Hacker attacca la botnet Emotet. Payload sostituito con immagini GIF

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

Il vigilante sta facendo letteralmente a pezzi la rete di computer controllati dai pirati informatici sostituendo il malware con immagini animate.

Contrattempo imprevisto per i pirati informatici che gestiscono la temibile botnet **Emotet**. Una delle più pericolose e coriacee botnet in circolazione sta subendo un attacco devastante da parte di un vigilante che sembra intenzionato a metterla K.O.

Tutto è cominciato lo scorso 21 luglio, quando il gruppo **Cryptolaemus** (un team di hacker etici che sta da tempo contrastando la diffusione di Emotet) ha rilevato una curiosa azione di sabotaggio diretta alla botnet.

Emotet, in realtà, era sparita dalla circolazione per quasi cinque mesi ed è tornata a far parlare di sé la scorsa settimana. I cyber criminali che la gestiscono sono ben conosciuti nell'ambiente della cyber security, ma la loro fama non è dovuta a grandi capacità tecniche. Tutt'altro.

La botnet Emotet, piuttosto, è da sempre considerata una sorta di gigante dai piedi d'argilla. I pirati che diffondono il malware, infatti, utilizzano uno schema di diffusione che prevede l'uso di messaggi di posta elettronica che contengono allegati malevoli.

Lo schema d’infezione, però, si appoggia su una rete di siti Web compromessi (su piattaforma **WordPress**) che vengono usati come “contenitori” per il payload che viene scaricato al momento dell’infezione.

È proprio il sistema di controllo di questi siti Internet che rappresenta il punto debole della botnet Emotet. I pirati, infatti, per controllarli utilizzano delle **Web Shell** open source piuttosto elementari. **Di più: secondo gli hacker di Cryptolaemus, usano sempre la stessa password**.

Il misterioso vigilante, a quanto pare, avrebbe scoperto la password e avrebbe cominciato a sabotare sistematicamente tutti i siti che i cyber criminali usano come rete di supporto per distribuire il malware, sostituendo l’eseguibile che contiene il malware con delle innocue GIF animate.

Come riporta ZDNet in un articolo, questa azione avrebbe innescato una sorta di “gara” tra il vigilante (che ora sta usando una GIF di **HackerMan**) e i pirati informatici, che starebbero cercando di ripristinare la loro rete. Nonostante gli sforzi dei criminali, al momento la botnet funzionerebbe a un quarto delle sue abituali capacità.

Nessun indizio, invece, riguardo l’identità del misterioso vigilante. Non è escluso, però, che si tratti di un pirata informatico parte di un gruppo rivale, che abbia come unico obiettivo quello di liberare “fette di mercato” su Internet.

Condividi l’articolo

La botnet Prometei usa ancora EternalBlue… davvero?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/27/hacker-attacca-la-botnet-emotet-payload-sostituito-con-immagini-gif/?utm_source=rss&utm_medium=rss&utm_campaign=hacker-attacca-la-botnet-emotet-payload-sostituito-con-immagini-gif