# Il malware arriva per posta… in una chiavetta USB!

Mar 27, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

---

***Il bizzarro attacco ha preso di mira una struttura sanitaria negli Stati Uniti. La memoria USB era in realtà un dispositivo in grado di infettare il PC.***

L'uso di memorie USB contenenti malware come vettore d'attacco non è una novità assoluta. In passato la cronaca ha infatti registrato numerosi casi in cui i cyber-criminali hanno adottato questa tecnica, per esempio "seminando" chiavette infette all'interno di parcheggi o ingressi degli edifici.

Il caso riportato da **Trustwave**, però, si distingue nettamente sia per il livello di sofisticazione dell'attacco sotto il profilo tecnico, sia per lo stratagemma adottato per recapitare la chiavetta.

Come si legge nel report pubblicato sul blog ufficiale della società di sicurezza, l'attacco ha preso di mira una struttura sanitaria statunitense e ha utilizzato, come vettore, un pacchetto recapitato negli uffici dell'ospedale.

Il plico, confezionato con un credibilissimo involucro marchiato **Best Buy**, conteneva una lettera in cui si annunciava l'accredito di una gift card del valore di 50 dollari. La chiave USB inclusa nel pacchetto, spiegava la lettera, conteneva l'elenco degli articoli acquistabili con il buono regalo.

La chiavetta, però, non era una semplice memoria USB. Si trattava invece di un dispositivo chiamato **BadUSB Leonardo USB ATMEGA32U4**, in vendita per pochi dollari sul Web.

**Si tratta di un dispositivo del tutto simile a una memoria rimuovibile, che contiene in realtà un microcontroller Arduino programmato per simulare una tastiera USB**.

La chiavetta, in pratica, era programmata per iniettare un comando PowerShell che avvia il download di un payload che viene installato sul computer a cui è collegata la chiavetta.

Per allontanare qualsiasi sospetto, lo script visualizza un messaggio di errore relativo a un presunto malfunzionamento della memoria USB. Insomma: l’obiettivo è quello di far credere alla vittima che la chiavetta sia semplicemente difettosa.

La realtà, però, è molto diversa. IL malware, infatti, agisce dietro le quinte per scaricare il terzo stadio del payload, attraverso una procedura che usa sistemi di crittografia per oscurare le comunicazioni con il server Command and Control.

Una volta operativo, il torjan invia una serie di informazioni al server C&C, tra cui le informazioni sull’utente, il livello di privilegi di cui gode, la versione del sistema operativo e delle eventuali installazioni di **Microsoft Office** e di prodotti **Adobe**. Da questo momento in poi, i pirati informatici hanno assoluta libertà d’azione e possono inviare qualsiasi tipo di comando tramite la backdoor installata.

Per la cronaca, almeno in questo caso, il destinatario del pacchetto si è insospettito di fronte a questo bizzarro stratagemma e non ha collegato la chiave USB al suo computer, avvisando i responsabili cyber security dell’azienda.

Condividi l’articolo

---

Cyber-spionaggio: attacco in grande stile del gruppo cinese APT41

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2020/03/27/il-malware-arriva-per-posta-in-una-chiavetta-usb/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-arriva-per-posta-in-una-chiavetta-usb