



Salt Typhoon e la riconfigurazione della strategia cibernetica USA

Pubblicato il 23/10/2025

Nel 2023 un gruppo di hacker legato alla **Repubblica Popolare Cinese** ha avviato una vasta campagna di cyber-spionaggio denominata **Salt Typhoon**. Si tratta di un'operazione di lunga durata volta a infiltrare le **reti di telecomunicazioni e infrastrutture critiche statunitensi**, tra cui **Verizon, AT&T e T-Mobile**, con l'obiettivo di ottenere accesso permanente a sistemi governativi e privati.

Secondo il **Senatore Mark Warner**, vicepresidente della Commissione Intelligence del Senato, Salt Typhoon rappresenta "il peggior attacco alle telecomunicazioni nella storia degli Stati Uniti". Gli aggressori hanno sfruttato vulnerabilità note in router e server per penetrare reti interne, monitorare comunicazioni e raccogliere dati sensibili.



Salt Typhoon e la riconfigurazione della strategia cibernetica USA

Un attacco sistemico

Tra marzo e dicembre 2024, gli hacker hanno violato la rete di una **unità della Guardia Nazionale dell'Esercito USA**, esfiltrando credenziali, mappe dei sistemi, dati del personale e schemi di comunicazione. L'**FBI** stima che siano stati sottratti **oltre un milione di registrazioni di chiamate** e dati di **geolocalizzazione di milioni di utenti**.

Le informazioni raccolte possono essere usate per **spionaggio politico, militare o industriale**, e persino per seguire in tempo reale i movimenti dei militari nelle basi.

Nonostante gli annunci di “contenimento” da parte delle compagnie colpite, un rapporto congiunto delle agenzie di sicurezza ha rivelato che **Salt Typhoon continua a mantenere un accesso persistente alle reti statunitensi**, confermando che le difese finora adottate non sono bastate.

Difesa e deterrenza

L'amministrazione statunitense sta orientando la propria risposta su due assi principali: **rafforzare le difese e rendere più chiara la postura offensiva**.

- **Sanzioni mirate:** il Dipartimento del Tesoro, tramite l'**Office of Foreign Assets Control (OFAC)**, ha già colpito società cinesi coinvolte, come **Sichuan Juxinhe Network Technology Co.**, ma è necessario estendere le misure a tutto l'ecosistema che supporta l'esfiltrazione dei dati.

- **Disruption tecnica:** l'**FBI** e la **CISA** stanno ampliando le operazioni per individuare dispositivi compromessi e bloccare i canali di comando e controllo usati dai gruppi di hacker.
- **Prevenzione:** la **Federal Communications Commission (FCC)** ha avviato una revisione dei dispositivi di rete ad alto rischio e proposto un obbligo di segnalazione degli incidenti di sicurezza alle autorità federali.

REWARD UP TO \$10 MILLION FOR INFORMATION ON CHINESE HACKING GROUP

Guan Tianfeng and other employees of People's Republic of China-based Sichuan Silence Information Technology Co. Ltd. developed and deployed malware that allowed them to access some 81,000 firewall devices without authorization. The malware damaged some of the devices and allowed the hackers to retrieve and exfiltrate data from the firewalls and the computers behind these firewalls.

If you have information on Guan Tianfeng, Sichuan Silence, associated individuals or entities, or their malicious cyber activity, contact Rewards for Justice via the Tor-based tips-reporting channel below. You could be eligible for a reward and relocation.

GUAN TIANFENG

U.S. Department of State
Diplomatic Security Service
Rewards for Justice

Tor Link: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

Salt Typhoon e la riconfigurazione della strategia cibernetica USA

Una deterrenza efficace dipende da **reti resilienti e risposte coerenti**. Senza una base difensiva solida, eventuali azioni di ritorsione contro la Cina rischierebbero di essere inefficaci o controproducenti.

Per questo, analisti e legislatori chiedono di fissare **soglie di escalation chiare** e procedure di risposta automatica a violazioni gravi, rendendo la postura statunitense più prevedibile e quindi più credibile agli occhi degli avversari.

Conclusione

Salt Typhoon non è solo un episodio di cyber-spionaggio: è la dimostrazione di come la **guerra digitale sia ormai un elemento strutturale della competizione geopolitica**.

Riconfigurare la strategia cibernetica americana significa passare da una difesa frammentata a una **dottrina integrata di resilienza, sanzione e deterrenza**, capace di proteggere infrastrutture, istituzioni e cittadini da minacce persistenti e sempre più sofisticate.