Ecco DDG: la prima botnet peer to peer

Apr 10, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati informatici che la gestiscono hanno sviluppato un sistema di comunicazione tra le macchine infette che la rende estremamente resistente.

Fino a qualche mese fa, la botnet **DDG** veniva considerata dagli esperti come qualcosa di assolutamente "normale". I suoi autori, infatti, la utilizzavano per installare crypto-miner su server vulnerabili e controllavano la sua attività attraverso un classico collegamento a un server Command and Control.

Le cose, però, sono cambiate lo scorso febbraio. I ricercatori di **Netlab 360** si sono infatti accorti che i cyber-criminali hanno introdotto un cambiamento significativo nell'architettura della rete, abilitando un sistema di comunicazione peer to peer tra le macchine infette.

Come spiegano nel loro report (consigliamo di usare un sistema di traduzione verso l'inglese per ottenere un testo abbastanza fedele all'originale) i pirati informatici hanno sviluppato un protocollo proprietario che consente a ogni dispositivo infetto di comunicare con altri 200 bot della rete.

In questo modo, DDG è in grado di sopravvivere anche nel caso in cui il server C&C venisse momentaneamente bloccato e il malware può garantire la sua diffusione e persistenza.

Quello messo in piedi, spiegano i ricercatori, è in realtà un sistema ibrido, in cui le comunicazioni P2P servono come elemento di ridondanza rispetto ai server C&C.

Da un punto di vista tecnico, DDG si diffonde utilizzando un sistema di brute forcing basato su attacchi a dizionario, che fanno leva sull'utilizzo di password "deboli" per l'accesso ai server.

Il database utilizzato dal malware, che viene offuscato attraverso un sistema di crittografia basato su algoritmo AES, comprenderebbe la bellezza di 17.907 password.

Secondo i ricercatori, che sottolineano anche la presenza di

un sistema di proxy utilizzato per offuscare le comunicazioni tra i peer, le caratteristiche di DDG permetterebbero alla botnet di diffondersi in maniera inesorabile, forse lenta, ma inesorabile.

Condividi l’articolo

La botnet dark_nexus fa strage di dispositivi IoT

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/10/ecco-ddg-la-prima-botnet-peer-to-peer/?utm_source=rss&utm_medium=rss&utm_campaign=ecco-ddg-la-prima-botnet-peer-to-peer