Juice Jacking: facciamo il punto sugli attacchi agli smartphone via USB

Author : Salvatore Lombardo

Date : 8 Gennaio 2020

Ognuno di noi può avere l'esigenza di ricaricare il proprio smartphone, in particolar modo quando si è in viaggio o fuori casa. L'attacco informatico denominato **Juice Jacking** consiste nella possibilità, da parte di un attaccante, d'iniettare sul dispositivo un malware o di carpire i dati in esso memorizzati tramite i servizi di ricarica USB pubblici sempre più diffusi in stazioni, aeroporti o hotel.

Questa tipologia di attacco - non molto conosciuta e tanto meno percepita come una potenziale minaccia - è tornata a far notizia nell'ultimo periodo a seguito di un comunicato in merito, rilasciato dal procuratore distrettuale di Los Angeles [1].

Los Angeles County District Attorney's Office

USB Charger Scam

FRAUD ALERT

Travelers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware.

In the USB Charger Scam, often called "juice jacking," criminals load malware onto charging stations or cables they leave plugged in at the stations so they may infect the phones and other electronic devices of unsuspecting users.

The malware may lock the device or export data and passwords directly to the scammer.

To learn about other frauds, visit **http://da.lacounty.gov/community/fraud-alerts**

Helpful Tips

- Use an AC power outlet, not a USB charging station.
- Take AC and car chargers for your devices when traveling.
- Consider buying a portable charger for emergencies.

IF YOU OR SOMEONE YOU KNOW HAS BEEN THE VICTIM OF A SCAM, PLEASE CONTACT YOUR LOCAL LAW ENFORCEMENT AGENCY

Jackie Lacey
Los Angeles County District Attorney

http://da.lacounty.gov

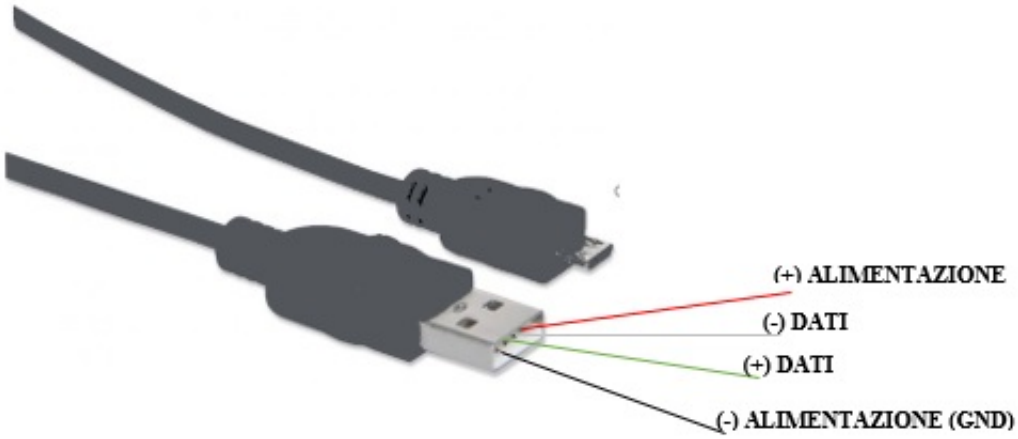
@LADAOffice
#FraudFriday

10/2019, Vol.04, Iss.11

Tuttavia, c’è da precisare che **non siamo di fronte a una novità**. Già in passato in occasione delle conferenze DEF CON 2011 [2] e Black Hat 2013 [3] sono state presentate delle dimostrazioni di fattibilità.

Di cosa si tratta

Una caratteristica accomuna tutti gli smartphone (Android, iPhone): *il cavo utilizzato per ricaricare la batteria del proprio telefonino è lo stesso che si usa per trasferire e sincronizzare i dati*. È proprio questo dualismo (dati/alimentazione) può essere sfruttato come vettore per ottenere l’accesso durante un processo di ricarica. Anche se il juice jacking è una minaccia in gran parte teorica, e le probabilità che le porte di ricarica di una stazione USB possano essere compromesse con relativa facilità sono molto basse, questo non deve assolutamente fare abbassare la guardia ma, piuttosto, ogni volta che colleghiamo il nostro smartphone o tablet con un device sconosciuto dobbiamo essere consapevoli dei potenziali rischi di sicurezza. Ricordiamoci che il connettore USB in dotazione al caricabatterie di ogni cellulare non è un semplice cavo di corrente ma dispone solitamente di 4 *pin,* due usati per la ricarica (1, 4) e due per trasferire solo dati (2,3).



Possibili scenari

Qualora la stazione di ricarica che si sta adoperando sia realmente compromessa, esistono due possibili scenari una volta collegato il nostro dispositivo: un **furto di dati** o **l’iniezione di *malware***. Gli smartphone sono dei veri propri archivi di informazioni sensibili e private e il movente che può spingere un cyber criminale ad attuare uno di questi scenari d’evento è, molto probabilmente, vendere i dati sul darkweb oppure riutilizzarli in successive campagne di *phishing*.

L’attacco può avvenire in modo automatizzato se lo stesso pc del chiosco, adoperato solitamente per l’elaborazione delle statistiche d’uso, è stato violato con il rilascio di applicazioni malevole per la sincronizzazione verso un altro dispositivo mobile. E questa eventualità non è per niente trascurabile se si pensa che i sistemi di queste stazioni potrebbero

non essere aggiornati e a causa di vulnerabilità non risolte rappresentare essi stessi dei potenziali vettori d’infezioni.

Esistono diverse tipologie di malware che i criminali informatici potrebbero installare per questi scopi:

- Il **cryptomine**r allo scopo di sfruttare il processore di un telefono cellulare per generare criptovaluta inficiando le prestazioni delle batterie;
- il **ransomware** allo scopo di prendere in ostaggio i dispositivi crittografandone i file per il riscatto;
- lo **spyware** [4] allo scopo di monitorare a lungo termine ed in background conversazioni, messaggi e quant'altro;
- il **Trojan** allo scopo di ottenere gli accessi per l’installazione di altri malware.

Come difendersi

Il principio alla base del juice jacking è sfruttare disattenzione, fretta, bisogno e scarsa consapevolezza. Va comunque notato che questa tecnica, utilizzata non solo tramite le prese elettriche USB ma anche con la compromissione degli stessi jack usb [5] o delle connessioni HDMI (*mirroring* dello schermo su altro dispositivo [6]), a fronte delle poche segnalazioni registrate, non sembra essere particolarmente diffusa anche se praticamente fattibile. Dal 2011, anno in cui si è parlato per la prima volta di questa minaccia alla sicurezza, fino ad oggi i principali produttori di sistemi operativi per smartphone hanno sanato le principali vulnerabilità, mitigando di fatto il rischio oggettivo. Ciò non toglie, però, che tale rischio possa essere ulteriormente calmierato seguendo delle *best practices*.

Le buone regole andrebbero applicate sempre e con qualsiasi dispositivo. È ormai assodato che ogni nostro spostamento e comportamento possa essere, a vario titolo, monitorato, analizzato e usato in rete; figuriamoci allora cosa possiamo aspettarci a opera di malintenzionati, anche con l’ausilio del juice jacking.

Ecco allora alcuni **consigli utili** da seguire:

- evitare di caricare il telefono usando un sistema di terze parti;
- portare sempre con sé il caricabatterie in dotazione o una *power bank*;
- evitare di collegare a un chiosco USB il proprio smartphone anche se preventivamente bloccato o spento, perché questi tipi di accorgimenti possono funzionare solo per alcuni modelli di telefonini, soprattutto adesso che le batterie sono integrate con il device e non possono essere rimosse, lasciando di fatto il circuito USB sempre alimentato;
- considerare l’utilizzo di soluzioni di protezione hardware aggiuntive:
  - un USB Data Blocker, adattatore USB che inibisce il traffico dati;
  - cavi USB di sola ricarica, privi dei pin per la trasmissione dati.

Note

[1] http://da.lacounty.gov/about/inside-LADA/juice-jacking-criminals-use-public-usb-chargers-steal-data-ff

[2] https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

[3] https://www.youtube.com/watch?v=EWTo8cg0wQM, *Mactans: Injecting Malware into iOS Devices via Malicious Chargers*

[4] https://www.cybersecurity360.it/nuove-minacce/spyware-cosa-sono-come-si-diffondono-e-come-eliminarli/

[5] https://mg.lol/blog/omg-cable/

[6] https://youtu.be/PiZkBH8KjEo, *iPhone Video Jacking*

Sitografia

- https://it.phhsnews.com/what-is-juice-jacking-and-should-i-avoid-public-phone-chargers2568
- https://blog.malwarebytes.com/explained/2019/11/explained-juice-jacking/
- https://www.fondazioneedison.it/blog/juice-jacking-attenti-alle-prese

Articolo a cura di **Salvatore Lombardo**