Lemon Duck adesso prende di mira anche i sistemi Linux

Ago 28, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

La nuova versione del cryptominer utilizza tecniche di brute forcing rivolte a Linux e nuovi exploit per colpire i sistemi Microsoft.

In continua evoluzione: **Lemon Duck**, il malware individuato da **TrapX Security** lo scorso febbraio, si presenta oggi in una nuova variante in cui i suoi autori hanno inserito tecniche di diffusione che ne ampliano il raggio d'azione.

Stando a quanto riportano in un post i ricercatori di **Sophos**, i pirati informatici avrebbero introdotto due nuovi strumenti nel malware. I primo, ancora rivolto ai sistemi Windows, sfrutterebbe l'exploit basato sulla vulnerabilità **SMBGhost**, emersa lo scorso marzo.

Teoricamente, la falla di sicurezza è stata corretta da **Microsoft** con una patch di emergenza. L'esperienza, però, insegna che gli amministratori IT continuano a essere piuttosto "pigri" nell'applicazione degli aggiornamenti e l'uso dell'exploit potrebbe dare ancora dei risultati.

Il modulo che sfrutta SMBGhost, in ogni caso, sembra essere stato inserito nel codice solo in via sperimentale, mantenendo i più classici exploit legati a **EternalBlue** e a un'implementazione di **Mimikatz**. Questi ultimi erano stati eliminati a giugno, ma reintrodotti in agosto.

La vera novità, però, è rappresentata da un sistema di brute forcing che sfrutta il sistema di controllo remoto **SSH** per colpire i sistemi **Linux** e le app su cloud.

Lemon Duck è un malware progettato per installare **XMRig**, un software che sfrutta la potenza di calcolo delle macchine infette allo scopo di generare **Monero**, la cripto-valuta preferita dai pirati informatici.

Il fatto che i suoi autori abbiano allargato gli orizzonti prendendo di mira Linux e applicazioni cloud, di conseguenza, ha una sua logica: i server su cui girano offrono infatti una dotazione hardware decisamente “allettante” per chi punta a monetizzare gli attacchi attraverso il crypto-jacking.

Tra le funzionalità più interessanti individuate dai ricercatori ce n’è una che prevede l’individuazione (e l’eliminazione) di eventuali cryptominer presenti sulla macchina.

Il motivo? Secondo gli esperti di Sophos l’obiettivo dei cyber criminali sarebbe quello di fare piazza pulita della concorrenza e, allo stesso tempo, evitare che risorse preziose per la loro attività di mining clandestina siano dedicate ad altro.

Condividi l’articolo

Raffica di bug per Cisco: “aggiornate subito”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/28/lemon-duck-adesso-prende-di-mira-anche-i-sistemi-linux/?utm_source=rss&utm_medium=rss&utm_campaign=lemon-duck-adesso-prende-di-mira-anche-i-sistemi-linux