ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4772 di Lunedì 14 settembre 2020

Mentre tu carichi il telefono, io ti rubo i dati!

Forse non tutti i lettori sono al corrente del fatto che un dispositivo di carica di un telefono cellulare, oppure di un personal computer, può essere utilizzato per sottrarre dati e inserire del malware nel dispositivo collegato. Cos' è il Juice Jacking?

Questa tecnica di attacco, che non è certamente nuova, ma negli ultimi tempi si è propagata in modo esponenziale, viene chiamata dagli anglosassoni con l'espressione "juice jacking".

Per capire come funziona questo attacco, dobbiamo studiare attentamente il funzionamento ed i collegamenti di una presa USB.

In una presa USB sono presenti cinque connettori, ma solamente uno è necessario per ricaricare l'apparato collegato; due altri punti di collegamento vengono utilizzati per il trasferimento dei dati. Grazie a questa architettura, è possibile utilizzare una presa USB sia per caricare un apparecchio, sia per spostare file tra un dispositivo mobile e un computer, quando il dispositivo mobile è collegato ad una presa, disponibile sul computer.

Oggi sono sempre più diffuse le postazioni di ricarica, ad esempio nelle sale di attesa degli aeroporti, e perfino presso frequentati locali pubblici, dove un cliente può collegare temporaneamente il proprio dispositivo mobile per ricaricarlo.

Il problema nasce dal fatto che il cavo di collegamento USB è normalmente attivo su tutti i connettori, e non solo sul polo del correttore, utilizzato per la ricarica.

Chi scrive ha partecipato un paio d'anni fa, a Berlino, allo European data protection days: un conferenziere, al termine dell'intervento, donò a tutti i partecipanti un cavo di collegamento USB, dotato di un interruttore. Azionando l'interruttore, era possibile sezionare tutti i cavi non necessari e attivare solo la funzione di ricarica. Spostando l'interruttore, era possibile invece avviare il dialogo tra l'apparato e l'altra stazione collegata.

Gli attaccanti possono sfruttare questa situazione in vari modi, appresso illustrati.

Ad esempio, è possibile sfruttare il collegamento una stazione di ricarica, nella quale in precedenza è stato caricato un malware, iniettando lo stesso all'interno del dispositivo mobile collegato. Se la stazione di ricarica è sufficientemente evoluta, e per solito l'utente non ha notizie in merito, la stazione di ricarica può essere utilizzata per estrarre una moltitudine di dati presenti sul dispositivo collegato, che successivamente vengono messi a disposizione del malvivente.

Come difendersi

Con un'espressione piuttosto colorita, gli anglosassoni raccomandano di utilizzare un profilattico USB! Si tratta, come accennato in precedenza, di un particolare cavo di collegamento, in cui sono attivi solo i collegamenti necessari per la ricarica, non collegamenti che permettono lo scambio delle informazioni.

Ecco la ragione per la quale si raccomanda di non utilizzare mai dei cavi, già disponibili presso la stazione di ricarica, ma di portare sempre con sé un proprio cavo, con questa caratteristica di sicurezza. Sarà così possibile provvedere alla ricarica, nella certezza che tutti i collegamenti, attraverso i quali dati possono essere scambiati, sono disabilitati.

Un'altra raccomandazione di sicurezza riguarda l'utilizzo, con estrema prudenza, di stazioni di ricarica omaggio, che talvolta vengono offerte durante mostre e fiere. Come accennato in precedenza, si possono usare queste stazioni di ricarica a condizione di usare un cavo di sicurezza.

Ricordo ai lettori che questo tipo di attacco venne pubblicizzato per la prima volta alla famosa conferenza negli Stati Uniti, chiamato DEF CON, nell'agosto 2011. Gli organizzatori della conferenza promossero questo elemento di sicurezza, regalando delle stazioni di ricarica per apparati mobili ai partecipanti alla conferenza. Quando i partecipanti utilizzarono queste stazioni, apparve un messaggio sul loro dispositivo mobile, che li metteva in guardia contro questo possibile tipo di attacco.

A seguito di quella clamorosa iniziativa, i maggiori produttori di sistemi operativi per telefoni mobili hanno inserito un applicativo di sicurezza, che viene attivato ogniqualvolta il telefono viene collegato ad una stazione di ricarica. Sullo schermo appare un messaggio nel quale si chiede all'utente di voler autorizzare o meno non solo l'attività di ricarica, ma che l'attività di trasferimento di dati.

Ciò purtroppo non vale per i personal computer ed ecco la ragione per la quale un poco di prudenza non guasta mai.

Adalberto Biasiotti