Da Windows a Linux: TrickBot si evolve

Ago 03, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

La nuova versione del trojan è stata battezzata con il nome di Anchor_Linux e consente di prendere il totale controllo delle macchine infette.

È uno dei "pesi massimi" tra i malware e sembra non avere nessuna intenzione di cedere il suo trono. Anzi: a quanto pare gli autori di **TrickBot** hanno deciso di espandere il campo d'azione del loro trojan per colpire anche le macchine con sistemi **Linux**.

A segnalare questa "invasione di campo" sono i ricercatori di **Intezer**, che hanno individuato un esemplare di malware collegato a TrickBot e in grado di colpire i computer Linux.

Come spiegano tutti i ricercatori che lo hanno analizzato, Anchor_Linux non è una versione derivata dal trojan vero e proprio. Il legame, infatti, è più complesso.

Gli autori di TrickBot, per diffondere e controllare il loro malware, utilizzano infatti una piattaforma chiamata **Anchor**, che sfrutta DNS per inviare comandi alle macchine infette.

Anchor_Linux sarebbe quindi una versione per Linux di Anchor, che al suo interno contiene anche una copia di TrickBot per Windows.

Il malware agisce come una classica backdoor e sfrutta i collegamenti sulla LAN per infettare ulteriori macchine (sia Linux che Windows) utilizzando principalmente alcuni exploit

basati su **Server Message Block**.

Insomma: siamo di fronte a un vero e proprio ecosistema che consente ai pirati informatici di diffondere i loro trojan sui due sistemi, aprendo la strada a qualsiasi genere di attività.

La versatilità di TrickBot e di Anchor_Linux consente infatti ai cyber criminali di rubare credenziali di accesso, documenti e installare qualsiasi tipo di ulteriore malware.

Tra questi, per esempio, i ricercatori evidenziano due ransomware (**Ryuk** e **Conti**) che vengono utilizzati come "payload finale" negli attacchi portati attraverso la piattaforma Anchor e anche strumenti pensati per compromettere i sistemi di pagamento POS attraverso campagne di lungo periodo.

Proprio la presenza di un installer del trojan per Windows, secondo gli esperti, indicherebbe che questa evoluzione di TrickBot non punterebbe tanto ad ampliare il campo di azione del malware per compromettere le macchine Linux, quanto per creare una "testa di ponte" che consenta di attaccare i sistemi Microsoft, che rimangono il principale obiettivo dei

pirati.

Condividi l’articolo

Attacco hacker a Twitter: individuati i responsabili Ti presento Doki: la backdoor per sistemi virtuali su Linux

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/03/da-windows-a-linux-trickbot-si-evolve/?utm_source=rss&utm_medium=rss&utm_campaign=da-windows-a-linux-trickbot-si-evolve