurezza che anche il mondo IT, ritenuto tendenzialmente più maturo, fa ancora fatica a realizzare nelle aziende; ormai è imprescindibile che tali azioni siano implementate, e che lo si faccia in modo trasversale anche coinvolgendo il mondo OT.
Tra queste, la più importante è ripensare il modello organizzativo, attribuendo le responsabilità di sicurezza a un appropriato livello gerarchico che possa anche garantire la necessaria indipendenza decisionale rispetto alle specifiche esigenze dei responsabili dei settori IT e OT. Una figura che abbia la responsabilità della sicurezza dell'azienda, indipendentemente da dove e come essa si eserciti, può costituire un trait d'union che oggi serve per accelerare un approccio convergente.
In secondo luogo, è necessario implementare un processo di Risk Management che preveda come attori il business, l'Information Technology e le operation industriali; orientare la gestione della sicurezza sulla base dei rischi è fondamentale per potersi adeguare alle nuove compliance europee (GDPR, NIS, …), in vigore proprio da questo anno. Una necessità evidenziata anche dai report internazionali, che illustrano uno scenario in cui sui sistemi OT non sono applicati i criteri di sicurezza di livello minimo per la protezione dei sistemi industriali, in quanto non c'è consapevolezza dei rischi a cui si è soggetti dalla fase di progettazione fino all'implementazione e all'esercizio dell'impianto industriale. L'orientamento *risk based* deve essere pertanto esteso a tutti gli attori che partecipano alla progettazione, al disegno, all'implementazione e alla maintenance di impianti e relativi sistemi di protezione. Ciò introduce l'azione successiva: adottare criteri di protezione *by design:* gran parte delle aziende ne parlano solo da qualche mese grazie al nuovo regolamento europeo sulla privacy (GDPR).
Infine, l'ultimo intervento che si ritiene prioritario è quello relativo al monitoraggio della sicurezza, integrando e correlando le fonti di informazioni dei mondi IT e OT, per essere costantemente a conoscenza dello stato dei propri asset e per individuare e mettere in campo le giuste azioni a fronte di un attacco. È ormai dimostrato ampiamente come la capacità di reagire tempestivamente a una violazione possa minimizzarne in modo significativo le conseguenze. La complessità, in questo caso, sta nel riuscire a interpretare correttamente i diversi "idiomi" degli apparati che forniscono informazioni sullo stato dei sistemi IT e OT.

Di nuovo, passare da un approccio "settoriale" a un modello convergente non è una scelta, è una necessità!

Maritime e Sicurezza IT

[A cura di Andrea Vallavanti]

La convergenza tra il mondo della Marina Mercantile e la sicurezza IT trova la sua naturale evoluzione nello sviluppo tecnologico degli ultimi decenni. Se valutiamo a ritroso il mondo Maritime in ottica anni 90, inizio terzo millennio, la distanza era siderale e il concetto stesso di sicurezza Informatica non aveva apparentemente ragione di esistere. Le funzionalità erano rilegate a collegamenti Satellitari e Radio, funzionali in primo luogo alla sicurezza della navigazione (sistemi GMDSS Global Marine Distress and Safety System) e alla sporadica funzione propria dei collegamenti Satellitari, volti alla trasmissione voce e segnalazioni automatiche via Telex. Lo sviluppo di connessioni aderenti alle necessità di navigazione, con costi che potessero giustificarne la presenza a bordo, ha modificato il paradigma di costo beneficio e ha portato a una massificazione delle connettività verso terra, ormai imprescindibile a livello business. A tale evoluzione ha contribuito anche la crescente richiesta di connessione ad internet, giunta sia dal personale marittimo che dai clienti in ambito croceristico.
L'IT in ambito Marittimo impone oggi un cambio di approccio manageriale e filosofico rilevante. Il governo di sistemi installati a bordo nave, grazie alla informatizzazione spinta, consente una valutazione da remoto di sistemi specifici (quali Sistemi di Navigazione, Manovra, Sala Macchine, Generatori di propulsione e Generatori elettrici) nei quali l'aspetto manutentivo – e il relativo costo – può essere mitigato da azioni e analisi effettuate da terra.

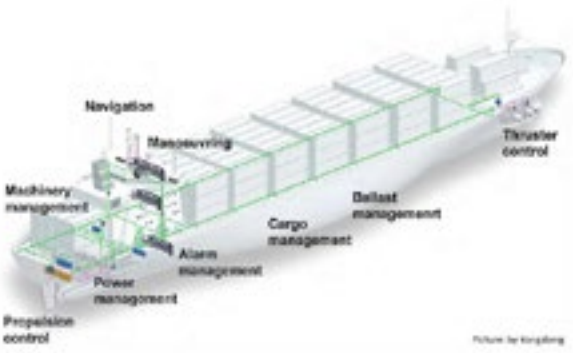


Figura 1

Non solo il fattore manutentivo concorre ad una vulnerabilità intrinseca, ma anche il personale specializzato o dedicato ai singoli sistemi può essere un veicolo di attacco. In **Figura 2** sono esemplificate le relazioni tra i vari sistemi, il personale addetto e il flusso dati da e verso l'esterno, necessario alla gestione della nave, ad esempio in porto.

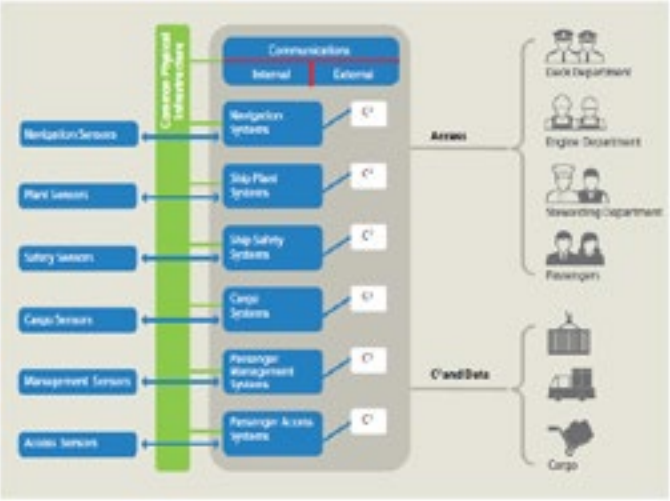


Figura 2

Il mondo Maritime è entrato nell'occhio del ciclone degli attacchi hacker

Secondo l'IBM Cyber security Intelligence Index il settore trasporti è stato il sesto maggior colpito da attacchi. [1]

Nel 2010, alcune trivellatrici nella Corea del Sud hanno subito danni tali da impedirne l'utilizzo per giorni. Nello stesso anno una piattaforma petrolifera è stata chiusa per mancanza di personale specialistico IT. [2]

Nel 2011 alcuni hacker sono riusciti a penetrare server della IRISL (Iranian Shipping Line) danneggiando dati riguardo il carico, dati di delivery e posizione. Molta merce è stata consegnata in porti errati. [2]

Nel 2013 alcuni hacker sono riusciti a compromettere il sistema di una nave controllata dalla Australian Custom and Border Protection Service, con l'intento di capire quali container erano sotto il controllo della polizia e valutare posti sicuri di scarico merci. [2]

Nello stesso anno anche il porto di Anversa, colpito da un APT, ha visto l'azione di un gruppo di malviventi che sono riusciti a consegnare container a camionisti di loro conoscenza, cancellando le informazioni di contrabbando dai DB. Le autorità locali erano all'oscuro di tutto, fino al sequestro di tonnellate di cocaina, armi e una valigetta con 1,3 milioni di €. [2]

L'attacco alla Moller MARESK

Venendo agli ultimi anni, particolare risonanza ha avuto, nel giugno 2017, l'attacco alla Moller MARESK [3]. Maersk A.P. Møller - Mærsk, nota anche come Maersk, è un gruppo danese, che ha attività in diversi settori: principalmente trasporto marittimo (Maersk Line), energia e cantieristico navale. È il più grande armatore di navi mercantili nel mondo dal

1996. Ha sede a Copenaghen con filiali e uffici in più di 135 nazioni e 108.000 dipendenti, con operatività su 343 porti serviti in 121 paesi con trade ogni 15'.
Maersk è stata vittima del ransomware Notpetya. La consapevolezza dell'attacco non è stata immediata e ha avuto impatti su diversi porti dislocati nel mondo. (Stati Uniti, India Spagna e Olanda). Le ripercussioni hanno impattato sulla gestione portuale nella movimentazione merci e nel secondo quadrimestre la società ha messo a bilancio perdite tra i 200 e 300 milioni di $. Se pensiamo che il 18% del trade dei container a livello mondiale è gestito da questo colosso del mare, le cifre possono essere ragionevoli. L'impatto sulle perdite a bilancio ha un effetto immediato sugli shareholder e sulla credibilità del Brand. L'attacco ha però posto l'accento sulla vulnerabilità del trasposto via mare e dei porti. Ogni giorno milioni di container vengono stipati in navi e trasferiti in porti di mezzo mondo. Le informazioni viaggiano in parallelo alle merci per l'opportuna localizzazione. È corretto quindi affermare che il sistema informatico è paragonabile al sistema nervoso: messo fuori uso perdiamo il controllo della periferia, impedendo la logica gestione delle merci ad esso collegate e il relativo margine di guadagno sul business indotto.

La divulgazione di un attacco è fondamentale per fare fronte comune agli attacchi informatici

L'effetto disclosure sugli attacchi subiti risulta essere, anche nel settore marittimo, un punto di conoscenza basilare per far fronte comune a questa "battaglia" quotidiana. Spesso le compagnie Navali ritengono opportuno celare un attacco al fine di mantenere intatta la loro reputazione. La stessa reputazione che viene ritenuta ponderalmente più importante del denaro perso nel corso dell'attacco. Questo è un primo punto sul quale porre la dovuta attenzione, agendo a livello di organismi marittimi competenti, affinché le banche dati sugli attacchi informatici possano essere disponibili come base di analisi del fenomeno.
La Disclosure è stata anche veicolata da notizie che hanno posto la dovuta attenzione a questo settore commerciale. Di seguito alcuni esempi tratti da siti web esteri:
The Security Threat On Your Desk: November 3, 2013 by EditorialBy Rich Madden, Cyber-security issues onboard your typical merchant vessel would seem to be fall into one of two categories - acts of omission or criminal intent. Acts of omission are those errors that we make ourselves that might leave us open to nefarious deeds. Criminal intent is pretty self-explanatory. For whatever the gain - financial, social or security-wise -… [4]
All At Sea: Global Shipping Fleet Exposed To Hacking Threat: April 24, 2014 by ReutersBy Jeremy Wagstaff SINGAPORE, April 24 (Reuters) - The next hacker playground: the open seas - and the oil tankers and container vessels that ship 90 percent of the goods moved around the planet. In this internet age, as more devices are hooked up online, so they become more vulnerable to attack. As industries like maritime and energy connect ships, containers and rigs to … [5]
IMB: Shipping Is 'Next Playground for Hackers': August 21, 2014 by gCaptain The International Maritime Bureau is warning that the global shipping and supply chain could become the ‹next playground for hackers› and is calling on the maritime sector to remain

vigilant amid an increased threat of cyber-attacks. "Recent events have shown that systems managing the movement of goods need to be strengthened against the threat of … [6]

Global Shipping Feels Fallout from Maersk Cyber Attack: June 29, 2017 by ReutersBy Jonathan Saul LONDON, June 29 (Reuters) - Global shipping is still feeling the effects of a cyberattack that hit A.P. Moller-Maersk two days ago, showing the scale of the damage a computer virus can unleash on the technology dependent and inter-connected industry. About 90 percent of world trade is transported by sea, with ships and ports acting as the arteries of the …[7]

Cyber Hackers – Editorial, What Shipping Must Learn From Maersk Cyberattack: July 3, 2017 by The LoadstarBy Alex Lennane (TheLoadstar) The shipping industry must learn from last week's cyberattack on Maersk, say analysts, and the line's chief commercial officer, Vincent Clerc, said the line would "have to ask ourselves some tough questions". Speaking to CNN, Mr Clerc said the company had focused on trying to restore normal operations, but as the … [8]

Maritime Wakes Up To Security Risks: July 6, 2017 by gCaptain Security is the Achilles' heel of connected technology. In the maritime space, cyber risks conflate with vessel safety making a multifaceted response essential, says Inmarsat Maritime security head Peter Broadhurst Today an estimated 30,000 vessels globally have some sort of access to always-on Internet via satellite. [9]

New UK Code Requires Tighter Security Against Cyber Attacks on Ships: September 14, 2017 by The LoadstarBy Alexander Whiteman (The Loadstar) - In response to the growing threat of cybercrime to the shipping sector, the UK government has launched a new code of practice to help shipowners improve security. There are also concerns that vessels with insufficient protection against cyber-attacks could be arrested. [10]

Rising Hacker Threat Seen Triggering Boom in Cyber Crime Insurance: October 4, 2017 by Reuters COPENHAGEN, Oct 3 (Reuters) - Insurer Tryg expects 90 percent of its corporate customers to buy cybercrime insurance within five years as the threat from hackers and viruses to crucial data and IT systems grows. Tryg, Denmark's biggest insurer, has sold 5,000 cybercrime insurance policies since the turn of the year when it launched a new product … [11]

Inmarsat Shipboard Communication Platform Found Vulnerable to Hacking: October 27, 2017 by gCaptain Seattle-based cybersecurity firm IOActive has uncovered what it describes as critical security flaws in one of Inmarsat's shipboard communication platforms that could leave the platform and vessels' networks vulnerable to remote hackers. [12]

UK Shipping Firm Clarkson Falls Victim to Cyber Attac: November 29, 2017 by Reuters British shipping services provider Clarkson Plc on Wednesday said it was the victim of a cyber security hack and warned that the person or persons behind the attack may release some data shortly. The company's disclosure, while a relatively rare event in Britain, follows a series of high-profile hacks in corporate America. [13]

Il fattore umano riveste una grande rilevanza

Futurenautics evidenzia una "wake up call" del settore Maritime nell'ambito It security [14]. La stessa survey evidenzia che solo il 12 % degli equipaggi ha ricevuto qualsivoglia forma di training nel campo della cyber security. Se caliamo tali percentuali in ambito Italiano (con un indotto marittimo di 350.000 unità di cui 185.000 occupati direttamente in attività naviganti) avremo solo 22.000 persone con nozioni base di cyber security. Sempre sulla base di queste statistiche, calate a livello mondiale, solo il 43% degli equipaggi hanno nozione di cyber safe policy o cyber guidelines fornite dalle proprie compagnie di navigazione. Non sarebbe poi così improbabile pensare che, quel 57% rimanente (ovvero quello privo di qualsiasi nozione) possa essere un veicolo privilegiato di attacco. Le motivazioni sono conosciute agli addetti ai lavori: software obsoleti o privi di qualsiasi basilare patch, errori umani, mancanza di conoscenza (e di training di base), mancanza di un approccio top down del management alle problematiche di IT security. Aggiungiamo la naturale sofisticazione dei sistemi, che impone un imprescindibile salto tecnologico del personale di bordo. L'evidenza che il fattore umano riveste uno dei pilastri da dove costruire una "cyber security culture" di base, deriva anche dalla promiscuità lavorativa del personale durante le lunghe tratte. Tale promiscuità si manifesta nella condivisione di supporti (USB keys o HDD portatili) con varie tipologie di file. File di varia natura, talvolta, sono il veicolo più consono nello share "informativo" e informatico tra gli addetti ai lavori, il che porta irrimediabilmente alla diffusione di malware e virus sui device personali. Utilizzare una USB key dal proprio laptop alla rete di bordo per motivi lavorativi può essere logico se, a monte, esistono sistemi attivi di analisi del device esterno e/o politiche e norme ferree sull'uso di tali device. Il fattore umano, come driver di infezioni, è evidente e l'investimento sulla informatizzazione di base dei dipendenti, di qualsiasi grado o mansione, deve essere oggetto di valutazione approfondita da parte delle società Armatrici, che devono considerarlo come investimento necessario anche in ottica di ROI (Return on Investment).
Chi investe ha un impatto aziendale, per esempio dei ransomware, ridotto del 50 – 60 %.

Danno economico e di reputazione sono i principali driver di una presa di coscienza nel mondo Marittimo

La presa di coscienza dei rischi derivanti dall'utilizzo dell'IT si è trasferita nei contratti di noleggio con la clausola OFF HIRE [15]. La nave è da considerarsi OFF HIRE laddove risulti non atta a performare il servizio richiesto. Applicata tale clausola e valutato il concetto di performance, a fronte di un attacco hacker che limiti l'utilizzo dei servizi, è possibile sospendere il pagamento del noleggio per il tempo perduto causato dall'evento. La performance della nave viene valutata non solo nel contesto meccanico manutentivo in genere, ma come entità connessa al mondo IT e, pertanto, affidabile anche in questo ambito. La mancata protezione di una nave su un evento cyber potrebbe quindi essere considerata come un mancato esercizio della dovuta diligenza nel rendere la nave idonea alla navigazione, e anche una violazione degli Articoli 3 e 4 delle Regole dell'Aja/Aja-Visby [16], tale da poter condurre ad un reclamo ai sensi di una polizza di carico o di un contratto di noleggio.

Riguardo deve essere inoltre prestato al Codice ISM (International Safety Management) [17], che stabilisce gli standard previsti per la gestione in sicurezza della nave. Né il codice ISM né il Codice ISPS (Codice internazionale per la sicurezza delle navi e degli impianti portuali) [18] affrontano specificamente il tema cyber. BIMCO (Baltic International Maritime Council, la più grande associazione di armatori a livello mondiale con una copertura del 65% del tonnellaggio mondiale) [19] ha proposto che i Codici ISM e ISPS usino le loro procedure di rapida diffusione per far fronte ai rischi connessi ad eventi cyber. Nel gennaio 2016, BIMCO ha pubblicato le linee guida per migliorare la sicurezza informatica a bordo delle navi.

THE GUIDELINE ON CYBERSECURITY ON BOARDS SHIP [20] con la collaborazione attiva di BIMCO, CLIA, INTERCARGO OCIMF e IUMI è il documento che traccia le basi di analisi sulla Cybersecurity nel mondo navale.

La valutazione prevede step di analisi che possono essere riassunti nei punti seguenti:
- Procedure dedicate alla sicurezza informatica
- Vulnerability assessment e penetration test con hacker etici
- Identificazione delle minacce e vulnerabilità;
- Analisi delle connessioni verso terra;
- Risk assessment interno coadiuvato da risk aseessment di terze parti
- Valutare il perimetro di pertinenza con protezioni informatiche adeguate;
- Analisi tecnica e procedurale
- Stabilire un piano di emergenza
- Stabilire un piano di riposta ad attacco hacker
- Prevedere un piano di ripristino funzionalità
- Investigare sulle motivazioni dell'attacco e sui danni subiti.

Il documento basa le sue fondamenta sul NIST framework (National Institute Of Stantard Technologies) [21], risulta completo ed esaustivo ed è una base solida per la valutazione della sicurezza informatica in ambito marino. Risulta utile ricordare, a questo punto, la convergenza fra sistemi IT e sistemi OT. Con questi acronimi intendiamo l'abbraccio fra l'information technology (l'informatica nel senso comune del termine) e l'Operation Technology (ovvero la tecnologia dedicata ai sistemi di bordo). In **Figura 3** sono esplicitate a blocchi le interazioni fra le connettività Radio e Satellitari disponibili, con le rispettive aree di pertinenza lavorativa (Bridge Vlan/rete ponte comando, Engine room Vlan/rete controllo propulsione, Admin Vlan/rete amministratore) da quella dedicata al personale marittimo (crew VLan).

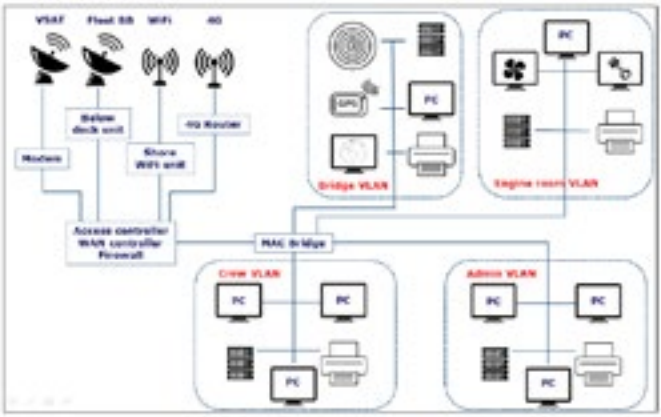


Figura 3

Conclusioni

Le acque si stanno muovendo. Investimenti dedicati alla Cybersecurity Marittima vedono la loro nascita coinvolgendo strutture istituzionali e Comunità Europea, con l'obiettivo di rafforzare la protezione degli scali seguendo good practice già attive in campo.
Se vogliamo declinare alcuni punti sui quali focalizzare la nostra attenzione potremmo riassumerli nei seguenti:

- Affrontare le tempeste Cyber necessita un forte impatto sugli shareholder, sulle società armatrici, sugli stakeolder e sui dipendenti
- L'alfabetizzazione Informatica non è più derogabile in relazione al rischio "Fattore Umano"
- La necessità di affidarsi a Standard disponibili & Good Practice
- La necessità di effettuare un Cyber Security Assessment (CSA)
- La necessità di Predisporre un Cyber Security Plan (CSP).

Se pensiamo ad un prossimo – non lontano – futuro, l'IOT (Internet of things) potrebbe rendere il sistema ancora più vulnerabile. In Italia Confitarma, l'associazione degli armatori, ha organizzato nel Maggio 2017 un seminario sulla Cybersicurezza nel cluster marittimo nazionale. Gli armatori hanno chiesto ai Ministeri dei Trasposrti e dell'interno di collaborare per contrastare la pirateria informatica, al pari della pirateria marittima. Un tavolo di discussione tra Guardia Costiera e Polizia Postale è di prossima attivazione per definire le procedure operative. È quantomeno curioso constatare che il concetto di Cybersecurity sia sempre stato associato a sistemi terrestri, e raramente ai relativi impatti in ambito marino. Non è più derogabile l'idea secondo la quale il mare aperto è un firewall naturale agli attacchi informatici. Non è più così.

Riferimenti

[1] https://www.ibm.com/security/infographics/data-breach/#scene2
[2] https://www.kaspersky.it/blog/maritime-cyber-security/6098/
[3] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#32bbc7874f9a
[4] http://gcaptain.com/cyber-security-threat/
[5] https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424
[6] http://gcaptain.com/imb-shipping-is-next-playground-for-hackers/
[7] https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE
[8] http://gcaptain.com/cyber-hackers-editorial-shipping-must-learn-maersk-cyberattack/
[9] http://gcaptain.com/maritime-wakes-security-risk/
[10] https://www.gov.uk/government/speeches/protecting-the-maritime-industry-from-cyber-attacks
[11] https://www.reuters.com/article/us-tryg-cyber/rising-hacker-threat-will-trigger-boom-in-cyber-crime-insurance-tryg-says-idUSKCN1C91MV
[12] http://gcaptain.com/inmarsat-shipboard-communication-platform-found-vulnerable-to-hacking/
[13] https://www.reuters.com/article/us-clarkson-cyber/uk-shipping-firm-clarkson-reports-cyber-attack-idUSKBN1DT1KO
[14] http://www.futurenautics.com/
[15] http://www.hfw.com/downloads/HFW-Il-rischio-di-attacchi-cyber-nel-settore-marittimo-settembre-2017.pdf
[16] http://www.hfw.com/downloads/HFW-Il-rischio-di-attacchi-cyber-nel-settore-marittimo-settembre-2017.pdf
[17] http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
[18] http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx
[19] https://www.bimco.org/
[20] http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16
[21] https://www.nist.gov/

Email security: i trend rilevati in Italia nel corso del 2017

[A cura di Rodolfo Saccani, Libraesva]

Introduzione

L'email è il principale canale di comunicazione per le aziende italiane, di conseguenza rappresenta il **primo canale** di diffusione di malware, phishing e attacchi informatici in generale.
Abbiamo aggregato e analizzato metriche su un flusso di oltre **10 miliardi di email** ricevute nel corso del 2017 in Italia. Un campione eterogeneo che offre uno spaccato rappresentativo del traffico email nel nostro paese: traffico di Internet Service Provider, Email Service Provider, aziende italiane di ogni dimensione, università, istituzioni.
Senza fornire un punto di vista troppo tecnico ci concentreremo su aspetti concreti, per i quali ciascuno può analizzare il proprio approccio in relazione all'email che, ricordiamo, veicola la quasi totalità delle minacce informatiche che ci raggiungono.

Il panorama italiano di email security nel 2017

L'**84%** del campione è rappresentato dalla posta indesiderata nel suo complesso (spam, malware, phishing, ..), valore che non si discosta particolarmente rispetto all'anno precedente. Quello che invece cambia è **la composizione** del traffico indesiderato: le componenti di **malware e phishing continuano a crescere** rispetto allo spam, consacrando la gestione della posta elettronica come un problema principalmente legato alla **security** piuttosto che alla produttività.
Se malware e spam si assomigliano molto per gli aspetti relativi alla trasmissione del messaggio poiché utilizzano **le stesse modalità e gli stessi canali** (principalmente botnet), differiscono notevolmente per gli aspetti legati al contenuto.
Nei paragrafi che seguono approfondiremo i trend più significativi del 2017, un anno che ci ha riservato diverse novità soprattutto in relazione all'evoluzione delle minacce e delle tecniche di distribuzione delle stesse.

1. Ransomware

Rispetto al 2016 la quantità di email veicolanti ransomware nel 2017 è **più che raddoppiata**: l'anno è terminato con un valore che si avvicina al triplo rispetto alla media di quello precedente. È la conseguenza della diffusione del **ransomware-as-a-service**, ovvero la disponibilità di servizi che consentono a "operatori" tecnicamente non esperti di condurre campagne di ransomware. Il "**terziario**" del ransomware, che ormai copre tutta la filiera, fornisce kit di sviluppo per realizzare il proprio attacco, servizi per l'invio di campagne email massive, servizi di "customer care" per guidare le vittime nella gestione della transazione economica attraverso criptovalute. Non sono più necessarie competenze specifiche per lan-

ciare una campagna di ransomware, questo spiega la rapida crescita del fenomeno.
Se nel 2016 avevamo osservato circa 100 nuove famiglie di ransomware che avevano dato origine ad alcune decine di migliaia di varianti (grazie ai kit di sviluppo un'unica famiglia genera molte varianti), nel 2017 questi numeri sono aumentati di circa il **20%**: più o meno 10 nuove famiglie ogni settimana.

2. Malware e latenze nell'identificazione di nuove varianti

Con l'espressione "**malware 0-day**" si fa riferimento a una nuova variante di malware (o un nuovo malware) che fino al giorno precedente non circolava. Nel paragrafo precedente abbiamo visto come nuove varianti appaiano **ogni giorno a decine** e come l'apparizione di una nuova famiglia di malware sia un'occorrenza ormai giornaliera.
Quando la difesa è affidata a sistemi basati su pattern o firme può esserci **una latenza** di alcuni giorni prima che una nuova famiglia o variante venga riconosciuta, in particolare se sfrutta una nuova metodologia di attacco. A titolo di esempio, quando a ottobre hanno iniziato a circolare campioni di ransomware che utilizzavano la funzionalità **DDE** all'interno di documenti Office, abbiamo visto susseguirsi una serie di varianti di questi attacchi che non venivano identificate dai sistemi antivirus. Per saggiare i tempi di reazione abbiamo realizzato una nuova inedita variante dimostrativa che non veniva riconosciuta da alcun antivirus, l'abbiamo pubblicizzata tra i vendor di security e pubblicata su VirusTotal. Dopo **quattro giorni solo due engine** antivirus la intercettavano.
Considerando che le nuove varianti sono **centinaia ogni giorno**, queste latenze non sono sostenibili. Il sandboxing basato su emulazione, nato come risposta a questo problema, si è scontrato nel corso dell'anno con un aumento del malware in grado di **evadere la detection** da parte delle sandbox (come il noto trojan bancario EMOTET, apparso nel settembre del 2017). Nel caso del sandboxing la latenza sta nel dover implementare nuove difese nei confronti delle nuove tecniche di evasione. Per dare un freno a questa eterna rincorsa tra attaccante e difensore è necessario un cambio di approccio e, come vedremo più avanti, è un concetto che comincia a maturare.

2.1 Distribuzione di malware attraverso file

Un'infezione di malware (ransomware, trojan bancario, cryptominer, etc) avviene abitualmente in più stadi. Il "primo stadio" è quello allegato alla mail e ha come obiettivo il bypassare i controlli di sicurezza ed essere eseguito dall'utente, per questo sono in crescita i tipi di file tra quelli che hanno più probabilità di essere confusi per un allegato legittimo: documenti Microsoft **Office** e documenti **PDF.** Questi due formati rappresentano circa il 50% degli allegati malevoli e circa l'80% dei veicoli di ransomware. Questi documenti contengono un "dropper", ovvero un software minimale che si occuperà di scaricare e installare il malware vero e proprio.
Complice la problematica affrontata nel paragrafo precedente, nel 2016 l'approccio **reattivo** basato su pattern ed emulazione ha ceduto progressivamente il passo a un approccio **proattivo:** sono apparse sandbox di nuova generazione basate su un approccio diverso e in

grado di "disarmare" i documenti che contengono il codice che abilita le funzioni di "dropper" (macro, javascript, oggetti incapsulati). Questa rimozione del codice avviene prima che la mail venga consegnata all'utente, il quale riceve un documento ancora fruibile ma senza la parte attiva in grado di eseguire azioni pericolose. Si tratta di una nuova strategia proattiva, più strutturale e decisamente promettente, che rende inefficaci gli attacchi **ancora non noti** togliendo agli autori del malware gli strumenti di cui necessitano per raggiungere il loro obiettivo.
Il principio è che i documenti contenenti codice che accede a internet o al filesystem, che invia comandi al computer dell'utente, che fa operazioni all'insaputa dello stesso, sono nella quasi totalità malevoli. Quelli legittimi rappresentano una **eccezione** che è corretto gestire in quanto tale al fine di minimizzare la **superficie d'attacco**.

2.2 Distribuzione di malware attraverso link

Il miglioramento delle tecniche di contrasto agli allegati malevoli porterà a un incremento della distribuzione di malware attraverso link contenuti nelle mail, trend già emerso nel corso del 2017. Il link contenuto nella mail nella maggior parte dei casi punta a un sito internet **compromesso** sul quale è depositato il malware o la pagina di phishing. Di norma la campagna di email parte immediatamente dopo la compromissione del sito e al momento della ricezione della mail il sito **non è ancora noto** come compromesso, rendendo più difficile intercettare la minaccia.
Abbiamo assistito, con una frequenza superiore rispetto agli anni precedenti, alla compromissione di account di **email marketing** poi utilizzati per diffondere malware e phishing. In alcuni di questi casi il malware stesso era distribuito dalla CDN (content delivery network) del fornitore stesso dei servizi di email marketing, senza neanche affidarsi a un sito esterno.
La difesa in questi casi passa principalmente attraverso servizi di "url sandboxing" la cui crescita registrata nel corso del 2017 proseguirà con ogni probabilità nel 2018. Il link contenuto nella mail viene **riscritto** prima della consegna della mail all'utente. Il link riscritto punta a un servizio in cloud che analizzerà il contenuto della pagina **al momento del click** (posticipare l'analisi offre grandi vantaggi in termini di rateo di riconoscimento). Se il link è sicuro l'utente vi viene automaticamente rediretto, altrimenti viene intercettato. La protezione della mail in questo casi si estende ai link in essa contenuti, posticipando l'analisi (basata non più solo sulla reputazione ma anche sul comportamento del sito di destinazione) al momento del click.

3. Phishing

Due sole categorie rappresentano oltre il 90% del phishing: la prima è legata alla monetizzazione **immediata** (phishing finanziario per il furto di credenziali bancarie o dati di carte di credito), la seconda categoria è legata alla monetizzazione **differita** attraverso furto di identità (acquisizione di credenziali di posta elettronica e di dati personali da rivendere).

Relativamente al phishing finanziario la novità del 2017 è l'apparizione di campagne particolarmente sofisticate attribuibili a soggetti italiani, di cui riportiamo due esempi:

- campagna che riproduce fedelmente il sito internet di Mediaworld (inclusa la riproduzione accurata del funzionamento del carrello degli acquisti) con l'obiettivo di acquisire di dati di carte di credito (**Figura 1**).
- campagna che riproduce fedelmente il sito di ING Direct in cui le credenziali fornite dall'utente vengono utilizzate per impersonare in tempo reale l'utente al fine di sottrarre fondi dal suo conto corrente. Alla vittima viene anche chiesto di inserire il codice presente nel messaggio di conferma ricevuto da ING per autorizzare definitivamente la transazione truffaldina (**Figura 2**).

Con particolare riferimento all'Italia, è il primo anno che rileviamo campagne di phishing realizzate con tale perizia, ospitate su servizi di hosting italiani e attribuibili ad attori italiani. La crescita del made-in-italy delle truffe online è quindi un trend prevedibile per il 2018.

Figura 1 - *Phishing MediaWorld (Fonte: Libra Esva)*

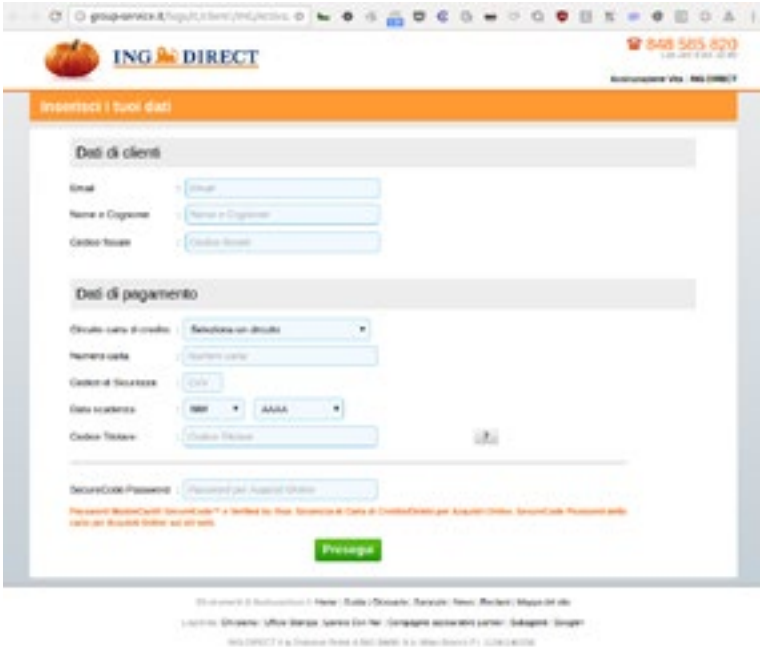


Figura 2 - *Phishing ING Direct Italia (Fonte: Libra Esva)*

Caratteristica particolare del nostro paese è una discreta **latenza** tra il momento in cui il phishing viene identificato e il momento in cui la campagna viene neutralizzata.
Problematiche di ordine **burocratico** vanno poi ad aggiungersi all'adozione da parte degli "attaccanti" di accorgimenti tecnici allo stato dell'arte volti a ritardare il takedown.

Citiamo un particolare caso in cui, dopo aver informato l'azienda relativamente alla clonazione del proprio sito, abbiamo rilevato con sorpresa che la contromisura adottata era stata quella di richiedere al proprio ufficio legale di redigere una diffida indirizzata a quello dell'operatore di hosting che ospitava, a sua insaputa, il sito di phishing. Un approccio complicato le cui tempistiche sono chiaramente incompatibili con la problematica di sicurezza. La latenza nella risposta a questi attacchi è dovuta alla mancanza, in aziende anche grandi, di **figure professionali specifiche**. Ancora oggi, chiedendo di parlare con un responsabile di IT security di un'azienda italiana per un'attività illecita in corso, non è inusuale che si venga messi in contatto con un ufficio legale.

Sul fronte tecnico, dal momento che un sito di phishing prima o poi viene scoperto e chiuso, sempre più spesso le campagne contengono un link a un sito intermedio che si limita a fare un **redirect** trasparente verso il sito di destinazione, il quale cambia ogni qualvolta il

precedente viene chiuso. Il link inserito nella mail quindi mantiene la sua efficacia per un tempo maggiore: il sito intermedio di norma viene scoperto e blacklistato più tardi. La URL sandboxing è la risposta che il mercato sta fornendo a questo tipo di attacco.
Altra tecnica adottata la fine di rendere più difficile l'identificazione delle mail di phishing è quella di inserire il link all'interno di un documento **pdf** allegato alla mail. Nel corso dell'anno questa tipologia di distribuzione di link malevoli è andata aumentando (+35%).
Il link nella mail quindi conduce la vittima a un sito web, che come abbiamo visto spesso viene analizzato da sistemi automatici come le url sandbox. La crescita dei sistemi automatici di rilevamento del phishing sulle pagine web, ha fatto crescere (+65%) il numero di siti malevoli che implementano forme di "**evasione**". Queste tecniche consistono solitamente in tentativi di **offuscamento** del codice html e javascript o di **crittografia** degli stessi. La presenza di queste contromisure, però, si sta rivelando un'arma a doppio taglio in quanto la presenza stessa di queste tecniche all'interno di una pagina web ne **rivela l'intento malevolo**, un po' come un malvivente che gira a volto coperto per non essere riconosciuto. L'evoluzione dei sistemi di rilevamento automatico delle frodi sta quindi seguendo anche questa strada.

Figura 3 - *Esempio di offuscamento del codice di una pagina web (Fonte: Libra Esva)*

4. Spearphishing

Gli esempi del paragrafo precedente appartengono alla categoria del phishing di massa, quella per cui il messaggio viene inviato a un **vasto pubblico** cercando di "pescare le vittime nel mucchio".
Una variante più sofisticata è lo spearphishing: un attacco **mirato** a una singola persona o a una specifica organizzazione. Abbiamo rilevato un incremento (+35%) degli attacchi diretti a una specifica organizzazione consistenti nella realizzazione di un finto portale di webmail

per raccogliere credenziali valide di posta elettronica.
È una tipologia di attacco, solitamente con finalità di **spionaggio** o **sabotaggio**, che da alcuni anni rileviamo con cadenza periodica nei confronti di organizzazioni come università o grandi aziende. Nel corso 2017 abbiamo constatato per la prima volta questo tipo di campagna nei confronti di bersagli **istituzionali**.


DocumentiOnLine - Nuovo documento

Ministero del Lavoro e delle Politiche Sociali (06/11/2017 6:55)

Gentile Cliente,
sono disponibili nuovi documenti nella sezione "DocumentiOnLine" del Suo Portale del Lavoro.

Per consultarli la invitiamo a copiare il link sottostante ed incollalo nella barra di navigazione del tuo browser.

https://microsoft.e-hec.space/office365/login-1/

Per ogni approfondimento La invitiamo a contattare il numero verde 800-001482.

A presto,
Il team Ministero del Lavoro e delle Politiche Sociali

Figura 4 - *Phishing indirizzato a organizzazioni istituzionali (Fonte: Libra Esva)*

All'inizio di Novembre alcune organizzazioni istituzionali hanno iniziato a ricevere mail di phishing che invitavano a cliccare su un link per accedere a un documento sul portale del Ministero del Lavoro. Il sito di phishing a cui puntava il link richiedeva l'inserimento delle credenziali di posta elettronica. Considerate le tempistiche, non è improbabile che questa campagna sia legata alla sottrazione di documenti istituzionali annunciata da **Anonymous** Italia verso la metà del mese di Novembre.

4.1 Whaling

Il whaling (propriamente "caccia alla balena") è un'ulteriore specializzazione dello spear-phishing che consiste nel contattare una persona interna all'azienda **spacciandosi per un dirigente** della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è **l'amministrazione** con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
Il caso della truffa di cinquecentomila euro a Confindustria verificatosi in Ottobre è un esempio di whaling che ha raggiunto la stampa generalista. La stessa tipologia di attacco, nel corso del 2017 si è diffusa nel nostro paese nei confronti di aziende di ogni dimensione.

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

di ROBERTO MANIA

Figura 5 - *Phishing a Confindustria*

Tra tutti, è questo il vero fenomeno emergente del 2017, con una crescita difficilmente quantificabile essendo un tipo di attacco estremamente raro durante il precedente anno e che nel 2017 si è propagato capillarmente in organizzazioni **di ogni dimensione**.

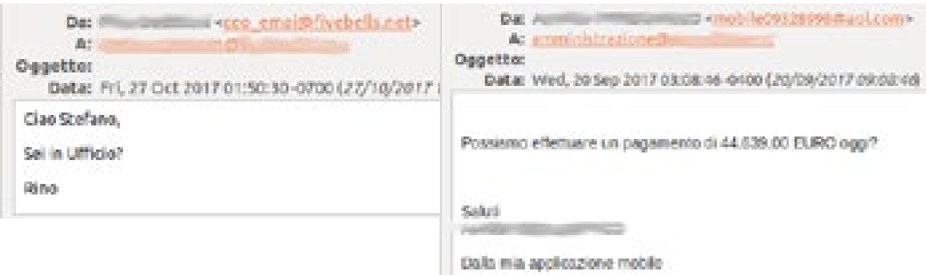


Figura 6 - *Tentativi di whaling:* **a**) *approccio iniziale e* **b**) *dopo uno scambio di messaggi (Fonte: Libra Esva)*

Generalmente "l'attaccante" conosce (direttamente o indirettamente) le persone coinvolte: il linguaggio utilizzato nei messaggi, infatti, ricalca quello delle conversazioni legittime. Di norma l'attacco inizia un una mail che sonda il terreno (**Figura 6a**) ("Sei in ufficio? Ho urgente bisogno di te"). Se il destinatario risponde, l'attaccante ha la conferma che la mail ha raggiunto il suo bersaglio il quale non si è accorto dell'inganno. A quel punto la conversazione prosegue e nel giro di qualche scambio (**Figura 6b**) si arriva a ordinare una **transazione economica** (di norma un bonifico).

Si tratta di un tipo di attacco estremamente difficile da intercettare per un sistema di email security in quanto le email tendono a essere brevi, prive di allegati o link, contenenti testo

che non si discosta dalle normali comunicazioni aziendali. Non è un caso che parte dell'attività lavorativa del sottoscritto nel corso del 2017 sia stata dedicata alla realizzazione di un motore di analisi del traffico specificamente progettato per intercettare tentativi di whaling.

5. Evoluzione delle tecniche di spamming

Le **botnet** composte da computer compromessi che vengono usati dai malviventi a insaputa dei proprietari, sono sempre più uno strumento utilizzato sia per l'invio delle campagne di spam che per la distribuzione del malware.
Due sono gli aspetti rilevanti che hanno caratterizzato il 2017: la crescita delle botnet basate su dispositivi della **Internet Of Things** e il progressivo cambiamento delle modalità di invio di email da parte dei "bot".
Tradizionalmente le mail di spam vengono inviate direttamente dal "bot" al mail server del destinatario. Durante lo scorso anno è divenuta prevalente una tecnica più efficace: il bot utilizza **account di posta legittimi** per inviare spam da service provider come gmail, office365, hotmail, etc. La posta proveniente da questi account legittimi ha una probabilità maggiore di transitare attraverso i sistemi di filtraggio dello spam.
I **centri di comando e controllo** che orchestrano i "bot", forniscono ai bot stessi elenchi sempre aggiornati di credenziali di posta da utilizzare a rotazione per l'invio delle mail. Le credenziali derivano da **campagne di phishing** e dagli ormai numerosi **database** trafugati che diventano di pubblico dominio e che contengono grandi quantità di username (di norma l'email) e password. Grazie al fatto che un gran numero di utenti **riutilizza la stessa password** su più servizi, moltissime credenziali presenti in questi database sono credenziali valide per accedere all'account di posta dell'utente. Il consiglio per evitare spiacevoli situazioni, è quello di non riutilizzare le password, avvalendosi eventualmente di un password manager.

Conclusioni

In conclusione, i trend più rilevanti da seguire nel 2018 sul fronte della difesa degli attacchi via email sono: gli engine per intercettare il Whaling, le sandbox di nuova generazione per disarmare il contenuto attivo degli allegati, le sandbox per l'analisi dinamica al momento del click delle URL contenute nelle mail.

In un certo senso questi due ultime elementi rappresentano una controtendenza rispetto all'evoluzione degli scorsi anni: l'analisi dei link web si fa dinamica per colmare le lacune dell'analisi basata sulla sola reputazione mentre l'analisi degli allegati cerca una risposta più strutturale al problema della continua evoluzione del malware puntando sulla riduzione della superficie d'attacco.

Attacchi e difese nel Cloud Computing nel 2017

[A cura di Andrea Piazza, Microsoft]

Nel corso del 2017 l'utilizzo del Cloud computing è aumentato significativamente anche in Italia. Lo confermano diversi studi, come quelli svolti da Sirmi[1] e dall'Osservatorio Cloud & ICT as a Service della School of Management del Politecnico di Milano[2].
Con l'accresciuto utilizzo, si sono regolarmente evolute le tipologie di minacce a cui sono state esposte le risorse nel Cloud, con modalità differenti a seconda del modello di Cloud Computing in uso. Oltre a portare attacchi alle risorse Cloud, gli attaccanti utilizzano sempre di più le risorse nel Cloud per sferrare attacchi verso le proprie vittime. Ad esempio, si stima conservativamente che almeno una macchina virtuale su 10000 sia parte di una qualche Botnet[3].

Nel report dello scorso anno relativo al 2016, ci siamo soffermati sulle principali tipologie di minacce a cui sono esposti i servizi cloud, le principali misure di rilevazione a disposizione, e le misure di protezione proattive che possono essere adottate per limitare le possibilità di successo degli attacchi più frequenti. A conferma di quanto evidenziato lo scorso anno, il 2017 ha portato all'onore delle cronache diversi data leak[4] in cui la protezione non appropriata di risorse nel cloud da parte di aziende che ne fanno uso ha portato all'esposizione di enormi moli di dati, spesso relativi ad aziende clienti delle aziende compromesse. Analogamente non sono mancati incidenti legati all'esposizione erronea su servizi come Github di credenziali[5], tanto è vero che nel 2017 è emerso un servizio (Gitleaks) che, in modo analogo a Shodan per gli strumenti IOT, aggrega le informazioni relative a credenziali esposte su Github.

Grazie al punto di osservazione privilegiato di Microsoft avevamo approfondito le statistiche 2016 relative agli alert generati sui clienti italiani ospitati in Azure. In questo focus-on siamo ora in grado di ampliare quella prima indagine in diverse direzioni:

- integrando le informazioni relative agli alert su Azure nell'ultimo quarto del 2017;
- ampliando l'analisi includendo le minacce rilevate da Office 365 Advanced Threat Protection nel secondo semestre del 2017;
- includendo le minacce rilevate dai sistemi antimalware Microsoft.

---

1 http://img.musvc2.net/static/83215/documenti/10/ListDocuments/Sirmi%20-%20Il%20mercato%20Cloud%20Computing.pdf

2 https://www.zerounoweb.it/cloud-computing/cloud-transformation-un-paas-per-il-futuro

3 https://azure.microsoft.com/en-us/blog/large-scale-analysis-of-dns-query-logs-reveals-botnets-in-the-cloud/

4 http://securityaffairs.co/wordpress/64150/data-breach/accenture-data-leak.html
https://www.upguard.com/breaches/verizon-cloud-leak
https://www.reddit.com/r/techsnap/comments/6i79yx/the_rnc_files_inside_the_largest_us_voter_data/

5 https://factordaily.com/tcs-employee-github-data-leak-jason-coulls/

Attacchi su Azure nel 2017

I dati qui descritti si riferiscono all'ultimo quarto del 2017. Si tratta di un campione di poco meno di 10000 alert, con una media di poco più di 100 alert al giorno. È importante sottolineare come gli alert si riferiscano sia ad attacchi verso i sistemi in Azure sia in uscita da essi.

I dati mostrano come:

- Quasi due terzi degli alert generati a fronte di attacchi su Azure faccia riferimento a comunicazioni DNS malevole. Si tratta in particolare di rilevazioni di client che tentano di comunicare con domini malevoli e canali di command&control. Il DNS viene spesso usato inoltre come canale per esfiltrare dati da sistemi compromessi, attraverso ad esempio il tunneling del traffico TCP attraverso l'infrastruttura DNS, oppure tramite server DNS custom in grado di interpretare messaggi DNS opportunamente codificati. Per un approfondimento sull'evoluzione delle modalità di detection di Azure Security Center basate sull'analisi delle query DNS, si rimanda all'articolo https://azure.microsoft.com/en-us/blog/large-scale-analysis-of-dns-query-logs-reveals-botnets-in-the-cloud.
- Circa il 30% degli attacchi rientra nella categoria Brute Force sui tradizionali protocolli di amministrazione (RDP ed SSH) e su SQL.
- Gli attacchi lato network, come DDoS lanciati a partire da sistemi ospitati in Azure e Port Sweeping (cioè la scansione di vari sistemi alla ricerca di una specifica porta in ascolto) rappresentano un sottoinsieme limitato degli attacchi complessivi, complessivamente intorno al 5%.

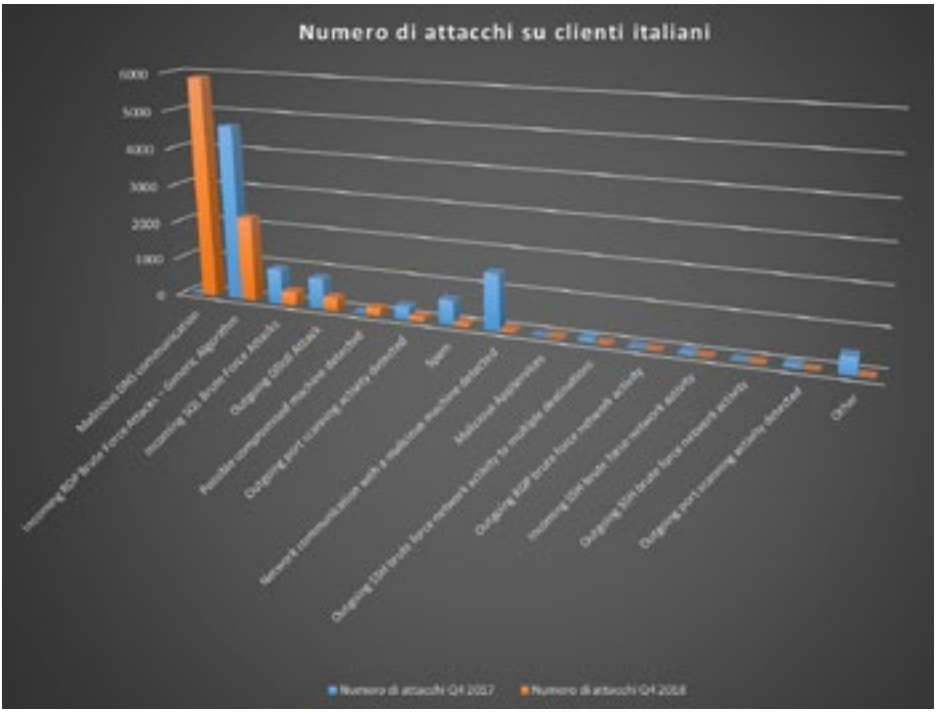
La tabella seguente fornisce il dettaglio del numero di alert generati per tipologia.

Alert Display Name	Number of attacks on Italy Q4 2017	Number of attacks on Italy Q4 2018
Malicious DNS communication	0	5886
Incoming RDP Brute Force Attacks – Generic Algorithm	3567	1144
Incoming RDP Brute Force network activity	1095	1107
Incoming SQL Brute Force Attacks	928	356
Outgoing DDoS Attack	814	340
Possible compromised machine detected	16	194
Outgoing port scanning activity detected	341	110
Spam	650	92
Network communication with a malicious machine detected	1479	54
Malicious AppServices	0	15
Outgoing SSH brute force network activity to multiple destinations	105	11
Outgoing RDP brute force network activity	34	7

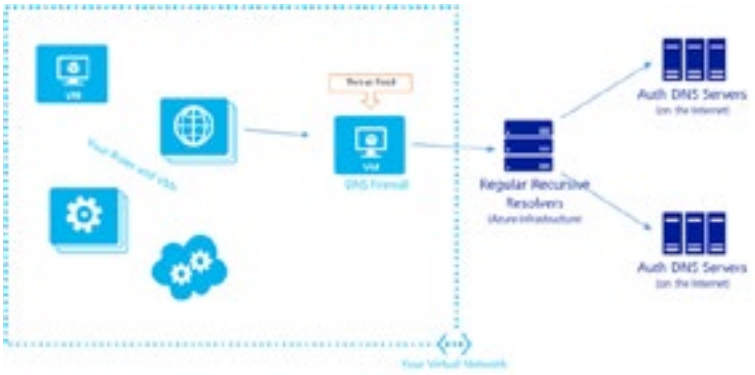
Incoming SSH brute force network activity	55	5
Outgoing SSH brute force network activity	21	5
Outgoing port scanning activity detected	83	1
Other	459	0

Trend

Il numero complessivo di alert rilevati nel Q4 2017 è rimasto del tutto analogo a quello dell'anno precedente, con poco meno di 10000 alert complessivi.
CI sono però variazioni molto significative nella tipologia di attacchi rilevati. Come mostra la figura seguente, il 2017 è stato caratterizzato dal predominio di attacchi relativi a comunicazioni malevole tramite DNS.
Trovano conferma, seppur in misura minore rispetto al 2016, gli attacchi brute force portati ai protocolli di amministrazione (RDP ed SSH) e a SQL.
Si nota infine una netta diminuzione del numero di attacchi di tipo Spam e DDoS in uscita da sistemi Azure.



A fronte di questi dati, ricordiamo che le misure principali per proteggere il traffico DNS ed individuare eventuale traffico malevolo consiste nell'utilizzo dei cosiddetti DNS Firewall, ovvero particolari server DNS che ispezionano le query DNS per individuare segnali di attività malware, generare alert e/o bloccare il traffico. Spesso un DNS firewall utilizza un feed di Threat Intelligence per restare aggiornato sull'evoluzione delle minacce. A livello di rete virtuale in Azure, è possibile aggiungere un firewall DNS dal Marketplace di Azure e inserirlo nella rete secondo l'architettura descritta nella figura seguente:



È infine consigliabile l'abilitazione di Azure Security Center e della componente DNS Analytics di Azure Log Analytics[6] per un monitoraggio continuo del traffico DNS.
Per la protezione dagli attacchi brute-force si rimanda al report dello scorso anno per quanto riguarda le best practice in materia, ricordando che anche questa tipologia di attacchi viene evidenziata attraverso l'abilitazione di Azure Security Center.
Per quanto riguarda la protezione dagli attacchi DDOS, oltre alle funzionalità di base incluse in Azure, sono disponibili sul mercato diverse opzioni sia Microsoft che di terze parti che consentono di aggiungere funzionalità avanzate di protezione[7].

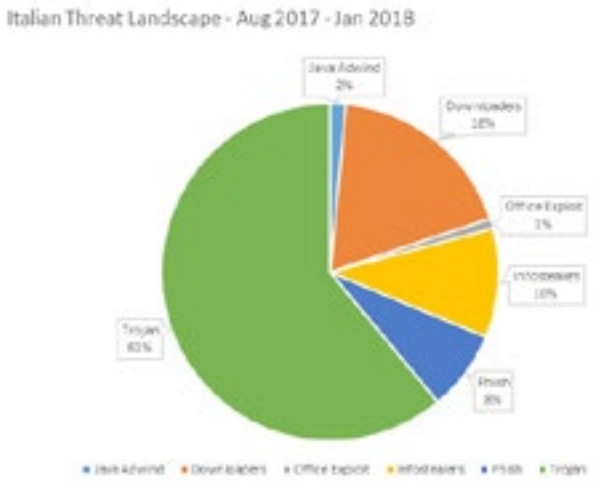
Attacchi su Office 365

Nonostante tutti i vendor di sicurezza cerchino di rispondere alle nuove minacce tramite il rilascio di nuove signature nei tempi più rapidi possibili, il numero di varianti di malware è tale che queste hanno tipicamente a disposizione diverse ore o talvolta giorni per compromettere dei sistemi prima di venire effettivamente rilevate. Nell'ambito della posta elettronica le minacce più tipiche sono rappresentate da allegati malevoli e da link a siti malevoli, che se aperti o raggiunti dall'utente portano alla compromissione del suo sistema.

6 https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-dns

7 https://azure.microsoft.com/en-us/blog/azure-ddos-protection-service-preview/

Office 365 ATP è lo strumento deputato alla protezione della posta elettronica dalle minacce più avanzate, attraverso l'utilizzo di tecnologie di detonation degli allegati e di analisi dei link che consentono di ridurre i tempi di rilevamento delle nuove varianti e di ridurre al minimo l'esposizione al rischio del paziente zero.
I dati seguenti mostrano quali siano, ad alto livello, le principali categorie di minacce rilevate da Office 365 ATP sui clienti italiani.



I dati coprono un arco temporale di 6 mesi, compreso tra agosto 2017 e gennaio 2018, ed evidenzia come oltre il 60% delle minacce rilevate dagli strumenti di protezione della posta elettronica rientri nella categoria dei Trojan. A questa categoria può essere aggiunta anche una minaccia specifica come Java Adwind, che presenta componenti di Trojan e Backdoor.
Al secondo posto in termini di prevalenza ritroviamo i cosiddetti Downloader, ovvero software deputati a scaricare ulteriori componenti malevole dopo l'infezione iniziale.
Troviamo poi i cosiddetti software Info Stealer, ovvero orientati a rubare informazioni all'utente compromesso.
Le mail di phishing rappresentano solo l'8% delle minacce rilevate.
In ultimo fanno la loro comparsa gli exploit, in particolare quelli legati ad Office, minacce che cercano di sfruttare vulnerabilità di prodotto per compromettere il destinatario del messaggio.

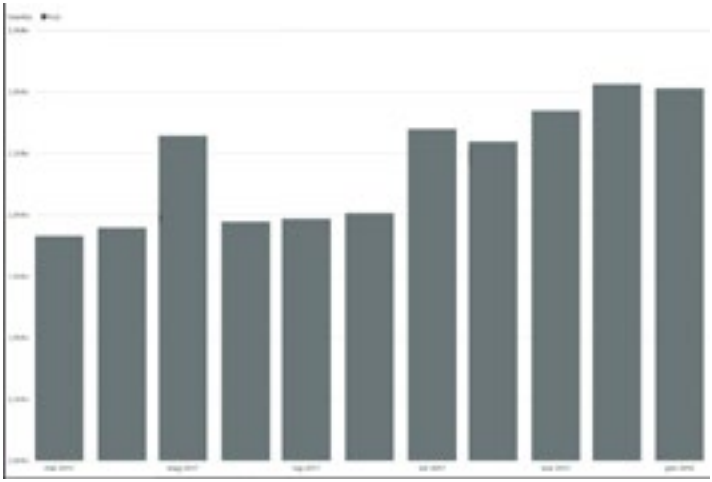
Category	Count
Trojan	808
Downloaders	243
Infostealers	138
Phish	102
Java Adwind	20
Office Exploit	13

È evidente come le tipologie di minacce rilevate richiedano nella maggioranza dei casi una collaborazione attiva dell'utente per portare a un'effettiva compromissione. È fondamentale quindi affiancare agli strumenti di protezione lato posta elettronica e sistemi client, un'adeguata formazione di sicurezza dell'utente finale per limitare il successo di questo attacchi.

Microsoft Antimalware

In quest'ultimo paragrafo ci soffermiamo sui dati relativi alle rilevazioni compiute attraverso gli strumenti antimalware Microsoft. Sono inclusi dati provenienti da strumenti come Windows Defender, System Center Endpoint Protection, Microsoft Safety Scanner e Microsoft Security Essentials, ed altri strumenti che utilizzano come minimo comune denominatore il Microsoft Malware Protection Engine. L'engine Microsoft è utlizzato anche come uno dei possibili meccanismo di protezione dei sistemi virtuali in Azure.

La figura seguente mostra i dati relativi ai cosiddetti "Malware Encounter" ovvero il numero di sistemi che hanno riportato la rilevazione di almeno un malware.



Si nota come complessivamente il trend sia in crescita, con un aumento del 50% delle rilevazioni tra metà del 2017 e la fine del 2017. Si nota inoltre il picco di maggio 2017, corrispondente al rilascio di WannaCry.

Minacce rilevate

Le due figure seguenti rappresentano rispettivamente:

- il numero di Machine Encounter per tipologia di minaccia rilevati in Italia nel corso degli ultimi 6 mesi.
- Il numero di File Encounter per tipologia di minaccia rilevati in Italia nel corso degli ultimi 6 mesi

I dati relativi al mese di febbraio 2018 sono parziali e quindi non confrontabili con i mesi precedenti.

Le famiglie di malware più diffuse rientrano nelle categorie:

- **Trojan**: tra le varie minacce prevalenti in questo ambito, segnaliamo Win32/Fuery.A!cl che, oltre è essere una delle più diffuse, ha particolari caratteristiche di pericolosità legate al fatto di aggregare diverse tipologie di malware in un'unica collezione:
  - Furto di informazioni bancarie
    - Botnet
    - Click-fraud
    - Ransomware
    - Trojan

Altra minaccia particolarmente diffusa a partire da inizio 2018 è CoinMiner, un miner di Bitcoins.

- **Browser Modifiers**: tra questi il più diffuso nel semestre analizzato è stato Win32/Xeelyak, un browser modifier che apporta dei cambiamenti al browser (Google Chrome e Internet Explorer) senza consenso:
  - Modifica della homepage
  - Modifica del motore di ricerca
  - Aggiunta di estensioni browser e toolbar
  - Disabilitazione di feature di sicurezza del browser

Tipicamente questa minaccia viene installata attraverso altri software non desiderati come BrowserModifier:Win32/Sasquor e BrowserModifier:Win32/Suptab.

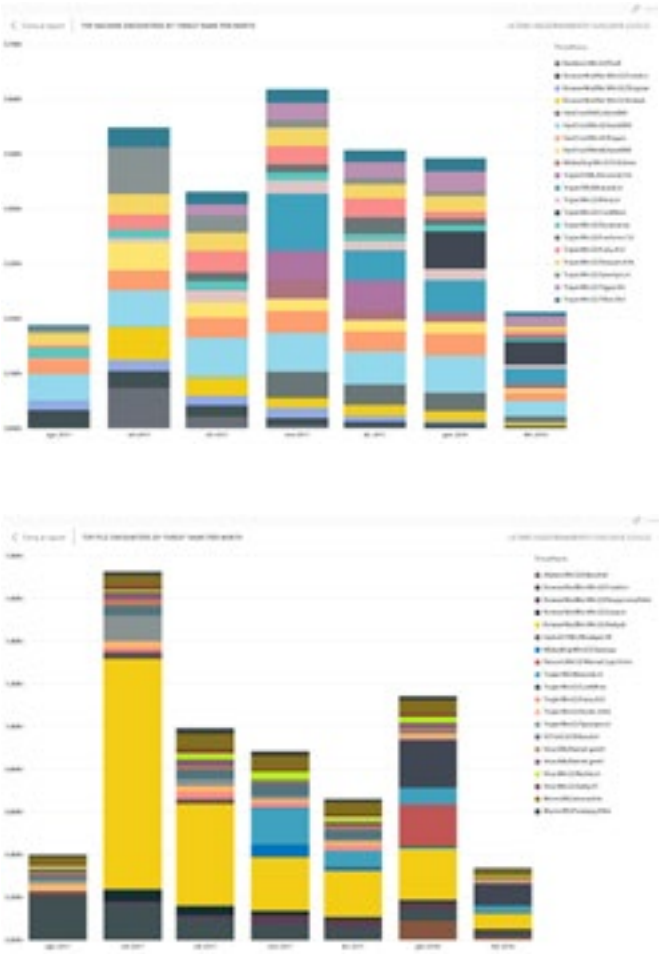
Per la definizione di questi software non desiderati, che alterano senza consenso la configurazione del PC, Microsoft utilizza un insieme di criteri oggettivi e documentati[8].

- Hack tools: particolarmente diffuso risulta AutoKMS, utilizzato per "craccare" copie non registrate di software Microsoft. Spesso l'utilizzo di questi strumenti è associato all'installazione di malware o software non desiderato[9].

[8] https://www.microsoft.com/en-us/wdsi/antimalware-support/malware-and-unwanted-software-evaluation-criteria

[9] SIR v13 https://www.microsoft.com/en-us/download/details.aspx?id=34955

- Backdoor: la minaccia di questo più diffusa nel 2017 è rappresentata da Win32/floxif, ovvero dalla versione "trojanized" del software CCleaner. Dopo aver raccolto una serie di informazioni dal sistema, questa minaccia comunica con un server di Command&Control dinamico da cui scarica ed esegue ulteriore codice malevolo.



Nel caso dei sistemi antimalware, l'utilizzo del cloud è diventato prevalente come meccanismo per migliorare la protezione. Diversi vendor, inclusa Microsoft, hanno introdotto funzionalità di verifica dei file sospetti nel cloud con l'obiettivo di ridurre i tempi di risposta alla rilevazione di nuovi malware da ore a secondi.

Attraverso meccanismi euristici, machine learning, e analisi automatizzate del file, viene determinato se il file sospetto è malevolo o innocuo, e in taluni casi viene richiesto l'invio del file completo per eseguire un'analisi più approfondita. Gli esiti delle analisi nel cloud vengono poi tipicamente messi a disposizione di tutti gli utenti del sistema antimalware in modo che di questi risultati possano beneficiare tutti gli utilizzatori dell'antimalware nel momento in cui dovessero venire a contatto dello stesso file.

Conclusioni

Il cloud introduce numerosi nuovi vettori di attacco che non erano precedentemente disponibili agli attaccanti nel mondo on-premise. Questi nuovi tipi di attacco richiedono un'evoluzione nelle metodologie di rilevamento.
Uno dei vantaggi nell'eseguire i propri workload nel cloud è sicuramente la possibilità di avvalersi di meccanismi avanzati rilevamento e di threat intelligence e della competenza di team con una vasta esperienza di sicurezza.
Rimane fondamentale adottare le best practice di sicurezza adottate nel mondo on-premises, che devono essere però aggiornate e rivisitate da un punto di vista differente in base alle nuove possibilità che il cloud mette a disposizione, accertandosi di aver definito accuratamente la matrice di responsabilità delle misure di sicurezza tra azienda e fornitore cloud.

La Cyber Security, una priorità per il Board

[A cura di Federico Santi, DXC Technology]

Una rivoluzione permanente

La CyberSecurity rappresenta ormai un sistema di tale ampiezza e pervasività che sperare di poterne dare una rappresentazione, anche solo etimologica, che pretenda di essere universale ed onnicomprensiva è una sfida di improbabile realizzazione.
Tuttavia questa complessità è ormai palesemente associata al bisogno da un lato di evitare semplificazioni e analisi statiche dall'altro di adottare una strategia omogenea per governarne gli obiettivi, le pratiche ed i risultati, facendo i conti con un contesto, scomodando Trotskij, di rivoluzione permanente, dove le analisi una tantum hanno una rapida obsolescenza e la resilienza riposa sulla capacità di gestire scenari in continuo cambiamento.
Seguendo questo filo appare come fisiologico il progressivo coinvolgimento della parte più alta dell'organizzazione, il Board, nella percezione dei rischi di Sicurezza e nei processi decisionali orientati alla mitigazione di questi rischi ed all'attivazione dei modelli di Sicurezza più adatti e dei relativi investimenti.
Questo percorso non ha certo stupito gli analisti e gli operatori più attenti che da anni ormai assistono a quattro macro-fenomeni:

- Evoluzione delle minacce da aspetti tipicamente infrastrutturali o applicativi verso i veri target oggetto di interesse: processi, utenti, dati, brand, valore azionario, etc.
- Integrazione degli approcci di sicurezza perimetrali con quelli più diffusi, in linea con la progressiva decentralizzazione delle infrastrutture nell'era della Quarta Piattaforma (mobile/big data/cloud/social)
- Integrazione delle strategie di sicurezza preventive (Sicurezza e Privacy By Design) con quelle reattive (la gestione e notifica degli incidenti)
- Compliance risk-based e con quote sempre maggiori di Sicurezza all'interno del sistema di controllo e di Risk Management complessivo

Il comune denominatore di questi fattori è proprio il passaggio delle preoccupazioni e delle decisioni relative alla Sicurezza da un piano meramente tecnico legato ai mezzi (intesi come strumenti e infrastrutture), ad un piano più direttamente legato ai fini (intesi come target degli attacchi e quindi come beni, materiali ed immateriali, da proteggere).
Le normative, da buoni reparti di retroguardia, stanno consolidando questa tendenza attribuendo sempre più spesso oneri al Management delle organizzazioni in termini di analisi e gestione dei rischi, più che responsabilità alle linee tecniche nella mera realizzazione di contromisure specifiche, i cui requisiti potrebbero variare velocemente nel tempo. Questa sembra essere la ragione della convergenza delle principali normative nazionali ed europee (GDPR e NIS in particolare) verso un approccio risk-based ed una significativa focalizzazione sui controlli by design e sui processi di notifica degli incidenti.

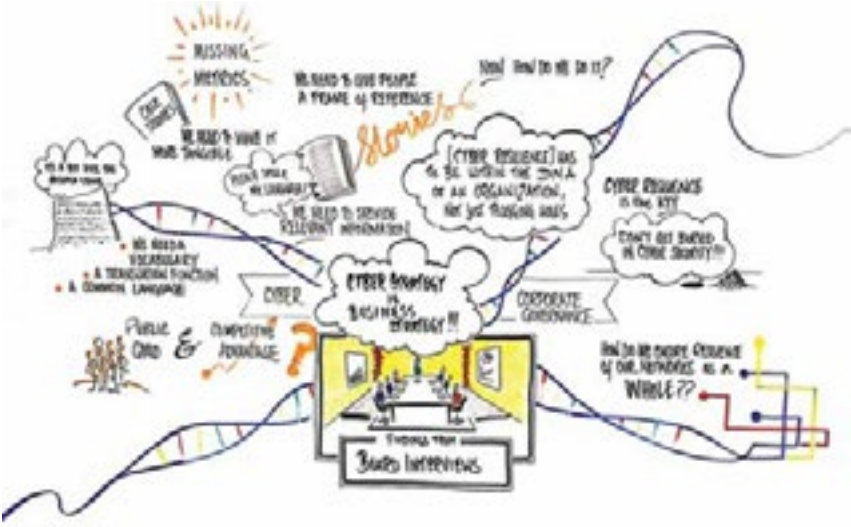
Alla luce di questo percorso evolutivo appare consequenziale il progressivo interessamento da parte dei vertici aziendali ai temi di CyberSecurity che un tempo non varcavano la soglia delle mura dei CED.
Oggi è il vertice aziendale ad essere esposto ai danni di un attacco o di un disservizio.
Sta al Board decidere investimenti e azioni necessarie per poter valutare correttamente anche i rischi di Sicurezza e attivare strategie e contromisure adeguate di mitigazione.
È il Top Management a dovere e voler tutelare i propri beni-chiave, sempre più immateriali e quindi sempre più digitali, quindi volatili ed esposti agli attacchi.
Per questa serie di ragioni la Comunità Cyber deve prepararsi anche a dare risposte diverse di fronte a problemi nuovi, adattando i propri paradigmi in termini di linguaggio, metodi e soluzioni.

La sfida

Per provare a raccogliere questa sfida ambiziosa nel 2017 il World Economic Forum, DXC e The Boston Consulting Group hanno costituito un Gruppo di Lavoro con un obiettivo molto sfidante: fornire al Board delle organizzazioni pubbliche e private una metodologia e degli strumenti per poter assumere decisioni appropriate in materia di CyberSecurity.
Dalle analisi svolte è emerso un ruolo del Top Management non più di soggetto informato ma di attore chiave nei processi di CyberSecurity.
Questo profondo cambiamento origina dal fatto che sia le tecniche di Cyber attack che le strategie di Cyber defense, essendo ormai intimamente collegate ai processi ed agli asset chiave delle Organizzazioni, richiedono entrambi una visione strategica più che un approccio tattico di pura risposta.
E questo approccio strategico di CyberSecurity non può che essere integrato all'interno di una più generale strategia aziendale di perseguimento dei propri obiettivi di breve e lungo periodo e di tutela dei suoi asset chiave, siano essi materiali o immateriali.
Questo è il motivo principale per cui, con riferimento a questo concetto esteso di Sicurezza, si preferisce parlare di Cyber resilience piuttosto che di "semplice" CyberSecurity, non solo in un'ottica di miglioramento dell'efficacia dei sistemi di Sicurezza ma anche ai fini di un efficientamento della crescente spesa di Sicurezza.
Non ultima è emersa la necessità di integrare questo approccio di coinvolgimento "verticale" con uno di diffusione "orizzontale". Le strategie decisionali, benché illuminate, non bastano senza un'adeguata awareness dei rischi di Sicurezza a tutti i livelli.

Cyber governance

Il World Economic Forum ha condotto lo scorso anno una serie di interviste con membri dei Board delle principali aziende di diversi settori industriali in tutto il mondo.
Il dato inequivoco è che l'84% degli intervistati ha affermato la necessità di migliori strumenti e linee guida per il loro lavoro di definizione delle strategie e di supervisione.



All'emergere di questo bisogno di strumenti e metodi di Governance della CyberSecurity a livello di Board va associata una nuova presa di coscienza.
L'Information Technology si affermato nei precedenti decenni come una fabbrica di automazione e velocizzazione di processi aziendali che però nascevano e rimanevano ancora concettualmente "analogici".
La rivoluzione digitale degli ultimi due decenni ha invece iniziato a sviluppare processi nativamente digitali, nella loro concezione e nella loro continua trasformazione. E di conseguenza l'IT ha smesso di essere un'officina, una variabile indipendente dai processi di business e dai relativi decision maker.
Come i processi di business oggi sono nativamente digitali così anche la Sicurezza non può più essere un add-on all'IT, una patch, un'officina nell'officina. I processi devono nascere anche nativamente sicuri. Questo lo percepisce il Board ma lo dettano anche le principali normative europee (NIS e GDPR), invocando la natura "by design" sia della Sicurezza che della Privacy.
Ed è questo che emerge in maniera lampante dallo studio condotto con il World Economic Forum: per il top management delle grandi imprese il business nel suo insieme e le sue componenti strutturali (processi, dati, utenti) sono il vero asset da proteggere. Comprendono loro stessi che la cyber resilience, la capacità di monitorare, rilevare, reagire, resistere agli attacchi è una loro responsabilità tra quelle più strategiche. In termini funzionali, logici prima ancora che tecnologici.
Ed è da questa presa di coscienza che nasce una preoccupazione, un'urgenza di governare i rischi cyber definendo una Governance della CyberSecurity, processi, modelli organizzativi, framework e infine tool.

Principi e strumenti

Date queste premesse il gruppo di lavoro WEF ha sviluppato un set di 10 Principi di Cyber Resilience per disegnare un quadro di Governance relativo alla cyber resilience e mettere il Board in condizione di definire le opportune strategie.

Uno dei punti-chiave di questa iniziativa è la necessità di colmare il gap degli ultimi anni tra la presa di coscienza nei Board sui rischi cyber e ancora l'effettiva carenza di principi attuativi.

I Principi enucleati sono i seguenti:

1. **Responsabilità.**
   Il Board ha la primaria responsabilità della cyber resilience, avvalendosi eventualmente di specifici comitati di Risk management o cyber resilience.
2. **Awareness.**
   I membri del Board ricevono informazioni continue utili al loro orientamento tempestivo su trend di attacco e difesa.
3. **Accountability.**
   Il Board assicura l'esistenza di un Officer a livello Corporate, dedicato al reporting relative alla capacità dell'azienda di definire e raggiungere gli obiettivi di cyber resilience.Cruciale sia l'adeguato profilo dell'Officer sia il necessario livello di empowerment.
4. **Integrazione.**
   Il Board assicura l'integrazione della cyber resilience nella più generale strategia di Risk management aziendale.
5. **Risk appetite.**
   Il Board definisce annualmente e quantifica la business Risk tolerance relativa alla cyber resilience, assicurandosi che sia coerente con la strategia di Risk management aziendale, tenendo in considerazione sia gli aspetti regolatori che la complessiva esposizione al rischio.
6. **Risk assessment.**
   Il Board assicura che il Risk management cyber sia integrato e coerente con il generale Risk management, anche in termini di reporting, avvalendosi di un proprio Board Cyber Risk Framework.
7. **Piani di resilience.**
   Il Board assicura che il Cyber resilience Officer sia supportato da tutto il Management al fine di garantire l'implementazione dei piani di cyber resilience.

8. **Community.**
   Il Board incoraggia la collaborazione tra il Management e gli stakeholder necessari.
9. **Review.**
   Audit annuale, formale, indipendente della cyber resilience.
10. **Efficacia.**
    Review periodiche della cyber resilience in un'ottica di miglioramento continuo.

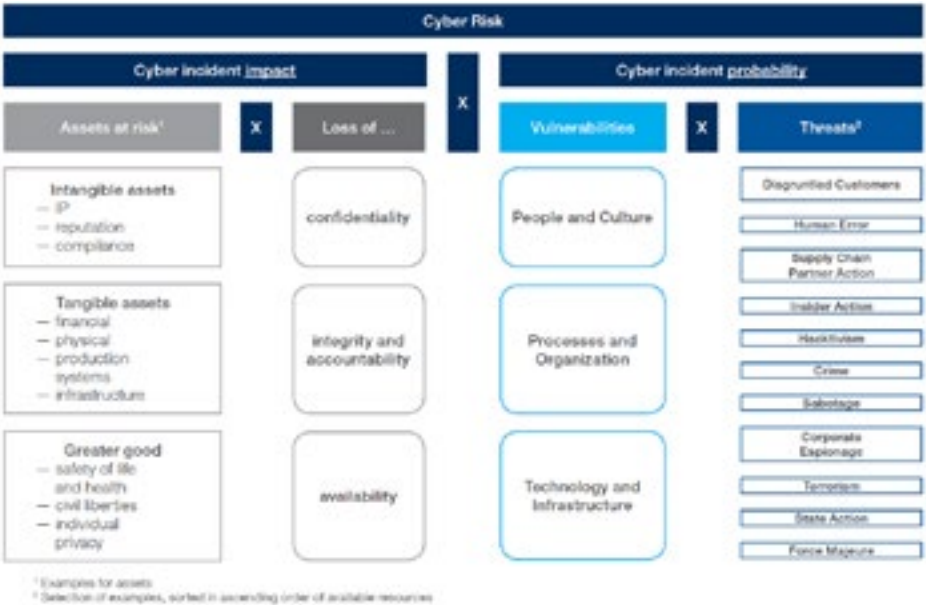
I Principi sono a loro volta integrati da un Toolkit composto da set di domande che consentano una reciproca migliore comprensione tra il Board ed il top management sul tema Cyber.

Board Cyber Risk Framework

Tra i dieci comandamenti definiti spicca in particolare il Sesto principio che stabilisce la centralità e crucialità di un modello di Governance dei rischi cyber per il Board. Per le ragioni descritte in precedenza emerge platealmente la necessità per il top management delle organizzazioni di presidiare e mitigare i rischi cyber allo stesso livello di priorità di quelli più ampi tradizionalmente considerati.
Si suggerisce ai ruoli apicali delle organizzazioni non solo di definire un framework di gestione dei rischi cyber ma anche di aggiornare l'analisi di quei rischi, la loro integrazione con il Risk Management generale e la gestione continua di un programma di Cyber Risk Management.
Per procedere in questa direzione virtuosa si suggerisce al Board di valutare:

1. Il livello corrente di Risk tolerance/appetite
2. I rischi cyber che insistono sulla specifica realtà organizzativa
3. I controlli e le azioni in essere per la gestione o mitigazione dei rischi
4. I rischi cyber residui, confrontati con l'iniziale livello di Risk tolerance

La valutazione di questi rischi dovrà avvenire attraverso una mutua valutazione della loro probabilità di accadimento e del relativo impatto.



Questo scenario, ben consolidato per gli esperti di settore, è in realtà sostanzialmente innovativo per vertici aziendali che fino ad oggi hanno spesso ignorato la componente cyber dei rischi delle loro organizzazioni considerandoli una technicality di cui qualcuno, all'interno dell'area ICT, si dovrebbe preoccupare.

Come guida a questo percorso sono stati sviluppati anche questionari per accompagnare il Board ad una più ampia comprensione di tutte le componenti che influenzano la comprensione e quindi la mitigazione dei rischi cyber che li riguardano:

- Individuazione e valutazione degli asset cruciali, i cosiddetti "gioielli della corona"
- Costi diretti e indiretti collegati ad attacchi o incidenti cyber
- Minacce generali e particolari riferite alla specifica tipologia dell'organizzazione e del mercato in cui opera
- Vulnerabilità generali e specifiche
- Fattori di influenzamento del livello di rischi (cambi organizzativi, nuove tecnologie, nuovi scenari di mercato)
- Stakeholder interni ed esterni da considerare

Il board di fronte ai rischi tecnologici emergenti

Proseguendo nel percorso di sensibilizzazione del Board ai rischi cyber, line guida specifiche sono state disegnate per supportare i processi decisionali legati all'affermazione di nuove tecnologie o meglio di nuovi scenari del loro utilizzo.

Lo scopo di questa sezione del lavoro è proprio quello di facilitare la discussione e le decisioni tra il Board e le linee operative partendo dalla considerazione di un loro mutuo influenzamento.
Se da un lato, come si diceva, le tecnologie influenzano le possibilità dei processi digitali a tal punto da trasformarli in processi nativamente digitali, dall'altro sono proprio le evoluzioni degli obiettivi di business a guidare la ricerca, lo sviluppo o la trasformazione delle tecnologie stesse.

I riflessi organizzativi di questa collaborazione si estrinsecano inevitabilmente nella necessità di governare la tecnologia con una prospettiva di business e di gestire le evoluzioni del business con una maggiore considerazione dei rischi tecnologici.
Questa integrazione è stata sintetizzata nei seguenti livelli:

- Presa di coscienza dei rischi tecnologici emergenti
- Concezione di una resilienza by design dei processi e delle infrastrutture
- Impostazione di un livello accettabile di Sicurezza
- Gestione dei rischi cyber anche dei vendor/provider
- Gestione sicura dell'intero ciclo di vita delle tecnologie
- Data privacy
- Considerazione dei riflessi etici, sociali e pubblici dell'utilizzo di nuove tecnologie
- Miglioramento continuo dei controlli
- Incremento della capacità di rapido adattamento ai cambiamenti (interni ed esterni).

Da questi principi generali ne discendono anche specifici use case sui rischi specifici legati a scenari tecnologici emergenti.
Sono particolarmente rilevanti da questo punto di vista i rischi che emergono da nuovi scenari legati al mondo IoT soprattutto nelle aree dei Trasporti, della Sanità e delle Smart Cities.
Non meno cruciale da questo punto di vista è anche la rete delle infrastrutture critiche, come pure ha evidenziato la Direttiva europea NIS di prossima entrata in vigore.

Scenari futuri

Vale la pena sottolineare come il World Economic Forum con i suoi partner su questa iniziativa (DXC e Boston Consulting) ha voluto stabilire dei principi e degli strumenti a supporto di una necessità sempre più sentita nelle organizzazioni pubbliche e private.
Non fa parte degli obiettivi del Forum voler stabilire un framework sul quale eventualmente avviare iniziative di certificazione piuttosto che di Audit.

L'iniziativa ha piuttosto l'obiettivo dichiarato di voler creare dei punti di riferimento, un metodo e degli agili strumenti per poter supportare il Board delle organizzazioni pubbliche e private di fronte a sfide crescenti nell'ambito CyberSecurity.

In questo contesto il Forum intende coltivare un progetto di miglioramento continuo del Cyber Risk Framework anche attraverso:

- Lo sviluppo di una rete di partnership che includa le diverse industry a livello globale
- La costruzione di una partnership pubblico-privato che coordini i governi, le aziende e la società civile. Richiamo questo cruciale nella logica della CyberSecurity come bene pubblico globale in un'economia sempre più digitale
- L'individuazione e la formazione di una leadership matura sul tema che si traduca in una classe dirigente matura sia nel pubblico che nel privato.

Come al solito le sfide complesse hanno bisogno di eccellenze, e lo scopo di questa iniziativa è proprio quello di aiutarle a formarsi ed emergere.

https://www.weforum.org/projects/partnering-for-cyber-resilience

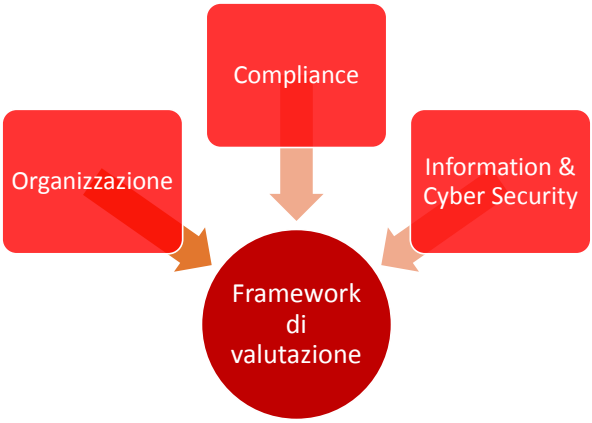
La governance dei fornitori: adottare un maturity model efficace

[A cura di Alessio Pennasilico]

Nell'attuale scenario di mercato, in cui i fornitori esterni che supportano aziende e pubbliche amministrazioni nella conservazione ed elaborazione dei dati sono sempre più numerosi e pervasivi, garantire l'information security e la cyber security è diventata una necessità ancor più stringente che in passato. Questa necessità non traguarda esclusivamente fini di compliance alle sempre più numerose leggi che regolano questi aspetti, come ad esempio il Regolamento Europeo sulla Data Protection (GDPR); la corretta gestione di tutti gli attori coinvolti nella gestione dei dati aziendali, infatti, diventa requisito per la tutela dei servizi di business e del patrimonio informativo aziendale.

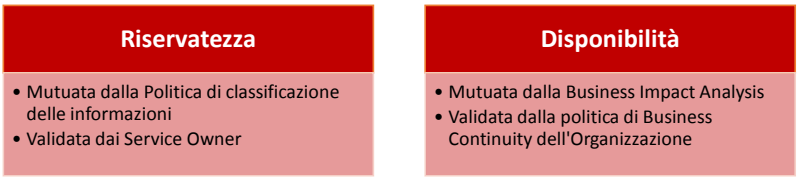
Nelle organizzazioni, indipendentemente dalle loro dimensioni o complessità, inoltre, sono sempre più frequenti i casi in cui diverse funzioni aziendali si dotano di fornitori di servizi informatici senza appoggiarsi in alcun modo alla funzione interna di gestione dei Sistemi Informativi. Si pensi a con che frequenza, ad esempio, uffici HR scelgono ed acquistano servizi esterni per la gestione di alcuni sub-processi di propria competenza o agli uffici Marketing che acquistano micro-servizi per la gestione di un portale o di un mailing temporanei, per l'esecuzione di una specifica campagna promozionale.

La gestione dei fornitori, inoltre, è un tema interdisciplinare che coinvolge molti aspetti diversi tra loro. Vanno infatti prese in considerazione tematiche di carattere legale per assicurare l'adeguatezza del contratto, di natura organizzativa per garantire l'adeguatezza dei processi e di carattere tecnico per garantire l'adeguatezza degli strumenti.



Per tutte queste ragioni l'adozione di un framework di gestione dei fornitori interdisciplinare, formale, noto, oggettivo e condiviso con tutte le funzioni aziendali, diventa una esigenza imprescindibile a tutela del business.

Molti dei criteri utilizzabili possono essere mutuati da informazioni già disponibili all'interno dell'azienda: questo permette di semplificare il modello e garantire coerenza ed uniformità di giudizio. Ad esempio, è possibile utilizzare la politica di classificazione delle informazioni esistente per stabilire il livello di riservatezza richiesto al fornitore e la Business Impact Analysis (BIA) del processo coinvolto nella fornitura per stabilire le necessità di disponibilità.
Questo fa si che non siano i Sistemi Informativi a decidere autonomamente il livello di riservatezza necessario, ma i service owner, che hanno contribuito in prima persona a classificare le informazioni gestite. La disponibilità richiesta inoltre, verrebbe validata dall'organizzazione e non soltanto dal singolo service owner.



Per questa ragione andrebbe ratificata una politica aziendale circa i criteri di valutazione dei fornitori, da cui far discendere le relative procedure operative, le checklist di verifica e le procedure di verifica di applicazione ed efficacia.

La politica di alto livello, infatti, dovrebbe regolare i principi di carattere generale che verranno poi recepiti nelle procedure e nelle checklist, oltre a raccordare tale politica con altre policy aziendali, come nell'esempio precedente.

Le procedure operative dovrebbero essere poi diffuse, non solo all'ufficio acquisti o al procurement, ma anche a tutte le funzioni aziendali in grado di acquistare autonomamente dei servizi.

Tali politiche operative dovrebbero includere delle checklist di verifica, al fine di poter fissare SLA e KPI oggettivi e misurabili al fine di poter eseguire valutazioni e misurazioni incontestabili.

Stabilito un set di controlli, infatti, andrebbero presi in considerazione diversi parametri di giudizio. L'applicabilità, ad esempio, permetterebbe di valutare se un controllo del modello

è necessario per un contratto di fornitura hardware o per uno di fornitura di servizi. La maturità permetterebbe di valutare la presenza e gli eventuali indici di misurazione di un controllo. L'efficacia, invece, supporterebbe tanto l'iniziale processo di valutazione quanto il successivo processo di monitoraggio delle performance del fornitore.
Per creare ordine all'interno del modello, e facilitare il lavoro tanto di chi dovrà compilare che di chi dovrà verificare, diventa estremamente funzionale l'approccio già utilizzato da molti standard, di dividere i controlli per domini ed obiettivi, come già avviene nella ISO/IEC 27002:2013.

Il modello, inoltre, dovrebbe permettere di valutare singolarmente ogni contratto, stabilendo quali siano i requisiti specifici dello stesso. Iniziando ad applicare il framework sulla situazione esistente, infatti, si arriverebbe a stabilire quali debbano essere i requisiti specifici, tanto del singolo contratto quanto del fornitore. Il modello, di conseguenza, applicato ad un partner di piccole dimensioni, otterrebbe gli indici necessari per tutti i contratti in gestione da tale partner. Un fornitore complesso, come potrebbe essere una multinazionale con diversi team, divisioni e linee di business, otterrebbe i risultati circa i requisiti specifici per un singolo accordo siglato/da siglare. Lo stesso fornitore complesso, tuttavia, potrebbe ottenere punteggi diversi per contratti diversi.

Un maturity model così strutturato riuscirebbe a calcolare dei punteggi oggettivi necessari al fine di poter gestire il singolo servizio e di paragonarli con quelli dei possibili o attuali fornitori.

Nel caso di fornitori esistenti sarà possibile creare un remediation plan prioritizzato per mettere in sicurezza il servizio.
L'applicazione pratica di tali framework, infatti, vede spesso utilizzare strumenti come quello della clausola risolutiva espressa per indurre in modo energico il fornitore a rimediare ad una situazione di patologia del rapporto, prima ancora che per risolvere realmente il contratto. Lo stesso vale per fornitori esistenti: un fornitore che non raggiunga alcuni requisiti, nonostante anni di onorato servizio non monitorato dal punto di vista della security, più facilmente godrà di una finestra temporale definita in cui adeguarsi ai livelli richiesti che non vedere risolto il rapporto consolidato.

Questo maturity model potrebbe essere strutturato su più livelli: uno da compilarsi da parte del Cliente, a fronte delle verifiche di ammissione all'albo fornitori, uno da compilare in self assessment, da utilizzare poi per eventuali audit. L'audit potrebbe essere effettuato solo sui fornitori strategici, a campione casuale o su chi si discosta in modo importante dalla media dei fornitori aziendali.

Dovrebbe poi esistere una procedura di verifica della reale applicazione di tale modello, dello stato di avanzamento dei remediation plan concordati con i fornitori esistenti. Tale

procedura dovrebbe tener conto anche della verifica di efficacia del modello. Soprattutto nelle prime fasi di adozione del framework, infatti, potrebbe essere necessario ottimizzare alcuni SLA o KPI rispetto a quanto stabilito inizialmente, in assenza di misurazioni.

Per concludere, un framework per la gestione dei fornitori basato su policy, procedure e checklist assicurerebbe la corretta gestione del rischio associato ai fornitori tramite l'adozione di un maturity model strutturato ed oggettivo, basato su informazioni consolidate. Questa modalità, quindi, permetterebbe di avere un outlook aziendale circa tutte le informazioni gestite da terzi, eventuali criticità presenti o nascenti e permetterebbe di stabilire tanto le strategie quanto le tattiche necessarie a governare la sicurezza del patrimonio informativo aziendale. In uno scenario come quello attuale, in cui l'accountability diventa sempre più rilevante, non solo per il GDPR, permetterebbe di dimostrare una gestione efficace di tutti i temi legati alla data governance, data protection, all'information e cyber security a tutela del business aziendale e di tutti gli stakeholder coinvolti.

Approfondimento: alcuni esempi

I controlli di estrazione esclusivamente legale potrebbero riguardare la regolamentazione della proprietà intellettuale di strumenti ed informazioni, la presenza di una clausola risolutiva espressa per poter risolvere il contratto in caso di grave e prolungata inadempienza, la presenza di una assicurazione danni a terzi ove necessario.

I controlli organizzativi potrebbero prevedere la presenza di specifiche politiche, processi o procedure, come ad esempio quelle volte a regolare accesso ai sistemi, change ed incident management.

I controlli di security potrebbero prendere in considerazione la presenza di eventuali piani di backup e/o disaster recovery.

Molti ambiti hanno contorni che toccano contemporaneamente diverse aree. Il tema audit, ad esempio, è il classico esempio di argomento interdisciplinare: se la possibilità di eseguire penetration test o altre verifiche sui sistemi che erogano il servizio può essere considerata un requisito di security, la gestione delle eventuali anomalie emerse può rientrare nella categoria organizzazione, mentre la possibilità di risolvere il contratto ad un fornitore che ignori le richieste di remediation è quasi sicuramente un aspetto di natura legale. Indipendentemente dalla categoria in cui si decida di far ricadere tali controlli, tuttavia, si tratta di requisiti necessari e strettamente correlati tra loro.

Tra i controlli generali potrebbero essere presi in considerazione parametri quali la storia e la solidità aziendale del fornitore, o ad esempio quanto il l'affidamento oggetto di analisi incida sul fatturato del partner. Questo permetterebbe di scegliere o evitare di legarsi ad un fornitore per i quali si è il principale committente o per il quale sussistono dubbi circa la capacità di erogare il servizio.

Potrebbe, inoltre, essere valutata la presenza di certificazioni specifiche di un vendor afferente la fornitura o certificazioni del sistema di gestione, come ad esempio ISO 27001 o ISO 20000.

Il fattore umano nella gestione dell'innovazione e dell'information security aziendale.
Social Engineering e Social Profiling

[A cura di Pamela Pace, Obiectivo]

Tecnologia leva primaria dell'innovazione

La rivoluzione introdotta dalle nuove tecnologie nella società postindustriale non ha precedenti: i fruitori di Internet nel 2015 hanno superato i 3,77 miliardi e si prevedono oltre **40 miliardi di dispositivi connessi entro il 2020**. Sono cifre che fanno venire le vertigini e che certamente mai si sono associate all'utilizzo di un qualsiasi servizio meglio, dunque, anticipare tale trend e **dettare il passo**.

Steve Jobs lo aveva ben chiaro: «È la capacità di innovare che distingue un leader da un gregario».

Ma cosa significa esattamente innovare oggi?

Fare innovazione oggi significa attivare un dialogo tra i diversi ambiti di conoscenza.

I gruppi di lavoro che operano all'interno delle organizzazioni e che riescono a produrre innovazione hanno un profilo sempre più multidisciplinare. Il dialogo costruttivo tra di essi aiuta a portare nuove visioni e ad aprire nuovi scenari all'interno dei contesti lavorativi.

In questo la tecnologica gioca un ruolo fondamentale perché può essere il primo motore d'innovazione e il suo abilitatore più importante.

Le aziende sono sempre più orientante verso un modello di Digital by Default.

Ma se da un lato il valore dell'innovazione è sotto gli occhi di tutti, dall'altro di certo non si può trascurarne anche altri aspetti un po' meno entusiasmanti.

L'innovazione infatti aiuta a crescere e confrontarsi con un mercato più globale, ma apre altresì la strada ad un sempre crescente perimetro di rischio e conseguenti minacce.

Se trascurassimo questo aspetto ci troveremmo a trattare l'innovazione non più come un fattore abilitante, ma piuttosto, come un potenziale elemento distruttivo, basti pensare al caso Equifax, una delle tre più grandi agenzie di credito al consumo al mondo.

A seguito della dichiarata violazione dei propri sistemi e della compromissione dei dati trattati, ritenuta la peggiore perdita di informazioni personali di sempre, nell'arco di poche settimane ha perso oltre un terzo del proprio valore in borsa, subito circa 240 azioni collettive, 60 indagini governative da parte di procuratori generali degli Stati Uniti, agenzie federali, governi britannico e canadese, e una rara azione collettiva promossa da 50 stati.

È chiaro che il futuro di Equifax non è roseo.

Questo esempio che rappresenta evidentemente un caso eccezionale, è però molto efficace per comprendere come un'azienda fortemente digitalizzata abbia saputo sfruttare appieno il potenziale dell'innovazione tecnologica, posizionandosi così tra le tre organizzazioni più grandi al mondo nel settore di riferimento, ma abbia pagato allo stesso modo duramente le vulnerabilità create da una non corretta gestione del processo di information security.

Information security asse portante dell'innovazione

Quando si parla innovazione e digitalizzazione dei processi di business o di servizi, quindi, non si può prescindere dal porre una grande attenzione al tema del rischio associato e alla sua gestione.

Parliamo quindi di information security o cybersecurity.

Leggendo i dati sul cyber risk, pubblicati nella ventesima edizione della EY Global Information Security Survey, Cybersecurity regained: preparing to face cyber attacks, emerge una fotografia molto peculiare.

Da un lato la poca volontà dei criminali informatici di tentare nuove strade per i loro attacchi – prevalgono ancora phishing e malware – dall'altro la scarsa reattività delle aziende che non riescono ad arginarli e rimangono in una situazione ad elevato rischio. Anzi, quand'anche stia crescendo la consapevolezza e la sensibilità verso questi temi, le aziende tendo a proteggersi solo se, e quando, hanno subito dei danni. Solo il 4% delle organizzazioni esaminate infatti afferma di monitorare in modo appropriato tutti i rischi rilevanti in tema di minacce cyber e vulnerabilità e altresì di non aver valutato nella loro attuale strategia tutti gli aspetti di information security.

È chiaro dunque che sebbene nelle aziende ci sia un sempre più pervasivo livello di digitalizzazione e una crescente consapevolezza del rischio ad esso associato, all'interno delle organizzazioni non vi sia ancora la maturità e la corretta coscienza di trattare questo rischio con la stessa dignità e modalità con cui si trattano altri rischi strategici.

L'information risk o cyber risk vengono demandati ad una gestione tattica e quasi mai strategica, quindi orientata a risolvere problemi puntuali, ma non inserita in un processo di gestione organico che affronti in modo olistico i vari aspetti.

Per una corretta gestione dell'information security, lo abbiamo detto già in molte occasioni, gli aspetti da indirizzare sono veramente molti Policy, Standards and Legal, Organisation e Governance, Procedures, Technology and Physical Infrastructure, Compliance and Audit.

Figura 1 - *Cyber risk management strategy*

Il fattore umano

All'interno delle organizzazioni un'attenzione particolare è posta agli aspetti tecnologici.
Questo fatto è dovuto in primis ad un aspetto culturale legato alle figure a cui ne viene demandata la gestione che, tipicamente, hanno un'estrazione tecnica, quindi sono più propensi a rimanere in un ambito per loro conosciuto e in cui si sentono confidenti; in secundis all'errata convinzione che un approccio tecnologico efficace possa da solo elevare sufficientemente il livello di sicurezza dell'azienda.
Le regolamentazioni internazionali e nazionali stanno invece spingendo l'attenzione delle aziende su aspetti più gestionali, organizzativi e normativi.
Un elemento che invece tende sempre ad essere trascurato o minimizzato, è quello della crescita formativa e informativa delle risorse interne, che viene tipicamente soddisfatta attraverso l'erogazione di pillole educative, o iniziative simili e di piccolo cabotaggio.
In questo modo però si ignora completamente il fatto che oggi gli attacchi più grandi e invalidanti sono stati, per la maggior parte dei casi, condotti da attaccanti che hanno sfruttano le "vulnerabilità" delle persone e la loro, a volte, incauta fiducia.
Pensare che le tecnologie o i processi più rigorosi da soli offrano la sicurezza è soltanto una mera illusione, abbandonandosi alla quale si rischia grosso.
Tecnologie di sicurezza sempre più sofisticate rendono arduo e a volte impossibile sfruttare i punti deboli legati alla tecnologia, è per questo che gli attaccanti decidono sempre più spesso di sfruttare l'anello debole della catena rappresentato dal fattore umano.
Bypassare questo tipo di "protezione" è facile, comporta rischi minimali e praticamente non richiede alcun investimento.
La mente del criminale, ingegnere sociale o hacker, è naturalmente indotta a trovare sempre strade alternative per eludere le misure di sicurezza messe in campo, pur di raggiungere il proprio obiettivo, e nella maggior parte dei casi lo fa concentrandosi sulle persone che usano la tecnologia.
Il Social Engineering rappresenta in molti casi il principale strumento utilizzato dagli hackers per sferrare un attacco.
Il fattore umano rappresenta quindi realmente l'anello debole dell'information security.
Se si vuole innalzare realmente il proprio livello di information security, quindi non si può prescindere dal formare adeguatamente tutti i propri collaboratori, e comprendere che tutta la tecnologia del mondo non potrà mai proteggerci da un attacco di social engineering ben congegnato.
La domanda, che correttamente dovremmo porci tutti, infatti è: "Per quale motivo un attaccante dovrebbe impegnarsi arduamente per superare barriere tecnologiche molto efficaci, quando, attraverso delle semplici analisi e correlazioni di informazioni presenti sul web e qualche telefonata ben congegnata, si può raggiungere lo stesso risultato ma con un terzo dell'impegno, della fatica e del rischio????"
Forse a tale proposito è opportuno chiarire un po' meglio cos'è l'ingegneria sociale e come agiscono gli ingegneri sociali.

Social engineering & profiling

L'ingegneria sociale, applicata all'information security, è lo studio del comportamento di una persona, e l'atto di manipolare una persona per accedere ai suoi dati sensibili o alle informazioni rilevanti gestite.
Le informazioni che apparentemente, se prese nella loro singolarità, sembrano ininfluenti, nella portata globale di un attacco saranno propedeutiche per averne ulteriori, o integrate ad altre, necessarie per completare il panel informativo utile all'attaccante per raggiungere il suo scopo.
Nessuna informazione è quindi irrilevante, ognuna di esse infatti ha un proprio valore intrinseco anche se non evidente agli occhi dei più.
Ogni frammento di informazione apparentemente innocua, o di per sé priva di valore, viene molto apprezzata dall'ingegnere sociale poiché, una volta raccolte e correlate potrà ottenere una visione d'insieme e un'immagine chiara.
È necessario sapere che gli ingegneri sociali sono persone tipicamente dotate di una grande intelligenza ed empatia.
Sono abilissimi nei rapporti umani, simpatici, dei veri professionisti della manipolazione, tutte doti necessarie per stabilire un rapporto di fiducia con le proprie "vittime", e sono quindi capaci di sfruttare al meglio tutte le parti del puzzle anche le più piccole.
Un esperto ingegnere sociale può accedere praticamente a qualsiasi informazione sfruttando le tattiche e strategie che ha affinato negli anni.
È quindi sempre più evidente che le persone rappresentano la più grave falla nella sicurezza propria e degli altri.
Soprattutto noi occidentali, infarciti della nostra cultura "buonista", pur sapendo che la maggior parte delle persone che ci circondano non sono oneste, viviamo apparentemente liberi dalla paura e quindi non mettiamo in conto il rischio comportandoci come se questo non esistesse.
Da questo punto di vista, a mio avviso, gli aeroporti sono l'emblema di questo assurdo paradigma.
La sicurezza all'interno di queste strutture è onnipresente, in alcuni casi attiva prima che si acceda fisicamente agli ambienti fisici, eppure in molti casi è successo che qualcuno sia riuscito lo stesso a superare i controlli in possesso di potenziali armi.
Il problema non sono i metal detector o le soluzioni di riconoscimento facciale, ma il fattore umano, le persone che le usano.
Ancora una volta è quanto mai chiaro che le più potenti tecnologie non sono utili se il personale che le usa non è sufficientemente accorto e quindi non controlla correttamente i passeggeri.
I manager più prudenti sviluppano con assiduità soluzioni di sicurezza atte a minimizzare i rischi connessi all'uso dei sistemi informativi, ma troppo spesso lasciano non gestito il punto debole più significativo, il fattore umano.
La preparazione la formazione rispetto alla politica aziendale per la tutela del patrimonio informativo aziendale deve essere rivolta a TUTTI i dipendenti, non solo agli addetti ai lavori

a chi ha accesso ai sistemi aziendali.
Oggi, più di ieri, facendo parte di una società iper-connessa risulta agevole per un ingegnere sociale avere informazioni da utilizzare, tracciare profili e utilizzare queste informazioni per sferrare attacchi.
Uno degli strumenti più utilizzati è appunto la profilazione, cioè la raccolta e la correlazione di tutta una serie di informazioni personali realizzata utilizzando dati sociali condivisi pubblicamente e volontariamente da ognuno di noi.
Un'altra straordinaria fonte di informazioni, per gli ingegneri sociali, è data dai metadati legati alle nostre attività su internet. In particolare ogni messaggio che scambiamo (es. Twitter, WhatsApp, ecc.), ogni e-mail che inviamo, ogni sito che visitiamo, fino alla cronologia di navigazione presente sul nostro browser sono attività che generano una mole enorme di dati e informazioni, dando a chi li analizza la possibilità di definire ancora meglio il nostro profilo personale e le informazioni che se ne possono ricavare sono decisamente moltissime.
I nostri metadati, infatti, possono essere raccolti da chiunque veicoli dati dal nostro dispositivo a quello di destinazione; quindi questi possono essere collezionati dai fornitori di servizi internet, dalle forze dell'ordine, ma anche da hacker con intenzioni malevole.
Per capire la potenza dei metadati il progetto ALTwitter (https://www.privacypies.org/ALTwitter) analizza i metadati degli account Twitter dei 618 membri del parlamento Europeo.
Da una rapida analisi sui profili dei dati aggregati si riescono a capire le abitudini personali e gli interessi degli utenti, gli orari in cui sono connessi su internet, i client utilizzati, ecc.

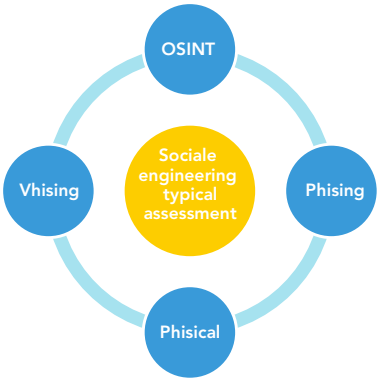


Figura 2 - *Information Engineering Typical Assessment*

Chiaramente questi sono profili pubblici e sono utilizzati espressamente a scopo di comunicazione politica, se fossero profili personali i dati che un Hacker potrebbe estrarre per profilare la potenziale vittima sarebbero decisamente più interessanti (interessi, amici, conoscenze, partecipazione ad eventi, ecc.)
Già diversi millenni fa SunTzu diceva: "Se conosci il nemico e te stesso, la tua vittoria è sicura."
La maggior parte delle persone non si rende conto che questa infinita mole di mole di informazioni diffuse, che noi tutti seminiamo nel magnifico mondo del web, possono essere facilmente raccolte e correlate, tracciando un profilo di noi di impressionate veridicità.

Questa ingenua apertura verso l'esterno ci espone a rischi non conosciuti e non sufficientemente ponderati, quale ad esempio il diventare il bersaglio di ingegnere sociale e il possibile veicolo di un attacco.

La Cultura della sicurezza valore d'impresa

È necessario che soprattutto in ambito aziendale sia posta la sufficiente attenzione a trattare questo tema nel modo più opportuno, non è infatti sufficiente realizzare qualche breve corso di formazione, si deve creare un substrato culturale diffuso e condiviso da e in tutta l'organizzazione che va costantemente alimentato.
Ogni componente della nostra organizzazione può essere potenzialmente il più grande dei nostri scudieri o trasformarsi, anche involontariamente, nel peggior nemico per la nostra organizzazione.

La sicurezza aziendale è questione di equilibrio tra i tanti elementi che compongono le strategie difensive, tutti devono essere organicamente sviluppati, governati e implementati, solo in questo modo si riuscirà ad ottenere un perimetro di difesa solido ed efficace.

La diffusione delle criptovalute: rischi ed opportunità in tema di sicurezza e regolamentazione del mercato

[A cura di Francesca Bosco e Marco Tullio Giordano]

1. L'anno delle criptovalute

Il 2017 è stato senza dubbio l'anno dell'esplosione del fenomeno legato al Bitcoin e, più in generale della diffusione delle c.d. criptovalute, valute digitali che utilizzano la *blockchain* e la crittografia a doppia chiave asimmetrica per creare e mantenere aggiornato un registro, solitamente decentralizzato e condiviso tra gli utenti, sul quale vengono annotate in maniera immodificabile le transazioni occorse tra i nodi della rete. Come si può vedere nella **Figura 1**, nel corso degli ultimi dodici mesi la capitalizzazione totale del mercato dell'intero segmento è cresciuta ad una velocità inimmaginabile – dai circa 20 miliardi di dollari di gennaio sino al picco di 800 miliardi di dollari raggiunti alla fine dell'anno[1], subito prima di subire una profonda correzione dei prezzi. Questo *trend* ha spinto alcuni detrattori a sostenere che vi sia, nel prossimo futuro, il pericolo di una nuova bolla finanziaria, al pari di quella occorsa con la diffusione incontrollata delle *dotcom* sul finire dello scorso millennio.

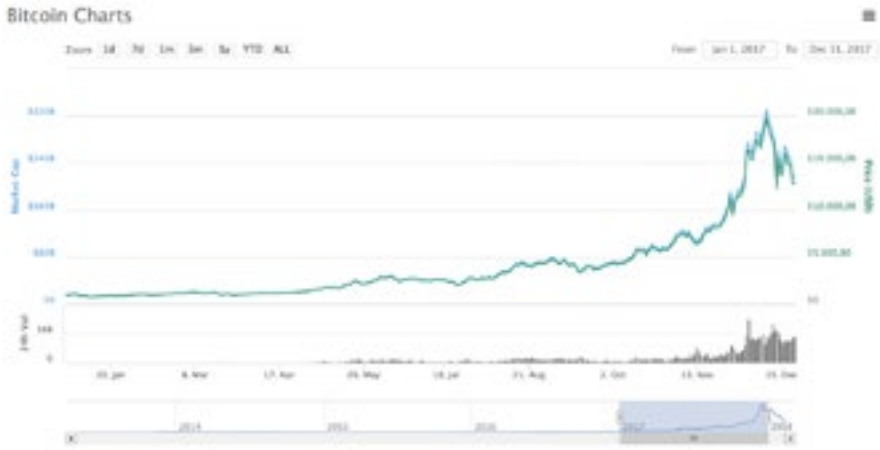


Figura 1 - *fonte Coinmarketcap.com*

Parallelamente all'aumento del valore e dell'utilizzo di Bitcoin, è grandemente cresciuto nel corso dell'anno l'interesse per le criptovalute di seconda generazione, denominate *altcoins*

[1] Per avere un termine di paragone con il mondo della finanza tradizionale, si consideri che all'inizio del mese di dicembre 2017 la capitalizzazione del mercato delle criptovalute ha raggiunto lo stesso valore del colosso Amazon (come riportato da CryptoCoinsNews all'indirizzo https://www.ccn.com/600-billion-cryptocurrencies-now-worth-amazon/).

(*alternative coins*), che spesso implementano funzioni o caratteristiche aggiuntive a quelle originariamente ipotizzate dai creatori di Bitcoin. Tra esse vi sono un maggior livello di anonimato o la non tracciabilità delle transazioni (Monero, Zcash, DeepOnion), la possibilità di generare e gestire *smart contract* o creare *token* di sviluppatori terzi ospitati sulla medesima *blockchain* (Ethereum, NEO, Stratis), l'aumento della velocità dei trasferimenti e della scalabilità del sistema (Ripple, Stellar Lumens), nonchè la predisposizione per l'utilizzo tramite dispositivi dell'*Internet of Things* (IOTA).

Un ulteriore fenomeno che ha concorso al crescente interesse mediatico nei confronti del mondo delle criptovalute – iniziato negli anni precedenti ma definitivamente affermatosi nel corso del 2017 – è quello legato al *boom* delle c.d. ICO, acronimo di i*nitial coin offering*, come si può vedere nella **Figura 2**. Con questo termine, mutuato dalle IPO del tradizionale mercato azionario, si definisce l'offerta iniziale di un *digital asset* da parte di una società o di un gruppo di sviluppatori che intendano lanciare sul mercato un protocollo o un'infrastruttura tecnologica basata sul paradigma della *blockchain*: in questo caso, si offrono al mercato *token*, strumenti digitali che incorporano diritti, con l'obiettivo di ottenere capitali sotto forma di criptovalute[2]. Si tratta, in definitiva, di una via di mezzo fra un'offerta pubblica iniziale tradizionale e la già nota attività di *crowdfunding*. Si distinguono solitamente due diverse tipologie di ICO: la prima, prettamente economica, somiglia molto da vicino alle già citate offerte iniziali di acquisto di azioni (si parla, in questo caso, di *security token*, che si intendono come una partecipazione ad un progetto dove i benefici del tale, verranno ripartiti tra i vari possessori); la seconda, invece, commercializza un prodotto, permettendo agli acquirenti/investitori di testare, grazie all'utilizzo della moneta virtuale sottostante, quelle che saranno le funzionalità della stessa tecnologia che si sta per finanziare (si parla, in questo caso, di *utility token*, il cui utilizzo è necessario per usufruire dei contenuti/servizi della piattaforma su cui sono implementati).

[2] Secondo una ricerca pubblicata da Fabric Ventures e TokenData e riportata da Bunsiness Insider UK, nel corso del 2017 sarebbero stati raccolti più di 5,6 miliardi di dollari attraverso il lancio di 435 ICO, una somma considerevolmente maggiore dei "soli" 240 milioni raccolti nel 2016 (http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1?IR=T).

Figura 2 - *fonte TokenData*

A prescindere dalla diffusione esponenziale delle criptovalute e dall'aumento dei ricavi del lancio iniziale e del *trading* di *token* sui molti *exchanges* nascenti in rete e nel *deep web*, frequentati da interessati della prima ora e speculatori attratti dai facili guadagni, il paradigma tecnologico rappresentato dalla *blockchain* sembra ormai destinato ad avere un ruolo fondamentale nelle prossime fasi di sviluppo di settori quali la finanza, il mercato e la distribuzione di energia, la decentralizzazione di dati ed informazioni e la sicurezza dei sistemi.

Mentre da un punto di vista prettamente finanziario non era forse prevedibile un confluire così elevato di capitali nel giro di dodici mesi in un mondo quale quello delle criptovalute, che esiste ormai da un decennio e sembrava riservato ad un numero ristretto di utilizzatori dalle competenze superiori alla media, è facilmente comprensibile come la criminalità informatica abbia confermato nel 2017 il crescente interesse per alcuni dei vantaggi che la tecnologia *blockchain* offre – primi fra tutti la decentralizzazione ed il relativo anonimato – ed utilizzato la diffusione su più larga scala del fenomeno per generare nuovi metodi tesi ad ottenere profitti illeciti o sottrarre fondi virtuali ai legittimi detentori.

In ultimo, il sempre più frequente utilizzo, anche in occasione delle centinaia di ICO occorse nel 2017, di *smart contracts* per la distribuzione dei *token* e la loro gestione su *wallet* più complessi – come quelli *multi-signature* o quelli detenuti dagli *exchanges* – unitamente all'avverarsi di alcuni clamorosi incidenti ed episodi di *hacking*, ha confermato nel corso dell'anno la necessità di sviluppare ed implementare maggiori presidi di sicurezza e nuove procedure di *auditing* al fine di evitare la perdita od il furto di ingenti somme in criptovalute. Gli *smart contracts* infatti, programmi per computer in esecuzione sul registro generale, sono diventati una caratteristica fondamentale delle *blockchain* di seconda generazione come Ethereum o NEO. Questo tipo di programmi sono attualmente utilizzati per facili-

tare, verificare o applicare regole tra le parti in occasione delle ICO o nella fruizione dei servizi offerti dagli operatori del settore, consentendo l'elaborazione diretta e le interazioni con altri contratti intelligenti. Secondo uno studio condotto da ENISA nel dicembre 2016 sulla sicurezza della *blockchain*[3], questa tecnologia fornirebbe ad eventuali *hacker* una più ampia area di superficie per l'attacco e, quindi, la possibilità di generare una sorta di effetto domino su altre parti della medesima piattaforma.

È stato un anno dinamico e denso di avvenimenti rilevanti per il mondo delle criptovalute e, nei paragrafi che seguiranno, si proverà a sottolinearne alcuni aspetti di carattere generale.

2. Malware e criptovalute

Proseguendo con un *trend* già registrato nell'ultima edizione del Rapporto Clusit[4], la quasi totalità delle più recenti versioni di *ransomware* diffuse nel corso dell'anno prevedeva quale metodo di pagamento del riscatto e quindi di raccolta dei proventi del reato l'utilizzo di criptovalute. Tuttavia, nonostante la crescita di valore e la diffusione di Bitcoin, nel gennaio 2018 si ha avuto la conferma che Monero, una moneta nata da un *fork* della *blockchain* di Bytecoin e focalizzata su una maggiore protezione della privacy[5] dei suoi utilizzatori, è ormai divenuto lo strumento preferito per la raccolta ed il riciclaggio dei proventi delle richieste di pagamento di riscatto dei *ransomware* [6], come si può vedere nella **Figura 3.**

Il passaggio dall'utilizzo di Bitcoin a quello di Monero testimonia il tentativo, da parte degli *scammers,* di implementare un maggiore livello di anonimato mediante l'uso di una criptovaluta *privacy-oriented* e, così facendo, di contrastare la tracciabilità delle transazioni sulla blockchain di Bitcoin[7]. La differenza più importante di Monero a confronto con Bitcoin è rappresentata proprio dal protocollo internet di livello applicativo utilizzato, finalizzato a garantire una privacy decentralizzata che rendele transazioni, di conseguenza, quasi del tutto anonime.

Non a caso la crescita di Monero, a partire dal momento della sua creazione nel 2014, è stata spesso giustificata dalla sua diffusa adozione nelle nel *deep web* e nelle *darknet*.

---

3 ENISA, Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector (https://www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport).

4 Cfr. "Ramsonware: un flagello che prende di mira privati ed aziende", a cura di Fabio Panada e Holger Unterbrink, in Rapporto Clusit 2017 sulla sicurezza ICT in Italia, CLUSIT, p. 205 e segg.

5 A differenza di molte altre criptovalute che sono derivate dal Bitcoin, Monero si basa sul protocollo CryptoNight, un derivato dell'algoritmo CryptoNote e possiede differenze algoritmiche significative sull'offuscamento della Blockchain (https://it.wikipedia.org/wiki/Monero).

6 CfrNotizia resa da CNN Tech il 3 gennaio 2018 all'indirizzo http://money.cnn.com/2018/01/03/technology/bitcoin-popularity-criminals-monero/index.html.

7 Attraverso la consultazione di un blockchain explorer come https://blockexplorer.com, è possibile visualizzare o monitorare in tempo reale il saldo di un wallet Bitcoin, eventualmente utilizzato come destinazione per i fondi raccolti dalla campagna di ramsonware. La blockchain di Monero non offre la possibilità di seguire con la stessa tecnica le transazioni intercorse tra i suoi utenti.

Figura 3 - *Schermata del ramsonware MoneroPay*

Nel 2017, tuttavia, il *ransomware* non è stato l'unico strumento a disposizione dei cyber-criminali per conseguire guadagni illeciti a discapito degli utenti della rete. L'ascesa del valore di Bitcoin e delle criptovalute in generale ha dato una scossa importante al mondo finanziario, arrivando a modificare anche gli obbiettivi perseguiti dagli attacchi informatici. Con l'aumento del cambio di Bitcoin a sfavore delle valute tradizionali, anche le CPU dei dispositivi delle vittime di determinati tipi di *malwares* è divenuta profittevole, se fruttata per il *mining* – ovvero per la creazione di nuova criptovaluta attraverso la potenza di calcolo di un personal computer. Il risultato, dal punto di vista del dispositivo attaccato, è l'inconsapevolezza della minaccia: si passa, infatti, dall'essere vittime di estorsioni informatiche all'essere complici inconsapevoli dell'attività di creazione di valuta digitale.

Come riportato a fine dicembre da Nova[8], periodico di approfondimento tecnologico de Il Sole 24 ore, nell'ultimo periodo dell'anno, un team di ricercatori ha registrato proprio in Italia un'impennata di infezioni di un *malware* denominato *JS/CoinMiner*, che a dicembre avrebbe raggiunto nel nostro paese il picco del 38% delle infezioni totali, attestandosi di gran lunga al primo posto tra le minacce che insidiano gli utenti italiani[9]. Questo genere di *malwares* utilizza un codice Java Script che si diffonde attraverso contenuti infetti, inseriti fraudolentemente in banner pubblicitari presenti su siti affidabili o molto frequentati come le piattaforme di condivisione di video in violazione del diritto d'autore, o ancora propagati grazie a campagne di *phishing* via email. Una volta eseguiti, essi avviano un programma silente finalizzato alla generazione di valuta digitale grazie allo sfruttamento delle risorse del

[8] Cfr. http://nova.ilsole24ore.com/nova24-tech/bitcoin-cosi-i-nostri-computer-vengono-usati-come-minatori-a-nostra-insaputa/.

[9] Questi i dati rilasciati dai ricercatori di Eset all'indirizzo https://blog.eset.it/2017/12/italia-il-paese-piu-colpito-dalla-minaccia-del-coinminer.

sistema infettato. Deve aggiungersi che l'utente non sempre si accorge immediatamente dell'infezione e le *botnet* di questo genere possono arrivare a contare centinaia di migliaia di dispositivi violati ogni giorno.

Figura 4 - *parte del codice di Coinhive (Fonte Coinhive.com)*

Il *mining* di criptovalute tramite il personal computer di terzi ignari, in ogni caso, sembra essere diventato la nuova frontiera dello sfruttamento illecito delle risorse altrui – anche tramite la sola navigazione e senza la vera e propria installazione di software malevoli sui dispositivi degli utenti. Nell'autunno del 2017, infatti, si è assistito ad una nuova ondata di episodi di *coinmining*, che hanno interessato tra gli altri anche il famoso motore di ricerca dedicato al *file sharing* ThePirateBay. I proprieratari dei siti in questione avrebbero volontariamente utilizzato un codice Java Script malevolo denominato CoinHive[10]: poche righe di codice permettevano infatti di utilizzare la potenza computazionale delle centinaia di migliaia di visitatori giornalieri del sito per l'estrazione di Monero a loro insaputa (Figura 4).

Proprio durante la redazione del presente contributo, inoltre, è stata resa pubblica la notizia che anche siti governativi statunitensi e britannici sono stati infettati da codice malevolo che ha causato il *mining* inconsapevole di criptovalute[11].

3. Le ICO ed i problemi di sicurezza delle transazioni virtuali

Come se non bastasse, con l'aumento degli utenti della rete che attivamente acquistano e scambiano criptovalute e partecipano al lancio quasi quotidiano di centinaia di ICO, nell'autunno 2017 ha fatto la sua comparsa una nuova minaccia, questa volta indirizzata specificamente ai proprietari di *wallet* ed a coloro che, per la prima volta, si apprestano ad effettuare transazioni sulle *blockchain*. Scoperto da Kaspersky Lab alla fine di ottobre[12], questo nuovo ceppo di attacco informatico di tipo *clipboard hijacking*, denominato CryptoShuffler, utilizza una tattica relativamente semplice per sottrarre preziose valute digitali ai loro possessori: invece di sfruttare con un attacco decisamente invasivo la potenza compu-

10 Cfr. http://punto-informatico.it/4406715/PI/News/the-pirate-bay-ritorno-coin-hive.aspx.

11 Cfr. https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/.

12 Cfr. la press-release rilasciata da Kaspersky il 2 novembre 2017 all'indirizzo https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-discovers-cryptoshuffler-new-threat-that-seized-140k-in-bitcoin-savings.

tazionale della vittima, il *trojan* si limita con poche righe di codice a modificare le operazioni di copia e incolla.

In primo luogo, gli hacker compromettono il dispositivo dell'utente e il codice CryptoShuffler inizia a monitorare l'attività nella *clipboard*. Questo perché molti utenti copiano e successivamente incollano l'indirizzo del *wallet* del destinatario nei campi del relativo ordine della transazione, il che è più facile che ricordare l'intera stringa e spesso anche più sicuro che scriverlo manualmente, considerato la possibilità di generare errori[13]. CryptoShuffler semplicemente aspetta silente l'occasione propizia, fino a quando non rileva negli appunti le caratteristiche di stringa del *wallet* di una determinata criptovaluta. Il *malware* intercetta quindi la stringa contenente l'indirizzo del portafoglio copiato e la sostituisce con quella di un indirizzo di comodo, determinando l'invio dei fondi direttamente al *wallet* agli aggressori. Se un utente non controlla attentamente l'indirizzo del destinatario previsto e lo confronta con quello che il sistema ha effettivamente incollato, i cyber-criminali otterranno senza fatica l'illecito guadagno (dettaglio in **Figura 5**).

Figura 5 - *Dettaglio dei fondi dirottati nel mese di ottobre sul wallet utilizzato da CryptoShuffler (Fonte Kaspersky blog)*

Come osservato da Kaspersky Lab, l'efficacia di CryptoShuffler dimostra come molti *malware* di nuova generazione riescano a mantenere un basso profilo ed operare il più rapidamente possibile. Poiché, infatti, esso si annida silentemente in memoria ed effettua soltanto un monitoraggio temporaneo del processo di sistema dedicato alla funzione di copia e incolla, gli utenti non percepiscono alcun degrado delle prestazioni del dispositivo, né ricevono pop-up casuali o messaggi di riscatto. Dal momento che le transazioni sulla *blockchain* devono intendersi immutabili ed irripetibili, non vi è modo per le vittime di rientrare in possesso dei fondi.

[13] Si deve considerare che un indirizzo bitcoin – così come quello di altre criptovalute – sebbene abbia una funzione simile all'indirizzo e-mail e sia utilizzato per ricevere e inviare fondi sulla blochckain (così come si utilizza un indirizzo e-mail per inviare e ricevere messaggi) non è personalizzabile dall'utente ed è solitamente formato da una stringa, assegnata dal sistema, di 26-35 caratteri alfanumerici. Per fornire un esempio della rappresentazione grafica di un indirizzo relativo ad un wallet di criptovalute, si confronti l'indirizzo bitcoin dell'exchange Bitifinex, il secondo per valore di tutta la rete: "3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r".

Deve in realtà rilevarsi che, anche qualora l'utente verifichi attentamente l'esattezza sul proprio sistema dell'indirizzo di destinazione della transazione che sta per generare sulla *blockchain*, non è sempre detto che i fondi arrivino al soggetto al quale essi erano stati inizialmente destinati. Nel corso dell'anno con il più alto numero di ICO lanciate sul mercato, infatti, non sono mancati episodi fraudolenti di *phishing*, social *engineering* e persino vera e propria compromissione di siti web e canali di comunicazione che hanno originato transazioni errate per milioni di euro durante le innumerevoli campagne di raccolta fondi organizzate con l'utilizzo di criptovalute. Uno dei casi più clamorosi è quello relativo all'*hacking* occorso in occasione del lancio di Coindash nel luglio 2017[14]. La startup, attiva nel campo dei pagamenti e delle spedizioni aveva infatti lanciato una *initial coin offering* della propria moneta digitale, arrivando a raccogliere in poche ore circa 7 milioni di dollari. Purtroppo, pochi minuti prima del lancio della ICO, un ignoto hacker era penetrato abusivamente sul server che ospitava il sito web della compagnia ed aveva sostituto l'indirizzo *ethereum* indicato per l'invio dei fondi, facendo in modo che le contribuzioni venissero deviate su un *wallet* estraneo all'operazione. A riguardo è interessante evidenziare che, sebbene la società abbia immediatamente bloccato il prosieguo della ICO ed abbia promesso di inviare ugualmente i propri *token* a coloro che avevano tentato di partecipare ed avevano perso le somme versate, alcuni investitori hanno approfittato della situazione, evidentemente degenerata, continuando ad inviare fondi all'indirizzo hackerato ed aumentando il danno per Coindash sino a complessivi 10 milioni di dollari. L'incidente mette sicuramente in risalto le difficoltà attualmente affrontate dai pionieri della criptofinanza, che nonostante abbiano raccolto ingenti somme di denaro, devono evidentemente ancora superare le complessità di una tecnologia in fase iniziale.

Proprio le problematiche di sicurezza, conseguenza di un livello di programmazione ancora acerbo dei software di gestione della *blockchain*, del resto, hanno causato per ben due volte nel corso dell'anno tipologie differenti di incidenti – un *breach* fraudolento ed un *freeze* colposo – in danno della società Parity Technologies, che sviluppa soluzioni client multi-firma per la *blockchain ethereum*, per un danno totale di più di 300 milioni di dollari complessivi. I problemi sono iniziati nel mese di luglio, quando la startup con sede a Londra ha rilevato lo sfruttamento da parte di ignoti di una vulnerabilità nella versione 1.5 del suo *wallet*, con la conseguente perdita di più di 150.000 Ether dagli account degli utenti (dettaglio del wallet di Parity in **Figura 6**). Quando il *bug* è stato finalmente individuato nel codice del wallet *multi-signature*, aveva ormai compromesso la raccolta fondi in corso attraverso le ICO di diverse società.

[14] Il 17 luglio 2017 la notizia dell'hacking ai danni di Coindash è stata diffusa da numerosi media di settore, tra i quali il sito Coindesk all'indirizzo https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/.

Figura 6 - *Il wallet di destinazione dell'hacking in danno di Parity*

A novembre, tuttavia, Parity è stata costretta ad emettere un nuovo alert di sicurezza[15], annunciando un ulteriore incidente, questa volta apparentemente incolpevole e generato da una vulnerabilità intrinseca del codice, che ha creato danni ancora maggiori: un utente ha eliminato per sbaglio una libreria nel *repository* ospitato su Git-Hub del progetto, convertendo lo *smart contract* che regolava i portafogli multi-firma, trasformandoli in normali indirizzi di portafogli e diventandone inavvertitamente proprietario. L'utente, forse spaventato dall'accaduto, ha poi terminato questo contratto, rendendo tutti i *wallet* multi-firma legati allo stesso immediatamente inutilizzabili e i loro fondi bloccati per sempre[16].

Anche nei primi mesi del 2018, infine, le criticità riscontrate nella gestione degli *hot wallet*[17] di diverse altre *altcoin* sulle piattaforme di differenti *exchanges* hanno confermato il preoccupante trend negativo in tema di sicurezza dell'architettura dei *ledger* delle *blockchain* di seconda generazione, causando incidenti per centinaia di milioni di euro, che ad oggi ancora impegnano gli informatici e gli investigatori di mezzo mondo. Nel mese di gennaio ben 533 milioni di dollari in equivalente criptovaluta NEM sono stati sottratti da ignoti *hacker* dalla piattaforma di scambio Coincheck, la più grande e la più attiva in Giappone dai tempi di Mt.Gox. La notizia è rimbalzata sui media occidentali[18] e di conseguenza ha impattato il mercato, dando il via ad una profonda correzione.

[15] Reperibile all'indirizzo https://paritytech.io/security-alert-2/.

[16] Secondo le notizie trapelate nei giorni successivi i fondi immobilizzati dal freeze ammonterebbero ad un valore di circa 1 milione di Ether, per un equivalente di circa 280 milioni di dollari al cambio applicato al momento dell'incidente (Cfr. https://motherboard.vice.com/it/article/ywbqmg/qualcuno-ha-bloccato-per-sbaglio-300-milioni-in-ethereum).

[17] Un hot wallet è un portafoglio contenente criptovalute – nel caso di quelli a disposizione degli exchanges, condiviso tra più utenti – che è connesso ad internet e permette il deposito, il prelievo ed il trading delle monete digitali a cui è destinato. Gli exchanges affiancano solitamente ad esso un cold wallet, sconnesso dalla rete e protetto da maggiori misure di sicurezza, destinato a custodire i fondi in deposito a lungo termine.

[18] Cfr. Fortune del 29 gennaio 2018 (http://fortune.com/2018/01/29/coincheck-japan-nem-hack).

Durante la redazione del presente contributo, infine, giunge la notizia[19] del probabile incidente informatico di cui sarebbe rimasto vittima nel mese di febbraio 2018 l'*exchange* gestito dalla società italiana BitGrail S.r.l. di Firenze, all'esito del quale sembrerebbero essere stati sottratti 17 milioni di monete denominate Nano – nate dal *rebranding* della precedente criptovaluta Raiblocks, che nel corso dei mesi precedenti aveva centuplicato il proprio valore – per l'equivalente di quasi 200 milioni di dollari al cambio attuale. Al momento in cui si scrive, non è chiaro se l'origine dell'incidente sia da rinvenirsi in un problema tecnico legato alla programmazione della *blockchain* di Nano e della gestione dei portafogli, o di un *hack* del *wallet* assegnato all'*exchange* italiano.

Figura 7 - *Avviso dell'incidente del 9 febbraio 2018 (Fonte Bitgrail)*

Sicuramente, la diffusione delle notizie relative ai sempre più frequenti incidenti di sicurezza ed attacchi informatici ai danni degli operatori dell'ecosistema delle criptovalute ha contribuito all'attuale crisi del mercato sottostante – che ha dimezzato la capitalizzazione degli investimenti raggiunta alla fine del 2017 – portando a galla, unitamente ai temi legati alla regolamentazione di cui si tratterà nel paragrafo successivo, insormontabili questioni tecnologiche che dovranno essere corrette prima della diffusione di massa della *blockchain*.

[19] La notizia è stata diffusa il 9 febbraio 2018 dal titolare di Bitgrail, che con una nota sul suo sito ha raccontato l'accaduto: «da controlli di verifica interna di congruità delle operazioni di prelievo – è scritto - sono emerse delle transazioni non autorizzate che hanno portato ad un ammanco di 17 milioni di Nano costituenti parte dei portafogli gestiti da Bitgrail S.r.l. Per l'attività fraudolenta di cui sopra, è stata presentata in data odierna regolare denuncia querela presso le autorità di polizia competente e le indagini di polizia sono in corso».

4. Le sfide in tema di regolamentazione della blockchain

Se dal punto di vista prettamente tecnico informatico, il 2017 è stato l'anno della diffusione incontrollata e della esplosione della tecnologia *blockchain*, è altrettanto vero che l'anno che verrà sarà fondamentale per definire una strategia globale in tema di regolamentazione del mercato. Attualmente, infatti, il fenomeno risulta non regolamentato in maniera uniforme e gli attori istituzionali hanno più volte indicato la necessità di porre delle regole chiare che, se da un lato permettano uno sviluppo organico, dall'altro tutelino gli utenti dai pericoli di frodi finanziarie e perdita di fondi per mano di cyber-criminali.

Nel febbraio 2018 il Senato degli Stati Uniti d'America ha ascoltato, nel corso di una audizione pubblica, i presidenti della SEC (*Security Exchange Commission*) e della CTFC (*Commodity Futures Trading Commission*), che hanno confermato l'approccio diffidente nei confronti delle ICO – intorno alle quali – a parere dei regolatori statunitensi – graviterebbe un alto rischio di frodi finanziarie ed informatiche[20]. Lo stesso orientamento, nel precedente mese di luglio 2017, aveva portato all'emissione di un divieto, per i cittadini statunitensi, di partecipare a quasiasi *initial coin offering* che immettesse sul mercato *security token*, considerati prodotto finanziario e quindi in relazione ai quali veniva prevista una più stringente regolamentazione.
Allo stesso modo, nel mese di settembre 2017 la seconda nazione maggiormente interessata dal fenomeno legato all'esplosione delle criptovalute, la Cina, ha emesso un divieto temporaneo di proseguire le attività di *trading* nei confronti degli *exchanges* nazionali (tra i più attivi sul mercato globale di scambio delle monete digitali), impedendo parallelamente la partecipazione alla raccolta di fondi per il tramite delle ICO[21].

Le preoccupazioni maggiori, anche in Europa, sono dettate dal rischio che le criptovalute, muovendosi in un mercato non controllato e per il tramite di tecnologie nascenti ed in relazione alle quali non vi sono ancora procedure di sicurezza, possano favorire attività di riciclaggio e trasferimento di fondi provenienti da precedenti condotte illecite. Le caratteristiche di decentralizzazione e relativa intracciabilità delle transazioni, del resto, pongono il livello della sfida a cui sono chiamati i legislatori ad un gradino più alto rispetto alle tematiche della finanza tradizionale. La Banca Centrale Europea da sempre favorevole all'introduzione di una regolamentazione delle criptovalute, attende la discussione in sede G20 che si terrà a marzo 2018 in Argentina. Nel nostro Paese, il Governo ha già previsto nel decreto legislativo 25 maggio 2017 n. 90 (che ha rafforzato la normativa italiana antiriciclaggio) che i prestatori di servizi relativi all'utilizzo di valuta virtuale debbano assolvere agli

[20] Cfr. la trascrizione della deposizione del Presidente J. Christopher Giancarlo del 6 Febbraio 2018 innanzi al Senato degli Stati Uniti d'America, reperibile sul sito web della Commodity Futures Trading Commission all'indirizzo http://www.cftc.gov/idc/groups/public/@newsroom/documents/speechandtestimony/opagiancarlo37.pdf.

[21] Come riportato dal sito di Techcrunch il 4 settembre 2017 (cfr. https://techcrunch.com/2017/09/04/chinas-central-bank-has-banned-icos/).

obblighi antiriciclaggio per evitare che le transazioni effettuate con le criptovalute possano essere utilizzate per fini illegali. Un successivo decreto ministeriale attuativo è attualmente in predisposizione presso il Ministero dell'Economia e delle Finanze[22]: riprendendo la definizione introdotta dal decreto legislativo 25 maggio 2017, n. 90, il provvedimento in consultazione chiarisce che la valuta virtuale seppur "*utilizzata come mezzo di scambio per l'acquisto di beni e servizi" (…) "non è emessa da una banca centrale o da un'autorità pubblica, non è necessariamente collegata a una valuta avente corso legale*". Lo schema di decreto disciplina le modalità con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al ministero dell'Economia e delle Finanze la loro operatività. Sono inclusi nell'obbligo di comunicazione anche gli operatori commerciali che accettano le valute virtuali quale corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità. La previsione di obblighi e cautele a carico dei prestatori di servizi relativi alle valute virtuali è coerente con le più stringenti regole dettate dalla V direttiva Ue antiriciclaggio, ormai prossima alla pubblicazione sulla Gazzetta Ufficiale della comunità europea, di cui l'Italia ha di fatto anticipato l'adozione prevedendo già dal 4 luglio 2017 (data di entrata in vigore decreto legislativo 25 maggio 2017, n. 90), norme più rigorose in materia di prevenzione dei reati finanziari.

Il 2018 sarà pertanto, con buona probabilità, l'anno della definitiva affermazione delle criptovalute sulla scena economico finanziaria globale, soltanto se potranno dirsi definitivamente superate le incertezze emerse in tema di sicurezza della tecnologia e regolamentazione coordinata del fenomeno da parte delle istituzioni e della finanza tradizionale.

[22] Il testo della proposta ministeriale è reperibile all'indirizzo http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/regolamentazione_bancaria_finanziaria/consultazioni_pubbliche/31.01.18_bozza_DM_prestatori_val_virtuale_.pdf.

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phising***.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
Adware	Tipo di ***malware*** che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità ***spyware***.
AISP **Account Information Service Provider**	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.
Apt **(Advanced Persistent Treath)**	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	***Vulnerabilità*** che consente ad un attaccante di accedere a file tramite richieste Web remote.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.

Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
Blind signature	Tecnica utilizzata nell'ambito dell'*e-voting*. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi *DDOS*.
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo *DDOS*.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale, nel corso di indagini su alcuni specifici crimini.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.

CERT (Computer Emergency Response Team)

Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce.
Fra i principali obiettivi di un CERT (vedi CERT Nazionale):

- fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini
- incrementare la consapevolezza e la cultura della sicurezza;
- cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione;
- facilitare la risposta ad incidenti informatici su larga scala;
- fornire supporto nel processo di soluzione di crisi cibernetica.

Cifratura omomorfa

Tecnica utilizzata nell'ambito dell'*e-voting*.
Con questo sistema di cifratura è possibile sommare due numeri cifrati o compiere altre operazioni algebriche senza decifrarli.

CISP (Card-based Payment Instrument Issuing Service Provider)

Prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta, che potranno emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso Istituti di Credito diversi.

Cloud weaponization

Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.

Cognitive Security

Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.

Constituency

Nell'ambito di un *CERT* indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).

C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.
CSIRT Computer Security Incident Response Team	Struttura sostanzialmente simile ad un *CERT.*
Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.

Cyber security

Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".
lo scopo complessivo di questo insieme di discipline è il proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.

Cyber-weapon

Malware (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber (NATO Cooperative Cyber Defence Centre of Excellence).

Cryptolocker

Malware che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.

Deep Web

L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).

Defacement

Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.

DES
(Data Encryption Standard)

Algoritmo per la cifratura dei dati a chiave simmetrica.

DNS
(Domain Name System)

Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.

DNS Open Resolver

Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.

DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai ***DNS***.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti). • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di *C&C* si parla di ***DDOS*** (Destribuited Denial of Service).
DDoS (Distributed Denial of Service)	Attacchi ***DOS*** distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni ***malware*** per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server *C&C*.
DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.

Drive-by exploit kit

Il fenomeno dei drive-by ***exploit kit*** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli ***exploit kit***, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.

DRdos
(Destribuited Reflection Denial of Service)

Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco.
Questa tipologia di ***DDOS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.

Dual use

I prodotti a duplice uso sono beni e tecnologie che possono avere un impiego sia civile che militare, includendo prodotti che possono in qualche modo servire nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari.
(da Regolamento (CE) n. 428/2009 - regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso)

Eavesdropping

Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni

EDR
(Endpoint Detection and Response)

Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.

eIDAS	REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE finalizzato a garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari.
E-voting	Con l'espressione "sistema di e-voting" ci si riferisce al momento in cui una tecnologia elettronica è impiegata in una o più fasi di un processo elettorale, scrutinio compreso, senza che sia necessariamente sfruttata la rete Internet.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.

HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Infostealer	*Malware* finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.

Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
Intrusion software	***Spyware*** (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti ***dual use***). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
Istant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.
Keylogger	***Malware*** (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).

Man in the browser — Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.

MFU (Malicious File Upload) — Attacco ad un web server basato sul caricamento remoto di ***malware*** o più semplicemente di file di grandi dimensioni.

MitC (Man in the Cloud) *Definizione coniata dall'azienda Imperva.* — Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.

Mix-nets schemi — Tecnica utilizzata nell'ambito dell'*e-voting*.
Gli schemi di voto mix-nets sono sistemi basati su insiemi di server con cui è possibile crittare e permutare i voti espressi, in modo da rendere pressoché impossibile ricostruire la coppia voto-elettore.

Mules — Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.

NIS (Direttiva)

NTP (Network Time Protocol) — *Protocollo* che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.

Overlay spyware

OTP (One Time Password) — Dispositivo di sicurezza basato sull'uso di password utilizzabili per una sola volta, di norma entro uno spazio temporale limitato.

Payload — Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.

Password hard-coded — Password inserite direttamente nel codice del software.

Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI **Protected Health Information**	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phising	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood:	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una ***botnet***, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PISP **(Payment Initiation Service Provider)**	Prestatori di servizi di disposizione di ordini che trasmettono un ordine di pagamento emesso da un cliente che detiene un conto online presso un Istituto di Credito a favore di un conto di un beneficiario o operatore commerciale (e-merchant).
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.

PSD2 **Direttiva 2015/2366/(UE) sui servizi di pagamento nel mercato interno (cd. PSD2)**	DIRETTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE che stabilisce le regole in base alle quali gli Stati membri distinguono le varie categorie di prestatori di servizi di pagamento.
QTSP **(Qualified Trust Service Provider)**	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
Ransomware	*Malware* che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware,).
RDP **(Remote Desktop Protocol)**	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server)
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Rootkit	*Malware* che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.

Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
Spear phishing	*Phishing* mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	*Malware* che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	*Protocollo* che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.

SSH (Secure Shell)	*Protocollo* cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
TOR	Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).

Trojan horse	*Malware* che si installa in modo occulto su un dispositivo con diverse finalità, quali ad esempio raccogliere informazioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come ***prestatore di servizi fiduciari qualificato*** o come prestatore di servizi fiduciari non qualificato.
UPD Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	*Protocollo* di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Vulnerabilità	Debolezza intrinseca di un asset (ad esempio un'applicazione software o un ***protocollo*** di rete) che può essere sfruttata da una minaccia per arrecare un danno.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization:	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.

XSS (**Cross Site Scripting**)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.

Gli autori del Rapporto Clusit 2018

Andrea Antonielli, laureato in Giurisprudenza presso l'Università degli Studi di Milano nel 2016. È Ricercatore presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy, con particolare focus sulla normativa europea in materia di protezione dei dati personali.

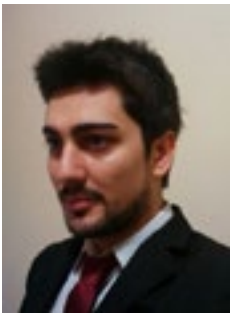
Luca Bechelli, Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Dal 2007 è membro del Consiglio Direttivo e del Comitato Tecnico Scientifico del Clusit, con delega su Tecnologie e Compliance. Svolge attività di divulgazione su tematiche di sicurezza IT, mediante la partecipazione a convegni, la pubblicazione di articoli su testate generaliste o di settore e la partecipazione a gruppi di lavoro.

Francesca Bosco si è laureata a pieni voti in giurisprudenza ed ha iniziato a lavorare nel 2006 presso l' UNICRI (United Nations Interregional Crime and Justice Research Institute), dove svolge il ruolo di program officer. Ha acquisito esperienza nei programmi di contrasto alla criminalità informatica ed alla criminalità organizzata. È attualmente responsabile dei programmi relativi alla sicurezza informatica e all'uso improprio della tecnologia, tra cui l'utilizzo terroristico di internet. Sta approfondendo la ricerca in tema di sfide e opportunità delle nuove tecnologie, tra cui la robotica e l'intelligenza artificiale, la blockchain, i big data e il quantum computing. È membro dell'Advisory Group dello European Cybercrime Center (EC3) presso l'Europol. È co-fondatrice del Tech and Law Center.

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Security manager, project manager e auditor presso gruppi bancari e consulente in ambito sicurezza e privacy. Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate. Ha pubblicato 21 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico, GDPR, Blockchain, di ISACA/AIEA, di Oracle Community for Security, di UNINFO sui profili professionali privacy; è fra i coordinatori di europrivacy.info. È membro della faculty di ABI Formazione per il quale fra gli altri ha curato il Percorso professionalizzante Privacy Expert e DPO in banca. È docente presso ITER, ISACA/AIEA, CLUSIT, Convenia, Informa Banca, CETIF, IKN, Università Statale di Milano. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMBCI.

Nunzia Ciardi, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con una pregressa pluriennale esperienza, maturata prima come Direttore della I Divisione del Servizio Polizia Postale e successivamente come Dirigente del Compartimento Polizia Postale e delle Comunicazioni del Lazio, coordina attualmente le unità specializzate della Polizia di Stato nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale.
È membro dell' European Union Cybercrime Taskforce di Europol e del Progetto europeo EU-OF2CEN per l'adozione di strategie comuni contro il crimine organizzato nel settore delle frodi on-line. È coordinatore e membro di gruppi di lavoro sulla tutela dei minori nel mondo della comunicazione, sulla disinformazione in ambito di piattaforme digitali, e sulla sicurezza digitale. È rappresentante del Ministero dell'Interno in seno al Nucleo sicurezza cibernetica ed al Tavolo Tecnico Cyber. Svolge attività di docenza presso le scuole di Polizia e numerosi Enti.

Davide Del Vecchio, membro del direttivo Clusit, lavora in ambito Cyber Security da circa 15 anni. Negli anni ha lavorato come ricercatore indipedente, ethical hacker, incident handler e SOC manager ed è attualmente il responsabile della Cyber Security di una grande multinazionale italiana. È co-fondatore del "Centro Hermes", associazione no-profit che si occupa di trasparenza e diritti digitali e nel 2014 ha vinto il premio Fibonacci come "miglior informatico dell'anno".



Luca Dinardo, laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2008, consulente in ambito Cyber Security da 10 anni. Lavora in Lutech dal 2015, specializzato in tematiche di Cyber Security in contesti CERT e SOC, si occupa attivamente di Cyber Threat Intelligence, Malware & Threat Analysis, Incident Response e Cyber Deception. Svolge attività di ricerca e sviluppo mirate all'analisi ed al contrasto di fenomenti legati al Cyber Crime.

Luca Dozio, laureato in Ingegneria Gestionale al Politecnico di Milano. Lavora come Ricercatore per gli Osservatori Digital Innovation del Politecnico di Milano sulle tematiche del Cloud e dell'Information Security.

Giorgia Dragoni si è laureata in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, con una Tesi sull'evoluzione di ruoli e competenze all'interno delle Direzioni ICT.
È Ricercatrice presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy e ai Big Data Analytics.

Francesco Faenzi, laureato in Scienze dell'Informazione, certificato CISSP, CISA, SANS GCIH e ITIL , è Head of Cyber Security Business Platform in Lutech. È stato Security Advisor e Head of IT Security Technologies Team in Securteam (oggi parte di Leonardo) fino al 2001. Ha poi continuato in Lutech, dove dirige i professional service, il business development, la ricerca e innovazione in generale in ambito Cyber Security e con particolare focus su Cyber Threat Intelligence, Breach Detection and Incident Response, Ethical Hacking, Governance Risk & Compliance, Cybersecurity by Design, Data Classification & Encryption, Telco Backbone Protection. Ha partecipato a progetti europei quali DRIVE, CANDELA, C2-SENSE e cura personalmente il Security Advisoring di grandi clienti. Speaker in numerose conferenze ed eventi (GCSEC, CLUSIT, ABILAB, ANIMP, ANIPLA, EECTF), è anche uno degli autori del libro Mondadori "La sicurezza dei sistemi informativi: teoria e pratica a confronto".

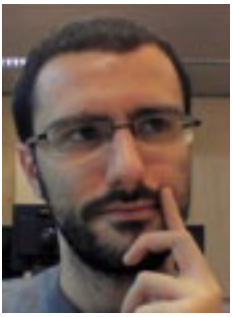
Gabriele Faggioli, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital360 Company di cui è socio e amministratore). È Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica).
È Responsabile Scientifico dell'Osservatorio Security&Privacy del Politecnico di Milano. È Adjunct Professor del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui, da ultimo, "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.co dell'anno".

Sergio Fumagalli è responsabile della Practice Data Protection di P4I, società di management consulting del Gruppo Digital360. È membro del direttivo di Clusit e del coordinamento di Europrivacy.info. Dal 2004 al 2012 è stato Vice Presidente del Cda di Webank Spa. Dal 1996 al 2001 è stato Deputato al Parlamento e Segretario della XIII Commissione Attività produttive. Co-autore delle pubblicazioni della Oracle Community for Security sui temi Fascicolo Sanitario Elettronico, Privacy nel cloud, Security e social media, Le frodi nella rete, è co-autore del testo "Privacy guida agli adempimenti", IPSOA 2004 (seconda editione 2005). È laureato in Fisica presso l'Università di Milano.

Marco Tullio Giordano è Avvocato dal 2008 ed esercita la professione presso il Foro di Milano, occupandosi prevalentemente di diritto penale delle nuove tecnologie, con particolare riguardo alla sicurezza informatica, alla protezione dei dati personali ed alla responsabilità di privati ed aziende in rete. Ha partecipato ad alcuni dei primi processi penali in tema di *cybercrimes* e violazione della privacy in Italia. Dal 2009 gestisce i rapporti con le Autorità Giudiziarie per alcune delle più conosciute *web companies* italiane ed internazionali e si occupa della formazione e dell'assistenza alle Forze di Polizia Giudiziaria in tema di richiesta di prestazioni obbligatorie agli Internet Service Provider e richieste di dati informatici attraverso le procedure previste dai *Mutual Legal Assistance Treaties*. È cultore della materia presso la cattedra di informatica giuridica della facoltà di Giurisprudenza dell'Università degli Studi di Milano Bicocca ed ha partecipato, in qualità di docente e relatore, a numerosi eventi formativi aventi ad oggetto il diritto delle nuove tecnologie. Ha conseguito la certificazione ISO Foundation per la gestione della sicurezza delle informazioni ed è *lead auditor* certificato UNI CEI ISO/IEC 27001:2014. Presta la propria consulenza in tema di *compliance privacy* e *cybersecurity* in favore di numerose aziende italiane. Iscritto alla Camera Penale di Milano, ha fatto parte del comitato di redazione dell'omonimo sito web. È autore di pubblicazioni specialistiche in tema di reati informatici. Scrive online di diritto e nuove tecnologie.

Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi è esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, membro per i mandati 2010-2012, 2012-2015 e 2015-2017 del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), membro del Comitato Direttivo di Clusit. In trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di *audit* ed *assessment*, e progettato infrastrutture di sicurezza e *trust*, presso grandi aziende e pubbliche amministrazioni. Collabora da oltre quindici anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del *cybercrime* e del cyberterrorismo. Ha collaborato con l'Ufficio delle Nazioni Unite su progetti internazionali di contrasto alla cybercriminalità. Insegna in diversi corsi di Laurea e di Master presso varie università italiane. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri.



Andrea Granata, Cyber Security Specialist presso Communication Valley Reply, si occupa delle attività di prevenzione, analisi e gestione degli incidenti informatici e contrasto al Cyber Crime presso il Cyber Security Command Center (CSCC) di Communication Valley Reply. Ha una pluriennale esperienza come Security Tester, Fraud Expert e Security Data Analyst, con particolare attenzione ai temi della Malware Analysis, del Reverse Engineering e della Cyber Threat Intelligence. Collabora alla stesura del bollettino mensile ABI LAB focalizzato sui principali fenomeni di Phishing e malware rilevati a livello italiano ed è attualmente impegnato nelle attività di ingegnerizzazione ed erogazione dei servizi antifrode.

Michele Onorato oggi è Security Office Manager di Hitachi Systems CBT S.p.A. Vanta un'esperienza di oltre 10 anni nel settore dell'Information Technology e della Sicurezza Logica in particolare, con una carriera manageriale che gli ha permesso di assumere crescenti responsabilità sino a divenire anche punto di riferimento per le aziende partner del Systems Integrator Giapponese dall'anima italiana. Con una laurea in Matematica e una profonda esperienza tecnica, Michele vanta oltre 14 certificazioni e numerosissimi progetti in ambito security per realtà di rilievo, come SIAE o Ministero della Pubblica Istruzione, ma anche ruoli manageriali in importanti player del mercato IT europeo, quali Sistemi Informativi e Visiant Security. Come Security Department Manager di Hitachi, oggi Onorato ha la responsabilità di guidare un team altamente specializzato con la mission di aiutare quotidianamente le aziende private e pubbliche di grandi e medie dimensioni nell'implementazione di progetti di Cyber Security e Compliance, tramite l'erogazione di servizi gestiti ed utilizzando le migliori soluzioni tecnologiche presenti sul mercato.

Stefano Orciari, appassionato di tecnologia e matematica fin dall'età di 10 anni, intraprende il percorso di studi in Informatica presso l'Università degli Studi di Milano Bicocca specializzandosi in sicurezza e crittografia, conseguendo poi nel 2008 il Dottorato di Ricerca. Da 10 anni lavora e coordina numerosi progetti nel campo della sicurezza informatica. Da sempre interessato al cybercrime, è attualmente responsabile del Cyber Security Operation Center e dell'unità antifrode di Fastweb.

Marco Pacchiardo è Senior Enterprise Security Architect EMEA per Akamai Technologies. Ha iniziato la sua carriera nella sicurezza informatica nel 1995, lavorando per diverse aziende italiane tra cui Siosistemi, dove ha avuto modo di sviluppare nuove funzionalità di sicurezza e ampliare il portfolio aziendale. Successivamente è entrato a far parte di INS, in qualità di Principal Security Consultant. In questa posizione si è occupato di supporto ai clienti a livello globale e ha avuto l'opportunità di collaborare con aziende ed enti governativi su attività e progetti legati alla sicurezza informatica, alla compliance e al risk management. É poi approdato in BT Italia, dove ha lavorato con l'obiettivo di ottimizzare e consolidare il posizionamento dell'azienda relativamente alla sicurezza. Marco è autore di due libri, *Intranetworking* (1998) e *Azienda Sicura* (2003) e nel corso della sua carriera ha avuto modo di ideare e progettare innovativi servizi di sicurezza, compliance e risk management.

Pamela Pace è Amministratore unico della Obiectivo, advisory company specializzata nella gestione dell'information security che propone un'offerta di servizi di Cyber Security Strategy, Information Security Governance, Risk Intelligence, Risk Management. Negli anni ha rivestito molteplici incarichi di crescente responsabilità nel campo dell'information security, dell'innovazione e delle tecnologie. È componente della Commissione Tecnologie, Sicurezza e Mobile Payment dell'Associazione Italiana Istituti di Pagamento e Moneta Elettronica, Vicepresidente della Piccola Industria di Unindustria e componente del Comitato Tecnico Nazionale Ricerca ed Innovazione di Confindustria. È inoltre membro del comitato direttivo del Centro Ricerche Nuove Tecnologie e Processi di Pagamento

dell'Università degli Studi Internazionali di Roma e Docente del corso "La Gestione della Sicurezza delle Informazioni a Tutela del Patrimonio Aziendale" presso la Business School Scuola di Palo Alto.

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, Presidente di Associazione informatici Professionisti - AIP, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

Andrea Piazza ricopre il ruolo di WW Cybersecurity Architect, Chief Security Advisor in Microsoft, collaborando allo sviluppo dei servizi di cybersecurity di consulenza e supporto, alla formazione dei team di consulenza e al miglioramento della qualità dei progetti di sicurezza e delle attività di risposta agli incidenti. Nei 17 anni in cui ha lavorato in Microsoft, ha svolto il ruolo di Technical Account Manager e successivamente di Security Premier Field Engineer, dove ha ricoperto mansioni di crescente responsabilità da Tech Lead Italia, a Tech Lead EMEA, a Technology Manager EMEA. Dal 2014 è stato National Security Officer della filiale italiana di Microsoft, dove ha coordinato le attività volte a promuovere la consapevolezza e l'adozione delle tecnologie di sicurezza da parte dei clienti, gestendo i rapporti sulle tematiche di sicurezza e cybersecurity con le government élites, i leader accademici e i decisori pubblici, nonché con i responsabili e i team di sicurezza delle

aziende italiane. A livello EMEA ha coordinato i servizi di sicurezza del supporto Microsoft, come Security Assessment, Workshop, attività di risposta agli incidenti e di remediation, si è occupato in prima persona dell'attività di formazione e aggiornamento degli engineer di sicurezza, e collaborato con i team di sviluppo dei servizi di sicurezza Microsoft. In Microsoft ha collaborato al whitepaper "Mitigating Pass-the-Hash Attacks and Other Credential Theft-Version 2". Collabora al Comitato di Redazione de "Il Documento Digitale", ed ha partecipato alla redazione delle linee guida UNICRI 2015 per le PMI e ai rapporti CLUSIT 2016 e 2017. È certificato CISSP, ISO27001 Lead Auditor e ITIL.

Alessandro Piva si occupa da oltre dieci anni di ricerca sui temi dell'innovazione digitale. Dopo essersi laureato in Ingegneria delle Telecomunicazioni ed Ingegneria Gestionale al Politecnico di Milano, ha conseguito un Executive Master in Business Administration presso il MIP. Attualmente è Direttore di svariati Osservatori del Politecnico, quali l'Osservatorio Information Security & Privacy, l'Osservatorio Artificial Intelligence, l'Osservatorio Cloud Transformation.

Domenico Raguseo è Manager del team europeo di Technical Sales per IBM Security. Ha 19 anni di esperienza manageriale e 27 nel campo della cybersecurity in diverse aree. Domenico collabora con alcune università nell'insegnamento di Service Management e del Cloud Computing. Domenico è IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è stato speaker su Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

Marco Raimondi, nato nel 1987, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Ha iniziato la sua carriera nell'ambito IT per poi orientare la sua attività nel mondo commerciale, con un focus particolare sul mercato Enterprise. Dal 2012 ha lavorato presso Vodafone Italia dove ha ricoperto nella Business Unit Enterprise dapprima il ruolo di Presales e successivamente il ruolo di Marketing Product Manager nel mercato delle PMI. Dal 2017 in Fastweb ricopre il ruolo di Product Manager responsabile dello sviluppo di servizi di sicurezza per il mercato Enterprise e del supporto alle attività di Go to Market.

Pier Luigi Rotondo si occupa di Technical Enablement per IBM Security. Con una laurea in Scienze dell'Informazione presso l'Università degli Studi di Roma "La Sapienza", ha ricoperto per oltre dieci anni incarichi di docenza presso università Italiane, tra cui il Master in Sicurezza delle Informazioni dell'Università di Roma "La Sapienza", e corsi di Dottorato per l'Università degli studi di Perugia. Organizza in per l'Italia alcuni degli eventi dell'iniziativa European Cyber Security Month, dell'Unione Europea, divulgando regole pratiche per il contrasto delle frodi online. È stato istruttore nella prima CyberChallenge nazionale, programma di addestramento alla cybersecurity per giovani di talento, e afferisce al Cyber Security National Lab.

Rodolfo Saccani, Security R&D Manager in Libra Esva, vive l'IT dal 1994, in qualità di sviluppatore, sistemista, consulente e project manager. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della *security*, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero.
In Libraesva coordina la ricerca e sviluppo per l'e-mail security.

Luca Sangalli si è laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2015 e da allora lavora presso Lutech occupandosi di tematiche di Cyber Security come Cyber Threat Intelligence Analyst, Researcher & Developer ed Ethical Hacking, specializzandosi in particolare nell'ambito Finance. Si occupa anche di attività di ricerca e sviluppo in contesto antifrode.

Federico Santi, Security Principal – South EMEA in DXC.technology, inizia la sua carriera in ambito sicurezza nel 2000, prima di assumere il ruolo di Security Principal per il Sud Europa in Hewlett Packard Enterprise, ha lavorato in Andersen e Deloitte fino ad assumere il ruolo di Director dei Security Services.La sua esperienza nella Security segue una vista risk & business-oriented centrando l'attenzione su processi (Security Monitoring & Incident Management), dati (Data Protection & Privacy) e utenti (Identity Governance). Tra le responsabilità principali Strategic Advisory, Relazioni Istituzionali e Go To Market. Numerose le collaborazioni accademiche (Università Nazionale di Milano, La Sapienza, Tor Vergata). In particolare è attualmente membro del Comitato Strategico del Centro di Ricerca e Sviluppo sull'E-Content dell'Università di Tor Vergata di Roma. Attiva partecipazione ai principali tavoli europei (collaborazione con la Commissione Europea per la NIS Platform e l'Organizzazione Europea per la Cyber Security - ECSO) e nazionali (DIS, CNR, CLUSIT, AIEA, AIIC). Ha sviluppato i suoi 20 anni di esperienza in contesti internazionali, in particolare Italia, Spagna, Francia ed Africa ed ha seguito con una particolare attenzione i contesti del Settore Pubblico e dell'Energy & Utilities.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Già Chief Executive Officer de iDIALOGHI, negli anni si è occupata di Social Media Security, ICT Security Training e di Servizi di Sicurezza Gestita, quali Vulnerability Management, Mobile Security e Threat Intelligence. Membro del Comitato Tecnico Scientifico di CLUSIT, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori del paper "La Sicurezza nei Social Media" pubblicato nel 2014 dalla Oracle Community for Security. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale e nazionale.

Claudio Telmon, Adviser e consulente da più di vent'anni nel campo della sicurezza e della gestione del rischio IT, è membro del Comitato Direttivo e del Comitato Tecnico di Clusit.

Mario Terranova, specializzato in Ingegneria dei sistemi di controllo e calcolo automatico presso "La Sapienza" di Roma nel 1979 e docente presso questa università dal 1980 al 1996, è dirigente dal 1998. È stato consulente di primarie società, tra cui Alenia, Urmet e Cap Gemini, occupandosi di basi di dati, sistemi distribuiti, reti locali, sicurezza informatica, crittografia e firma digitale. Per quest'ultima è stato rappresentante italiano a Bruxelles. Oggi è responsabile dell'Area Sistemi, tecnologie e sicurezza informatica dell'Agenzia per l'Italia Digitale, nonché del CERT-PA.

Girolamo Tesoriere si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari. 10+ anni di esperienza nel settore delle TLC con una specializzazione nella consulenza sui servizi di Network Security e Cyber Security. Dopo aver lavorato per diversi anni come Technical Consultant in ambito networking e reporting operativo, nel 2013 partecipa allo start-up del Security Operations Center Enterprise di Fastweb. Ha lavorato per Eni come Cyber Security Engineer e al momento occupa la posizione di Enterprise Security Architect in Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

Enrico Tonello, laureato in ingegneria a Padova, è socio co-fondatore di TG Soft S.a.s. Da sempre attento agli aspetti di sicurezza informatica ed in particolare agli attacchi da virus&malware, è autore di numerosi articoli su virus&malware informatici pubblicati su alcune delle principali riviste italiane del settore e relatore in conferenze e seminari sui virus&malware informatici realmente circolanti come Security Evangelist. È co-autore della suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft.

Gianfranco Tonello, laureato in ingegneria informatica a Padova, è Malware Analyst e CEO di TG Soft. È riconosciuto a livello internazionale quale analista di virus&malware di nuova generazione e sviluppatore di tecnologie AntiMalware. Dal 1990 è analista di Virus/Malware con pubblicazione di analisi tecniche presso il VTC (Virus Test Center) dell'Università di Amburgo e su numerose riviste italiane. È Autore/Sviluppatore di software, specializzato nella produzione di tecnologie AntiVirus-AntiSpyware-AntiMalware. È docente CLUSIT. È analista/reporter della WildList, che individua i virus/malware on the wild cioè realmente circolanti a livello mondiale. È membro di AMTSO (Anti-Malware Testing Standards Organization), di VIA (Virus Information Alliance di Microsoft) e di MVI (Microsoft Virus Initiative).

Giuseppe Vaciago è Avvocato, iscritto all'Ordine degli Avvocati di Milano dal 2002. Le aree di specializzazione sono il diritto penale delle nuove tecnologie e il diritto penale societario. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore dell'information technology. Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha partecipato a numerosi convegni presso le più prestigiose Università italiane ed estere. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia. È membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes", "Digital Forensics" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01". È membro dell'Organismo di Vigilanza di Procter & Gamble Italy S.p.A., Whirlpool S.p.A, Duracell, Labocos S.r.l., Team System S.r.l., Gruppo Ospedaliero San Donato.

Andrea Vallavanti è ICT Manager del Rigassificatore di Livorno OLT, una delle realtà industriali Italiane OFFSHORE (FSRU – floating storage regassification Unit) dedicate alla trasformazione del gas naturale (LNG) In questo ruolo ha acquisito significative esperienze in ambito ICT Maritime. Prima del mondo Oil&Gas ha ricoperto posizioni di senior Project Manager IT nel mondo Energy in EON Italia dove si è occupato della reingegnerizzazione delle rete SCADA ed IT manager in Endesa Italia nella gestione di progetti TLC volti alla completa autonomia societaria. Ha inoltre ricoperto ruoli di responsabilità in Elettrogen nel distacco tecnologico dai sistemi di telecomunicazioni su power over line ed in ENEL, come specialista di Elettroregolazioni. Viene aggiunto alla sua esperienza lavorativa, un periodo di insegnamento nella Scuola Pubblica Superiore ed una collaborazione con l'Università Cattolica del S. Cuore di Piacenza.

Alessandro Vallega lavora in Oracle con il ruolo di Business Development Director e si occupa a livello EMEA (Europe, Middle East and Africa) di Security e di GDPR (regolamento EU 679/2016 sulla protezione dei dati personali) . È il responsabile della Oracle GDPR War Room (EMEA - Tech). È il fondatore e il coordinatore della Oracle Community for Security. È coautore, editor o team leader di una decina di pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Nel 2015 ha fondato insieme a Clusit e ad Aused un osservatorio permanente sul GDPR chiamato EuroPrivacy.info. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. È socio AIEA, CSA Italy e membro del Consiglio Direttivo di Clusit.

Giancarlo Vercellino è Research Manager, IDC Local Research, dove si occupa di ricerca per clienti nazionali e internazionali del settore IT, con particolare focus in area software applicativo. Prima di raggiungere IDC, Giancarlo ha lavorato come market analyst e business manager presso diverse fondazioni e centri ricerca e ha insegnato economia presso il Politecnico di Torino. Giancarlo si è laureato con lode presso l'Università di Torino, ha un Master in gestione strategica dell'IT presso il Politecnico di Torino, un Phd in economia industriale al Politecnico di Milano e ha frequentato i corsi di MBA della Anderson School of Management, University of California, Los Angeles.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa e autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar e i Seminari CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 13ª edizione.
- Le Conference specialistiche: Security Summit (Milano, Treviso, Roma e Verona).
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT e le Pillole di Sicurezza.
- I Gruppi di Lavoro: con istituzioni, altre associazioni e community.
- Il progetto "Rischio IT e piccola impresa", dedicato alle piccole e micro imprese.
- Progetto Scuole: la Formazione sul territorio.
- Rapporti Clusit: Rapporto annuale sugli eventi dannosi (Cyber crime e incidenti informatici) in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT P.A., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (Interna-

tional Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
Certificata dalla folta schiera di relatori (più di 500 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 15.000 partecipanti, e sono stati rilasciati circa 10.000 attestati validi per l'attribuzione di oltre 16.000 crediti formativi (CPE).
Tutte le sessioni prevedono il rilascio di Attestati di Presenza e danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.

La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione e organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

L'edizione 2018

La decima edizione del Security Summit si tiene a Milano dal 13 al 15 marzo, a Treviso il 16 maggio, a Roma il 6 e 7 giugno e a Verona il 4 ottobre.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882.
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: http://www.securitysummit.it/
- Foto reportage: https://www.facebook.com/groups/64807913680/photos/?filter=albums
- Video riprese e interviste: http://www.youtube.com/user/SecuritySummit

In collaborazione con

F-Secure

panda

TREND MICRO

Research Partner

IDC

Il presente Rapporto è stato prodotto in occasione del

EUROPEAN CYBER SECURITY MONTH

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT 10 ANNI

www.securitysummit.it