Nuovo malware per Linux installa rootkit e backdoor

Lug 25, 2022 Redazione news Malware, News, RSS 0

Lightning Framework è stato definito dai suoi scopritori come un "coltellino svizzero" del malware e ha plugin modulari e la capacità di installare rootkit

Intezer ha identificato una **minaccia per Linux precedentemente non documentata né rilevata, chiamata Lightning Framework**, traducibile in italiano come Framework Fulmine. Come sottolinea il report, è raro vedere un framework così complesso sviluppato per colpire i sistemi Linux.

Lightning è infatti un **framework modulare dotato di una vasta gamma di funzioni e della capacità di installare diversi tipi di rootkit, nonché di eseguire plugin**. Dispone di funzionalità passive e attive per la comunicazione con l'attore della minaccia, tra cui l'**apertura di collegamenti SSH su una macchina infetta e la creazione di backdoor.**

Fa un uso massiccio del typosquatting, ossia il mascherare un elemento malevolo con il nome di un programma legittimo scritto con un piccolo errore di battitura, per rimanere inosservato. **Si fa passare per il gestore di password e chiavi di crittografia Seahorse per GNOME per eludere il rilevamento sui sistemi infetti**.

Il malware è composto da un downloader e da un modulo centrale, con una serie di plugin che includono strumenti open source. Il modulo centrale è quello principale ed è in grado di ricevere comandi dal server di comando e controllo (C2) e di eseguire i moduli plugin. Ha molte funzionalità e **utilizza una serie di tecniche per nascondere gli artefatti e rimanere inosservato**.

Stabilisce anche la persistenza creando uno script che viene eseguito all'avvio del sistema. Per farlo crea un file in /etc/rc.d/init.d/elastisearch. Il nome sembra essere un typosquat del server di ricerca legittimo Elasticsearch. **Non sono ancora stati individuati attacchi basati su Lightning**

Framework.

Come sottolinea Intezer, anno dopo anno **gli ambienti Linux sono sempre più oggetto di attacchi** a causa del crescente interesse dei pirati per questo sistema operativo, molto utilizzato sul cloud.

Il malware che prende di mira gli ambienti Linux ha registrato un'impennata nel 2021, con molta innovazione che ha portato alla creazione di nuovo codice malevolo, soprattutto per quanto riguarda ransomware, trojan e botnet.

Windows 11 alza le difese contro gli attacchi brute-force
Diminuiscono gli attacchi ransomware

Articoli correlati

Altro in questa categoria
