Kobalos mette nel mirino i supercomputer e i sistemi degli ISP

Feb 03, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware per sistemi Linux è piccolo, versatile e… cattivo. Secondo i ricercatori sarebbe in grado di colpire anche altre piattaforme.

I ricercatori di **ESET**, che lo hanno individuato per primo, lo hanno battezzato con il nome di **Kobalos**, che nella mitologia greca indica una sorta di piccolo fauno.

Le ragioni all'origine della scelta del nome si capiscono leggendo il report pubblicato dagli analisti che hanno "sezionato" il malware: si tratta infatti di un software di piccole dimensioni ma estremamente pestifero, che starebbe procurando non pochi grattacapi nel settore IT.

Il trojan, la cui presenza può essere rilevata scansionando i sistemi sulla porta TCP 55201 per verificare la presenza di servizi **SSH (Secure Shell)**, sarebbe programmato per sottrarre le credenziali dei sistemi che colpisce.

Sul vettore di attacco utilizzato dai pirati per diffonderlo, però, non ci sono al momento indizi rilevanti. In pratica i ricercatori sanno che esiste, ma non hanno la minima idea di come venga distribuito.

Dall'analisi eseguita da ESET, il malware avrebbe colpito numerosi Internet Service Provider in Asia, **reti gestite da diverse università e supercomputer in Europa**, mentre negli USA

i casi individuati riguarderebbero (ancora una volta) società di sicurezza e agenzie governative.

Immagine: ESET

Da un punto di vista tecnico, Kobalos si distingue per una spiccata versatilità, che consente ai pirati di comunicare con la backdoor attraverso diversi canali. **Il malware, inoltre, sembrerebbe essere in grado di adattarsi ad altre piattaforme oltre a Linux, tra cui Solaris e (forse) Windows**.

Una volta installato, il malware è anche in grado di agire come proxy o come server command and control e questo, secondo i ricercatori, garantirebbe alla botnet un livello di resilienza estremamente alto, **In altre parole, anche se i server principali venissero "abbattuti", i cyber criminali potrebbero adattare qualsiasi macchina infetta per sostituirli**.

Immagine: ESET

Nessun indizio, infine, sugli obiettivi degli autori di Kobalos. Il malware potrebbe puntare a rubare informazioni riservate, installare crypto-miner o usare le macchine per qualsiasi altro scopo.

Insomma: poche certezze e tante preoccupazioni per un malware che, a dispetto delle piccole dimensioni del codice che lo compone, sembra avere un livello di complessità (ed efficacia) molto elevato.

Condividi l’articolo

La botnet Matryosh sfrutta i dispositivi Android per portare attacchi DDoS Ti presento Cedar: gli hacker libanesi che hanno violato centinaia di server

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/03/kobalos-mette-nel-mirino-i-supercomputer-e-i-sistemi-degli-isp/?utm_source=rss&utm_medium=rss&utm_campaign=kobalos-mette-nel-mirino-i-supercomputer-e-i-sistemi-degli-isp