

Allarme QSnatch: il malware ha colpito più di 60.000 NAS

Lug 28, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La botnet prende di mira i dispositivi QNAP per installare una backdoor che consente ai pirati di accedere a qualsiasi contenuto memorizzato.

L'allarme arriva direttamente dalla statunitense **CISA** (Cybersecurity and Infrastructure Security Agency) e dalla britannica **NCSC** (National Cyber Security Centre). Lo spauracchio del momento è invece **QSnatch**, un malware comparso nell'ormai lontano 2014 e che prende di mira i NAS marchiati **QNAP**.

Secondo gli analisti delle due agenzie, negli ultimi mesi QSnatch avrebbe incrementato la sua attività, raggiungendo una diffusione davvero notevole. Se nell'ottobre del 2019 erano stati individuati 7.000 dispositivi infetti, a metà di giugno sono diventati più di 62.000. I bersagli, rappresentati per lo più da aziende, sono concentrati nell'Europa occidentale e negli Stati Uniti.

Nel rapporto pubblicato su Internet, gli esperti della CISA spiegano quali siano le caratteristiche del malware, che è composto da più moduli. Uno di questi visualizza una versione “alterata” della pagina di login, che consente ai pirati informatici di sottrarre le credenziali di accesso e prendere così il controllo del dispositivo.

QSnatch, però, integra anche altre funzionalità, tra cui una **backdoor SSH** che consente ai pirati informatici di eseguire codice in remoto sul dispositivo. In altre parole: una volta installato il malware, i cyber criminali possono aggiungere qualsiasi funzionalità desiderino.

QSnatch integra in ogni caso una funzione che consente di esfiltrare dati verso il server che lo controlla, trasformando il malware in u perfetto strumento per il furto di informazioni sensibili.

Il report, anche se non contiene alcun riferimento a possibili attribuzioni degli attacchi. Un’anomalia, in tempi in cui qualsiasi attività cyber viene normalmente collegata all’attività di gruppi hacker collegati a governi e servizi segreti stranieri. In questo caso, forse, a fare impressione sono bastati numeri.

Condividi l'articolo

Hacker attacca la botnet Emotet. Payload sostituito con immagini GIF

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/28/allarme-qsnatch-il-malware-ha-colpito-piu-di-60-000-nas/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-qsnatch-il-malware-ha-colpito-piu-di-60-000-nas