La botnet dark_nexus fa strage di dispositivi IoT

Apr 09, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Utilizza un codice copiato da altre botnet, ma i suoi autori hanno introdotto funzionalità e strumenti di attacco innovativi che la rendono più robusta.

La si potrebbe definire "evoluzione della specie". La comparsa della botnet **dark_nexus**, infatti, rappresenta un nuovo sviluppo nel campo dei malware che prendono di mira i dispositivi IoT come **Mirai** e **Qbot**.

Il malware, che secondo i ricercatori di **Bitdefender** è stato sviluppato partendo proprio dal codice del celebre Mirai, è stato ripetutamente aggiornato tra dicembre 2019 e aprile 2020, introducendo una serie di funzionalità che lo rendono più potente e robusta rispetto ai suoi predecessori.

In particolare, si legge nel report, dark_nexus usa due moduli (uno sincrono e uno asincrono) per sfruttare exploit e tecniche di **credential stuffing** che gli consentono di prendere il controllo dei dispositivi attraverso il collegamento **Telnet**.

La botnet utilizza poi un payload estremamente specializzato, che viene scelto sulla base delle caratteristiche del dispositivo compromesso. **I ricercatori hanno individuato ben 12 varianti, ognuna delle quali è programmata per ottimizzare il funzionamento del malware sullo specifico modello di processore installato**.

Gli autori di dark_nexus hanno, come obiettivo, quello di utilizzare le macchine compromesse per portare attacchi DDoS, ma hanno scelto di **adottare un sistema di offuscamento** che altera la trasmissione dei dati in modo che a una prima analisi sembri normale traffico generato da un browser.

Secondo i ricercatori, le dimensioni della botnet sarebbero ancora piuttosto limitate. **Il numero di dispositivi infetti sarebbe infatti di 1.372 bot, principalmente distribuiti tra Brasile, Cina, Sud Corea e Tailandia**.

Le caratteristiche di dark_nexus, così come indica anche la frequenza degli aggiornamenti, sono però tali da far pensare che si tratti di un processo in piena fase di sviluppo.

Il rischio, insomma, è che la botnet raggiunga nel giro di qualche settimana dimensioni decisamente maggiori e possa trasformarsi in un problema pari, per impatto sulla rete globale, a quello che ha rappresentato Mirai per lungo tempo.

Condividi l’articolo

Ancora xHelper: il trojan per Android è immortale

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/09/la-botnet-dark_nexus-fa-strage-di-dispositivi-iot/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-dark_nexus-fa-strage-di-dispositivi-iot