La botnet IPStorm ora colpisce anche Linux, Android e Mac

Ott 01, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L'evoluzione del malware prende di mira qualsiasi tipo di dispositivo. Gli esperti di sicurezza: "Non è ancora chiaro quale sia l'obiettivo".

In continua crescita e pronta a diversificare la sua attività: la botnet **IPStorm** in questo momento è in cima ai pensieri degli esperti di sicurezza, che ne stanno monitorando l'evoluzione con una certa preoccupazione.

Come spiegano in un report i ricercatori di **Barracuda**, il malware che diffonde IPStorm (abbreviazione di **InterPlanetary Storm**, ossia "Tempesta InterPlanetaria") si è presentato in una nuova variante che allarga il campo d'azione del gruppo di pirati informatici che lo distribuisce.

Se la prima versione di IPStorm colpiva solo i sistemi **Windows**, la nuova variante prende infatti di mira anche **Linux**, i sistemi **macOS** e **Android**.

L'evoluzione di IPStorm toglie qualsiasi dubbio sulla reale natura del malware. Molti ricercatori, infatti, lo consideravano un'anomalia, sia per le tecniche che usa (lo stesso nome Inter Planetary è derivato da un protocollo peer to peer utilizzato dal malware per comunicare) sia per il linguaggio di programmazione usato per crearlo, quel **Go** che fino a qualche tempo fa era raramente appannaggio di pirati informatici.

Insomma, il dubbio di molti esperti era che IPStorm fosse una sorta di esperimento e che non avese di fronte a sé un gran futuro. Invece, la nuova versione conferma le intenzioni di sfruttare il malware per creare una botnet di tutto rispetto, che sta crescendo inesorabilmente.

Le tecniche di diffusione prevedono l'uso di attacchi a dizionario (una versione "evoluta" del brute forcing – ndr) verso i servizi SSH dei computer Linux e Mac, mentre per Android utilizza tecniche che prendono di mira i dispositivi in cui è attivo il sistema **ADB (Android Debug Bridge)** sfruttato da molti malware per dispositivi mobili.

Se nel maggio 2019 i dispositivi infetti erano poco più di 3.000, a oggi la rete ne conta più di 12.000 ed è probabile che la crescita continui.

Tanto più che l'allargamento ad altri sistemi operativi, e soprattutto al mondo degli smartphone, è un elemento di preoccupazione che lascia pensare a possibili futuri sviluppi.

In tutto ciò, rimane un mistero quale possa essere l'obiettivo

dei pirati informatici che hanno creato IPStorm. Oltre a diffondersi, infatti, il malware non ha per il momento mostrato alcun comportamento riconducibile a uno dei soliti obiettivi (attacchi **DDoS**, diffusione di altri payload) che solitamente caratterizzano le campagne malware.

Probabilmente, spiegano i più pessimisti, è solo quesitone di tempo prima di capire quale sia il reale obiettivo dei suoi autori.

Condividi l’articolo

Hacker specializzati nella truffa BEC hanno già incassato 15 milioni Come ti installo il malware sfruttando una falla del mouse

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/01/la-botnet-ipstorm-ora-colpisce-anche-linux-android-e-mac/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-ipstorm-ora-colpisce-anche-linux-android-e-mac