Iran: lo strano caso degli attacchi dai proxy per Telegram

Nov 13, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Scenario 0

I server sono proliferati per aggirare i blocchi governativi, ma qualcuno li sta usando per portare attacchi DDoS ai siti Internet.

La potremmo definire una nuova tecnica di **DDoS**, ma ha una particolarità: per le sue caratteristiche interessa soltanto l'**Iran**. Il caso è stato reso pubblico da **Arvan Cloud**, azienda specializzata in servizi cloud e hosting che opera nella repubblica mediorientale.

La società ha infatti denunciato di aver subito un attacco DDoS estremamente particolare, portato da ignoti pirati informatici attraverso una rete di **server MTProxy**. Si tratta di un particolare tipo di proxy dedicati alla gestione del protocollo **MTProto** utilizzato da **Telegram**.

Utilizzati solo nelle nazioni che limitano l'uso del servizio di messaggistica, i proxy di questo tipo permettono agli utenti di Telegram di "offuscare" il traffico e utilizzare la piattaforma aggirando le restrizioni imposte dal governo di **Teheran**.

A quanto pare, però, qualcuno li sta usando anche per un altro obiettivo: portare attacchi DDoS a siti Internet iraniani. Gli esperti di Arvan Cloud sono giunti a questa conclusione dopo aver subito i primi attacchi. Dal momento che erano basati su traffico con caratteristiche anomale, gli analisti

dell’azienda hanno cominciato a indagare e, dopo una serie di simulazioni, sono giunti alla conclusione che l’attacco provenisse proprio dagli MTProxy presenti in Iran.

Lo stratagemma sarebbe semplice: basterebbe sostituire l’indirizzo IP di un server con quello del bersaglio all’interno della rete di proxy. In questo modo la vittima viene bersagliata dal traffico, mentre la rete Telegram, che distribuisce i collegamenti su più server, non subisce alcun rallentamento.

L’attacco non ha effetti devastanti, ma nei 4 giorni di attacchi è stato sufficiente ad “abbattere” un discreto numero di siti Internet gestiti da Arvan Cloud. Nel suo comunicato, la società tecnologica denuncia il fatto che un attacco simile è stato possibile solo a causa del fatto che in Iran esiste un sistema di censura che ha “stimolato” la crescita del circuito degli MTProxy.

Condividi l’articolo

Brutta falla di sicurezza in Magento. È allarme rosso

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/11/13/iran-lo-strano-caso-degli-attacchi-dai-proxy-per-telegram/