Una campagna malware ancora in corso colpisce Linux, soprattutto in Italia

**Check Point Research, la divisione Threat Intelligence di**[**Check Point® Software Technologies Ltd.**](https://www.checkpoint.com/)**(NASDAQ: CHKP), il principale fornitore di soluzioni di cybersecurity a livello globale, ha scoperto una campagna di attacchi informatici in corso che sfrutta le recenti vulnerabilità dei sistemi Linux per creare una botnet infettata da una nuova variante malware chiamata “FreakOut”, in grado di effettuare il port scanning, la raccolta di informazioni, lo sniffing di rete, attacchi DDoS e flood.**

La campagna, tutt’ora in corso, sfrutta le più recenti vulnerabilità Linux per creare botnet infette che possono essere controllate a distanza. La nuova variante malware utilizzata, FreakOut, se sfruttata con successo, può trasformare ogni dispositivo infetto in una piattaforma di attacco per lanciarne di ulteriori attacchi, come ad esempio l'utilizzo di risorse di sistema per il crypto-mining, diffondendosi lateralmente su una rete aziendale o inviando attacchi verso obiettivi esterni spacciandosi per l’azienda appena compromessa.

Gli attacchi sono indirizzati a dispositivi Linux che eseguono una delle seguenti azioni:

* TerraMaster TOS (sistema operativo TerraMaster), noto vendor di dispositivi per data storage
* Zend Framework, popolare raccolta di pacchetti di librerie, utilizzata per costruire applicazioni web
* Liferay Portal, portale aziendale gratuito e open-source, con funzionalità per lo sviluppo di portali e siti web

**Le vittime**

Finora Check Point Research ha rintracciato 185 sistemi infettati dal malware; inoltre, ha evitato oltre 380 tentativi di attacco aggiuntivi, distribuiti secondo la lista di seguito. L’Italia si è classificata al secondo posto (6.61%) e ciò fa capire che il nostro Paese è stato uno dei target principali. In generale, i settori bersagliati da questi attacchi sono stati la finanza e il governo.

**Paese e % di tentativi di attacco**

USA - 27.01%

Italia - 6.61%

Gran Bretagna - 5.46%

Paesi Bassi - 5.17%

Cina - 4.89%

Brasile - 3.74%

Germania- 3.45%

Spagna - 3.45%

Russia - 3.45%

Singapore - 3.16%

**Cosa sappiamo dell’aggressore?**

L’hacker è “volto noto” della criminalità informatica, ben conosciuto, e che utilizza diversi soprannomi, come Fl0urite e Freak. I ricercatori non ne hanno ancora individuato la vera identità.

**Come funziona l’attacco**

1. L'aggressore inizia con l'installazione del malware attraverso lo sfruttamento di tre vulnerabilità: CVE-2020-28188, CVE-2021-3007 e CVE-2020-7961.
2. Successivamente carica ed esegue uno script Python sui dispositivi compromessi.
3. A questo punto, l’aggressore installa XMRig, un noto coinminer
4. Infine, conduce un movimento laterale nella rete attraverso lo sfruttamento delle CVE

Diagram, schematic

Description automatically generated

**Installare la patch, ora!**

I ricercatori invitano gli utenti a patchare i framework vulnerabili di TerraMaster TOS, Zend Framework, Liferay Portal, se utilizzati. Inoltre, raccomandano l'implementazione sia di soluzioni di sicurezza informatica di rete, come IPS, sia di soluzioni per gli endpoint, al fine di prevenire tali attacchi.

**Pierluigi Torriani, Security Engineering Manager di Check Point:**

“Abbiamo identificato una campagna pericolosa e ancora in corso, rivolta a specifici utenti Linux. L'hacker dietro questa campagna è molto esperto in materia di criminalità informatica. Il fatto che alcune delle vulnerabilità sfruttate siano state appena pubblicate, fornisce a tutti noi un buon esempio per evidenziare l'importanza della messa in sicurezza della propria rete, su base continuativa installando le patch più recenti e gli ultimi aggiornamenti. La reattività e l'urgenza sono molto rilevanti quando si tratta di proteggere un’organizzazione. Raccomando vivamente tutti gli utenti interessati a installare le patch su TerraMaster TOS, Zend Framework e Liferay Portal.”