Battaglia tra due gruppi hacker: è strage di server sul cloud

Mag 10, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, News, RSS, Scenario 0

Le due gang di cyber-criminali si stanno facendo la guerra prendendo di mira i server vulnerabili per installare i loro crypto-miner ed eliminare quelli dei rivali.

È un copione già visto, ma questa volta la battaglia che si è scatenata tra due gruppi hacker per assicurarsi l'egemonia nel settore del crypto-jacking sta facendo una vera strage di server, mettendo in crisi i servizi cloud e le aziende che li usano.

Protagonisti di questa cyber-guerriglia sono i gruppi **Rocke** e **Pacha**, entrambi specializzati nella compromissione di server con sistemi Linux su cui installano i loro crypto-miner per generare moneta digitale a spese dell'ignara vittima.

Come spiegano in un report i ricercatori di **Intezer**, questa sorta di "disputa territoriale" è iniziata alla fine dell'anno scorso, quando il gruppo Pacha ha fatto la sua comparsa sulle scene, sfidando apertamente i rivali di Rocke, fino a quel momento padroni incontrastati del settore.

Gli attacchi ai sistemi cloud si sono infatti intensificati dopo che i pirati informatici hanno realizzato che mettono a disposizione una maggiore potenza di calcolo rispetto ai normali Web server, che fino a qualche mese fa rappresentavano il normale "terreno di caccia" dei crytpo-jacker.

Entrambi i gruppi utilizzano malware estremamente sofisticati, che al loro interno contengono anche dei moduli pensati per rimuovere eventuali miner di altri pirati informatici che dovessero rilevare sui sistemi compromessi.

Rispetto ai rivali di Rocke, i cyber-criminali legati al gruppo Pacha sembrano però adottare una strategia più aggressiva. Prima di tutto perché il loro malware (**Linux.GreedyAntd**) cerca specificatamente il miner dei rivali con l'obiettivo di eliminarlo.

In secondo luogo perché la loro tecnica di attacco si è evoluta e adesso sfrutta alcuni strumenti che gli consentono di disattivare i software di protezione su cloud (come **Alibaba Server Guard Agent**) esattamente come faceva da tempo il gruppo Rocke.

I nuovi arrivati, inoltre, avrebbero implementato anche un altro strumento utilizzato dai rivali. Si chiama **Libprocesshider** ed è un rootkit open source (il progetto è disponibile su GitHub) che consente di offuscare alcuni processi nell'ambiente cloud per garantire persistenza al malware.

Il risultato è un'escalation in cui, tanto per cambiare, ad avere la peggio sono le aziende che utilizzano i sistemi cloud peresi di mira dai due gruppi di cyber-criminali.

Please follow and like us:

Mega-truffa su Amazon. Sottratti gli incassi di 100 venditori

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/05/10/battaglia-tra-due-gruppi-hacker-e-strage-di-server-sul-cloud/