[Ermanno Goletto](#)
Microsoft Most Valuable Professional
Microsoft Certified

Ricariche USB pubbliche e sicurezza

Introduzione

Ormai è consuetudine avere con noi uno o più device che ci permette di operare in mobilità sia per ragioni di lavoro che per motivi personali. Si pensi ad esempio a notebook, tablet, ebook e ovviamente smartphone, questi device vengono spesso utilizzati parecchie ore e quindi non è insolito avere necessità di ricaricarli per poter continuare ad utilizzarli o mentre li si utilizza.

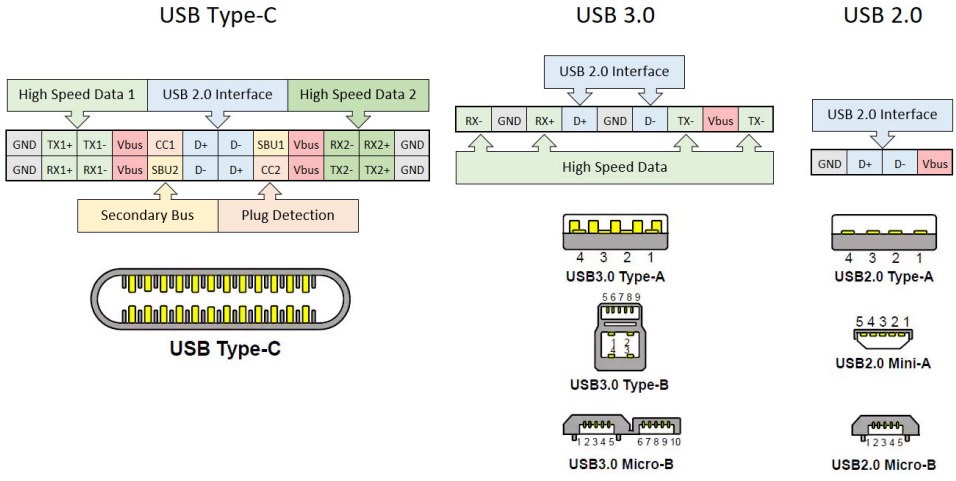
Per questo motivo già da qualche anno hanno fatto la loro comparsa le colonnine per ricarica USB in vari luoghi come centri commerciali, supermercati, hall degli alberghi, locali pubblici, aeroporti, stazioni, mezzi pubblici e ultimamente anche integrate in arredi urbani innovativi concepiti per progetti di Smart City come ad esempio panchine e pensiline.

Sebbene le ricariche USB pubbliche possano sembrare estremamente comodi e utili per chi ha necessità di ricaricare i propri device occorre però considerare che connettere un device tramite USB ad un apparato può comportare problematiche di sicurezza.

Attacchi di tipo Juice Jacking

Lo scorso anno nell'articolo [Tecniche di attacco e difesa contro l'utilizzo di dispositivi USB](#) ci eravamo concentrati sugli attacchi che un device può subire quando un attaccante connette ad un device una chiavetta USB infetta o progettata per compromettere o danneggiare il device.

Negli attacchi di tipo **Juice Jacking** sebbene il vettore di attacco sia sempre il canale USB, il possessore del device si connette ad un apparato di ricarica che è stato compromesso precedentemente da un attaccante con l'obbiettivo di violare o danneggiare i device che verranno connessi per ricaricarsi. Alla base dell'attacco sta nel fatto che il cavo che spesso si utilizza per ricaricare un device è un cavo dati che ha quindi la possibilità oltre che di ricaricare il device anche di permettere un eventuale comunicazione tra device e dispositivo di ricarica. Infatti un classico connettore USB prevede d pin dedicati all'alimentazione e due dedicati al trasferimento dati, nei nuovi standard USB 3.0, 3.1 o USB Type-C sono poi presenti più pin dedicati ad altre funzioni.



Grazie a questa connessione dati una stazione di ricarica compromessa potrebbe scaricare dati dal device o caricare un malware nel device.

Questo tipo di attacchi è in realtà noto da tempo, infatti già nel **2011** durante la conferenza DEF CON 19 erano state predisposte delle stazioni di ricarica per smartphone gratuite che avvertivano chi tentava di utilizzarle delle potenziale pericolosità. Durante la DEF CON 19 almeno 360 partecipanti collegarono i loro smartphone al chiosco di ricarica costruito dagli stessi ragazzi che gestiscono il "Wall of Sheep" ovvero il tabellone su cui sono pubblicati i furti di credenziali che sono stati eseguiti durante la manifestazione ai danni dei partecipanti meno accorti. A riguardo si veda Beware of Juice-Jacking.

Nel **2012** ricercatore Kyle Osborn ha rilasciato un framework di attacco chiamato P2P-ADB che utilizzava USB On-The-Go (una specifica dell USB 2.0 che permette la connessione drive free tra device) per connettere lo smartphone di un attaccante al device di una vittima. Tale framework includeva esempi e proof of concepts con il quale un attaccante può sbloccare telefoni bloccati, rubare dati da un telefono, incluse le chiavi di autenticazione che consentono all'attaccante di accedere ad esempio all'account Google. Per maggiori informazioni si veda Hak5 1205 – Extreme Android and Google Auth Hacking with Kos.

Nel **2013** durante la conferenza Blackhat USA 2013 studenti e ricercatori Georgia Institute of Technology (Georgia Tech) nella sessione Mactans: Injecting Malware into iOS Devices via Malicious Chargers rilasciarono appunto "**Mactans**", una stazione di ricarica malevola in grado di infettare tramite la porta di ricarica USB un iPhone installando un'app malevola mentre il device veniva caricato. L'iPhone eseguiva la versione di iOS 6 e il software malevolo era potenzialmente in grado di annullare qualsiasi misura di sicurezza integrata in iOS e mascherarsi nello stesso modo in cui Apple maschera i processi in background in iOS. In iOS7 Apple implementò la funzionalità di richiedere all'utente il consenso di connettersi per la prima volta ad un host sconosciuto tramite USB.

Nel **2014** i ricercatori Karsten Nohl e Jakob Lell di SRLabs durante la conferenza Blackhat USA 2014 pubblicato le loro ricerche su **BadUSB**, un attacco basato su un difetto intrinseco nell'interfaccia USB che permetterebbe di manomettere il firmware del dispositivo USB. Nella sessione BadUSB - On accessories that turn evil i ricercatori indicavano che uno dei metodi più semplici per propagare malware tramite la vulnerabilità BadUSB è quella di connettere smartphone o tablet ad un computer computer per ricaricare la batteria e mostravano il Proof - of - concept del codice di un firmware malevolo tramite cui infettare Android con BadUSB.

Nel **2016** i ricercatori Aries Security hanno rivisitato l'attacco Juice Jacking alla conferenza DEF CON 24 realizzando una stazione di ricarica in grado di registrare lo schermo degli smartphone che venivano ad essa collegati, i device che al tempo erano vulnerabili a questo tipo di attacco erano gli Android che supportavano i protocolli SlimPort o MHL tramite USB e gli iPhone che utilizzavano un lightning charge cable connector. A riguardo si veda anche Road Warriors: Beware of 'Video Jacking'.

Nel **2018** i ricercatori di Symantec durante l'RSAConference 2018 hanno reso pubbliche nella sessione iOS Trustjacking - New iOS Vulnerability le loro ricerche su un attacco denominato **Trustjackin** basato sul fatto che quando viene approvato l'accesso ad un computer su un device iOS tramite USB a tale livello di accesso sarà applicato anche alle API di iTunes che rendono il dispositivo accessibile tramite Wi-Fi. Questo significa che un attaccante potrebbe accedere ad un device iOS anche dopo che l'utente l'ha scollegato dal computer da una stazione di ricarica malevola o infetta. L'issue era stato comunicato ad Apple a luglio 2017 e in iOS 11 l'approvazione dell'accesso ad un computer da parte di device iOS richiede un passcode. A riguardo di veda iOS Trustjacking - A Dangerous New iOS Vulnerability.

Conclusioni

In base alla storia degli attacchi Juice Jacking e alle vulnerabilità che sono state sfruttate appare evidente che questo tipo di attacco ha un'elevata probabilità di poter essere messo a segno per le seguenti ragioni:

- Le vulnerabilità che di volta in volta sono state sfruttate sono correlate a funzionalità di connessione USB, quindi è logico aspettarsi che possano presentarsi nuove vulnerabilità o che vi siano delle vulnerabilità 0-day.
- La realizzazione di stazioni di ricarica contraffatte per sembrare verosimili è relativamente semplice.
- Anche la compromissione di una stazione di ricarica può non essere difficoltosa se questa è dotata di un computer a cui le porte USB sono connesse, scenario non inusuale perché consente a chi a chi eroga il servizio di avere dati sull'utilizzo e capire come e quanto la stazione è utilizzata. Quindi la compromissione può avvenire infatti tramite la connessione USB sfruttando vulnerabilità non risolte, infatti i sistemi di tali stazioni potrebbero non essere così aggiornati e quindi diventare a seguito di un attacco veicoli di infezione di malware o strumenti di attacco.
- Le stazioni di ricarica normalmente non sono presidiate in modo da poter impedire ad un attaccante di poter studiare il sistema e comprometterlo anche impiegando diverso tempo e svariati tentativi.

Per questo motivo già nel 2012 l'NSA (National Security Agency) aveva rilasciato il documento *Security Configuration Recommendations for Apple iOS 5 Devices* in cui avvertiva i dipendenti del governo di ricaricare i loro dispositivi solo da sistemi di ricarica approvati dall'organizzazione o di utilizzare l'adattatore connesso alla presa elettrica dato in dotazione:

> *"Recharge your device by either connecting to an organization-approved system or by using the AC power adapter you received when you were issued your device."*
> *"Connecting your iOS device to unknown systems exposes the device to unnecessary risks, including the loss of personal or company information. Syncing only with trusted systems also helps maintain the integrity of your iOS device."*
>
> *"Distribute AC power adapters to users when issuing devices and warn users not to connect their devices to unauthorized systems. It may be prudent to distribute additional AC power adapters to remove the temptation to connect the devices to unknown PCs."*
> *"Connecting iOS devices to unauthorized systems, even if only intending to recharge the device, presents a security risk. Providing a power adapter, and easy access to replacements and additional adapters, will help combat temptation to connect to other systems. Users should never be left with connecting to a computer as their only option to recharge their device."*

Per mitigare attacchi di tipo Juice Jacking vale ovviamente prima di tutto la regola di **non connettersi a sistemi non personali per ricaricare i propri device** o di **utilizzare l'adattatore di ricarica connesso ad una presa elettrica**.

In commercio esistono anche soluzioni di protezione di tipo "hardware":

- **Cavi USB di sola ricarica** non abilitati al alo scambio dati in quanto privi dei relativi collegamenti elettrici.
- Dispositivi denominati **Condom USB o SyncStop**, ovvero adattatori USB che se connessi ad un cavo USB impediscono il traffico dati.

Un'ultima considerazione che si può quindi fare è che **se è consigliabile evitare di utilizzare stazioni di ricarica USB allora è anche non consigliabile investire nella realizzazione di ricariche pubbliche**, soprattutto in ottica di realizzare servizi Smart City sicuri. Infatti anche se le stazioni di ricarica sono comode non sono poi così necessarie, dal momento che già da tempo esistono Power Bank che permettono di risolvere senza rischi le emergenze energetiche dei propri device.