Smantellata la botnet Emotet

Gen 28, 2021 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

L'operazione congiunta tra Europol e FBI ha messo fuori combattimento centinaia di server usati dai pirati per gestire la rete di computer infetti.

Viene definito come uno dei maggiori successi mai ottenuti dalle forze di polizia nel contrasto al cyber crimine e l'entusiasmo che trasuda dal comunicato stampa pubblicato da **Europol** è più che giustificato: l'abbattimento della botnet **Emotet** rappresenta infatti un colpo storico nella lotta alla pirateria informatica.

L'operazione, che ha visto il coinvolgimento di diverse agenzie tra cui l'**FBI** e la britannica **National Crime Agency**, ha preso di mira centinaia di server che i pirati informatici utilizzavano per controllare a distanza i computer compromessi con il trojan, consentendo alle autorità di prenderne, di fatto, il controllo.

Emotet è una delle botnet più longeve e pericolose in circolazione, la cui diffusione è stata portata avanti sistematicamente attraverso tecniche di attacco che sfruttavano principalmente l'invio di documenti infetti di Word tramite messaggi email.

Il "peso" di Emotet, però, dipende anche dal fatto che i cyber criminali che gestivano le sue operazioni sono stati in grado, nel tempo, di tessere relazioni di affiliazione con altri gruppi di pirati informatici.

Emotet, in pratica, ha rappresentato per anni una sorta di vettore di attacco che consentiva ai cyber criminali di

installare ulteriore malware sui computer compromessi, favorendo così la diffusione di ransomware e trojan bancari come il famigerato **TrickBot**.

Uno schema, quello delle affiliazioni, che assume spesso la forma del "**malware as a service**" e che consente ai pirati informatici di espandere il loro raggio d'azione con estrema facilità.

L'operazione messa a segno si somma ad altre azioni simili portate negli ultimi mesi, tra cui la (parziale) distruzione della già citata botnet TrickBot, di cui abbiamo parlato in questo articolo.

La vicenda, in ogni caso, conferma come le agenzie delegate alla cyber sicurezza stiano adottando sempre più spesso un approccio "proattivo", che mira a disarticolare le organizzazioni criminali piuttosto che giocare la partita "in difesa".

Condividi l'articolo

La vulnerabilità Sudo “Baron Samedit” mette a rischio le distro Linux

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2021/01/28/smantellata-la-botnet-emotet/?utm_source=rss&utm_medium=rss&utm_campaign=smantellata-la-botnet-emotet