Raffica di attacchi ai server con Oracle WebLogic

Mag 07, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

I pirati sfruttano una recente vulnerabilità. La patch è disponibile, ma ci sono ancora migliaia di server vulnerabili che vengono bersagliati dai cyber-criminali.

L'allarme arriva da **Palo Alto Networks**, che sta analizzando la situazione e segnala un'attività anomala da parte di gruppi di pirati informatici che negli ultimi giorni stanno prendendo di mira le installazioni di **Oracle WebLogic** esposte su Internet.

A scatenare la crisi, spiegano i ricercatori in un post sul blog della Unit 42, è stata la pubblicazione di una patch che corregge una vulnerabilità (CVE-2019-2725) in WebLogic.

Secondo gli analisti di Palo Alto Networks, subito dopo la pubblicazione dei dettagli del bug sarebbero comparsi su Internet una serie di **Proof of Concept (PoC)** che consentivano di sfruttare l'exploit legato alla vulnerabilità e i cyber-criminali hanno cominciato a utilizzarli in maniera intensiva.

La cronaca riporta di attacchi che sfruttano la falla di sicurezza (tecnicamente un problema di deserializzazione) per installare sui server miner per generare cripto-valuta, ma anche una campagna che sta sfruttando il bug per compromettere i server e collegarli a una nuova variante della botnet **Muhstik**.

Non mancano poi gli attacchi ransomware, che nello specifico starebbero utilizzando un nuovo malware chiamato **Sodinokibi**.

Insomma: Internet in questo momento sembra un campo di battaglia e la situazione è tutt’altro che rosea. Nonostante la disponibilità della patch, infatti, **dalle analisi dei ricercatori risulta che ci siano almeno 41.000 istanze di WebLogic accessibili da Internet**. Tutte potenziali vittime di un attacco che rischia di creare non pochi problemi agli amministratori di sistema.

Non è la prima volta che WebLogic finisce nell’occhio del ciclone. La popolare piattaforma Oracle per la realizzazione e implementazione di applicazioni Java a livello enterprise, aveva attraversato un vero e proprio calvario già l’anno

scorso in almeno due occasioni.

La prima a gennaio 2018, in seguito a un attacco massiccio che sfruttava una vulnerabilità conosciuta dall'ottobre precedente. La seconda a causa di una patch errata, che aveva esposto nuovamente i server WebLogic ad attacchi.

Please follow and like us:

Antivirus? Firewall? No: Israele usa i missili

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/07/raffica-di-attacchi-ai-server-con-oracle-weblogic/