Pochi aggiornano e i pirati continuano a sfruttare la falla in Windows

Giu 11, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I cyber-criminali stanno sfruttando attivamente una vulnerabilità che in teoria è stata corretta a fine 2017. Ma i PC a rischio sono ancora tanti.

Difficile capire esattamente che cosa sia andato storto, ma a quanto dicono dalle parti di **Sophos** i pirati informatici stanno sfruttando per i loro attacchi un exploit che, almeno teoricamente, non dovrebbe più rappresentare un problema.

L'attacco, che sfrutta come vettore documenti allegati a messaggi di posta elettronica, fa leva su una vulnerabilità individuata tempo fa (CVE-2017-11882) e corretta con un aggiornamento di Windows nel novembre 2017.

Il bug, che interessa un componente di **Office** chiamato **Equation Editor**, aveva provocato un certo clamore. Il componente in quesitone, infatti, era stato "dimenticato" in tutti gli aggiornamenti precedenti e la versione integrata nel pacchetto software di Microsoft risaliva addirittura al 2000.

Come abbiamo raccontato in questo articolo, i pirati informatici hanno cominciato a sfruttarlo immediatamente dopo la notizia della sua esistenza, ma a quanto pare il suo utilizzo continua anche a più di 18 mesi di distanza.

Secondo i ricercatori Sophos, infatti, la vulnerabilità è la più utilizzata nei kit per la creazione di malware come

NebulaOne.

Non solo: a segnalare una crescita di questi attacchi è la stessa Microsoft, che in un tweet ha messo in guardia gli utenti riguardo la possibilità di ricevere messaggi che contengono documenti di Office modificati per sfruttare la vulnerabilità.

La falla in Equation Editor è particolarmente pericolosa. L’exploit che la sfrutta consente infatti di avviare l’esecuzione di codice sul sistema senza che sia necessaria alcuna interazione da parte dell’utente. **Insomma: basta aprire il documento per ritrovarsi il computer infetto**.

L’elemento curioso riguarda il fatto che molti computer, evidentemente, non abbiano installato correttamente l’aggiornamento che correggeva il bug.

Un problema che alcuni ricercatori hanno già segnalato in passato e che ha una causa molto semplice: sono poche le persone che controllano periodicamente lo stato degli aggiornamenti per verificare che non ne sia stato lasciato indietro qualcuno a causa di errori di varia natura.

Il suggerimento, piuttosto scontato, è quello di verificare che la cronologia degli aggiornamenti sia in ordine e che sia impostata per **scaricare gli aggiornamenti anche per gli altri prodotti Microsoft oltre al semplice sistema operativo**.

Condividi l’articolo

Traffico Internet europeo dirottato verso la Cina per due ore

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/06/11/pochi-aggiornano-e-i-pirati-continuano-a-sfruttare-la-falla-in-windows/