Hacking dei router con controllo remoto

Nel vasto e ombroso mondo del cybercrimine, gli attori delle minacce avanzate persistenti (APT) e i cybercriminali si muovono con destrezza, avvalendosi di sofisticati strati di anonimato forniti da proxy e VPN. Come spie in un romanzo di spionaggio, questi malintenzionati si celano dietro un velo di segretezza, rendendo arduo il compito di chi cerca di svelare le loro trame nefaste. Il loro obiettivo è chiaro: operare indisturbati, mescolando traffico internet dannoso con intenti di lucro e spionaggio.

Immaginate un botnet, una rete di dispositivi infettati, che dal 2016 ha tessuto la sua tela nell'ombra, utilizzando dispositivi Ubiquiti EdgeRouter compromessi. Questa rete è stata un campo di battaglia per l'FBI e alleati internazionali, che il 26 gennaio 2024 hanno messo fine a questa minaccia. Ma prima di questo epilogo, nel aprile 2022, il gruppo APT noto come Pawn Storm (alias APT28 o Forest Blizzard), ha messo le mani su questa rete, trasformandola in uno strumento per le sue oscure campagne di spionaggio.

Attraverso l'analisi dei dati telemetrici forniti da Trend Micro e altre fonti, è emerso un quadro inquietante: centinaia di router Ubiquiti EdgeRouter sono stati deviati dai loro scopi originari. Sono diventati strumenti per attacchi di forzatura SSH, fattorie di spam farmaceutico, riflettori SMB in attacchi di relay hash NTLMv2, proxy per credenziali rubate in siti di phishing, proxy multipurpose, macchine per il mining di criptovalute e lanciatori di e-mail di spear phishing. Un arsenale di strumenti malevoli, nascosto alla vista ma devastante nelle sue capacità di infiltrazione e distruzione.

Secondo quanto riportato dai ricercatori della società di sicurezza Trend Micro, la situazione è talvolta pacifica: gli hacker che mirano al profitto concedono alle spie accesso ai router già compromessi, in cambio di una certa somma. In altre situazioni, invece, gli hacker al servizio di gruppi di minacce avanzate, supportati dagli stati nazionali, prendono il controllo dei dispositivi precedentemente infettati da cybercriminali comuni. Ci sono persino casi in cui un dispositivo viene violato più volte da diversi gruppi di hacker. Il risultato è una sorta di mercato nero all'interno dei router e, in misura minore, dei dispositivi VPN e dei server virtuali privati forniti da società di hosting.

I ricercatori hanno recentemente rivelato che criminali informatici e spie di stato si stanno muovendo dietro le quinte, nascosti all'interno dei router di marche note. Utilizzando questi dispositivi come copertura, orchestrano una varietà di attacchi, sia per scopi finanziari che per operazioni di spionaggio strategico.

Secondo quanto riportato dai ricercatori della società di sicurezza Trend Micro, la situazione è talvolta pacifica: gli hacker che mirano al profitto concedono alle spie accesso ai router già compromessi, in cambio di una certa somma. In altre situazioni, invece, gli hacker al servizio di gruppi di minacce avanzate, supportati dagli stati nazionali, prendono il controllo dei dispositivi precedentemente infettati da cybercriminali comuni. Ci sono persino casi in cui un dispositivo viene violato più volte da diversi gruppi di hacker. Il risultato è una sorta di mercato nero all'interno dei router e, in misura minore, dei dispositivi VPN e dei server virtuali privati forniti da società di hosting.

I ricercatori di Trend Micro, Feike Hacquebord e Fernando Merces, hanno recentemente evidenziato un fenomeno inquietante nel mondo della cybersecurity. Criminali informatici e attori delle minacce persistenti avanzate (APT) stanno condividendo un interesse comune negli strati di anonimizzazione proxy e

nei nodi della rete privata virtuale (VPN), al fine di mascherare le proprie attività malevole e rendere più difficile il loro rilevamento.

Un esempio concreto di questa tendenza è emerso nel caso di una rete composta principalmente da dispositivi EdgeRouter del produttore Ubiquiti. L'FBI ha scoperto che questa rete era stata infettata da un gruppo sostenuto dal Cremlino, utilizzando i dispositivi come botnet per mascherare attacchi mirati a governi, militari e altre organizzazioni in tutto il mondo. In un curioso sviluppo, gli hacker russi hanno preso il controllo dei dispositivi già infettati da un malware noto come Moobot, originariamente installato da gruppi di minacce finanziariamente motivati non affiliati al governo russo. Questa situazione ha messo in luce la complessità delle interazioni tra diversi attori delle minacce nel panorama della sicurezza informatica.

Trend Micro ha osservato che **Pawn Storm**, uno dei nomi noti associati a questa rete di criminalità informatica, stava utilizzando la botnet dirottata per svolgere un duplice ruolo: da un lato, fungeva da proxy per gli accessi utilizzando credenziali di account rubate; dall'altro, supportava gli attacchi sfruttando una vulnerabilità zero-day critica in Microsoft Exchange, che non è stata risolta fino a marzo 2023. Questi attacchi miravano a ottenere l'hash crittografico delle password di Outlook degli utenti, consentendo agli hacker di eseguire un attacco di relay hash NTLMv2 e instradare gli accessi agli account utente attraverso la botnet.

Ma la storia non finisce qui. Trend Micro ha rivelato che la stessa botnet veniva utilizzata anche per inviare spam con temi farmaceutici, oltre che per installare il malware noto come Ngioweb su altri dispositivi compromessi. Questo malware, scoperto per la prima volta nel 2019, mirava a fornire proxy per instradare le attività online attraverso una serie di indirizzi IP in continuo cambiamento, principalmente situati negli Stati Uniti. Ciò dimostra la complessità delle

operazioni condotte da gruppi come **Pawn Storm**, che sfruttano una varietà di risorse per i propri scopi criminali.

Il team di Trend Micro scrive questo:

> *In the specific case of the compromised Ubiquiti EdgeRouters, we observed that a botnet operator has been installing backdoored SSH servers and a suite of scripts on the compromised devices for years without much attention from the security industry, allowing persistent access. Another threat actor installed the Ngioweb malware that runs only in memory to add the bots to a commercially available residential proxy botnet.* ***Pawn Storm*** *most likely easily brute forced the credentials of the backdoored SSH servers and thus gained access to a pool of EdgeRouter devices they could abuse for various purposes.*
>
> *https://www.trendmicro.com/fr_fr/research/24/e/router-roulette.html*

> *Nel caso specifico dei router Ubiquiti EdgeRouter compromessi, abbiamo osservato che un operatore di botnet ha installato server SSH con backdoor e una suite di script sui dispositivi compromessi per anni senza molta attenzione da parte dell'industria della sicurezza, consentendo un accesso persistente. Un altro attore minaccia ha installato il malware Ngioweb, che funziona solo in memoria, per aggiungere i bot a una botnet proxy residenziale disponibile in commercio.* ***Pawn Storm*** *molto probabilmente ha facilmente forzato le credenziali dei server SSH con backdoor e ha quindi ottenuto accesso a un pool di dispositivi EdgeRouter che poteva abusare per vari scopi.*

La situazione è resa ancora più intricata dalla scoperta che i dispositivi EdgeRouter compromessi erano stati infettati da diversi gruppi di minacce, compresi quelli finanziariamente motivati e quelli supportati da stati nazionali, oltre a **Pawn Storm**. Questo evidenzia la corsa in corso tra più gruppi di minacce per stabilire posti di ascolto segreti all'interno dei router, creando una situazione di estrema complessità per gli esperti di sicurezza informatica.

Sebbene l'operazione dell'FBI abbia rappresentato un importante colpo per l'infrastruttura su cui si basava **Pawn Storm**, i limiti legali hanno impedito di prevenire completamente la reinfezione. Inoltre, la botnet comprendeva anche server pubblici virtuali e dispositivi Raspberry Pi, che sono rimasti intatti dall'azione dell'FBI, garantendo a Pawn Storm un accesso persistente a numerosi altri asset compromessi.

In definitiva, il caso dei router Ubiquiti EdgeRouter compromessi illustra la complessità e l'interconnessione delle minacce informatiche moderne, che coinvolgono attori di varia natura e motivazioni. La situazione richiede una risposta integrata e coordinata da parte della comunità della sicurezza informatica, al fine di contrastare efficacemente questa crescente minaccia alla sicurezza digitale.