Salt Typhoon: violazione della National Guard USA



Negli ultimi anni gli Stati Uniti hanno identificato una crescente attività di cyber-spionaggio cinese nota come la campagna *“Typhoon”*, in cui il gruppo *Salt Typhoon* – collegato al Ministero della Sicurezza di Stato cinese (MSS) – ha preso di mira infrastrutture critiche statunitensi. Nel 2024 il gruppo ha compromesso a lungo le reti informatiche di importanti operatori di telecomunicazioni (Verizon, AT&T, Lumen, ecc.), sottraendo metadati di milioni di comunicazioni, inclusi quelli di politici di rilievo.

Successivamente è emersa la notizia che Salt Typhoon aveva infatti penetrato anche la rete informatica di una Guardia Nazionale statale statunitense. La violazione è durata nove mesi (marzo–dicembre 2024) ed è stata svelata da un memo interno del DHS ottenuto via Freedom of Information e riportato da NBC News. Secondo tale rapporto, i cybercriminali cinesi hanno esfiltrato credenziali amministrative, diagrammi di rete, file di configurazione e dati personali di soldati della Guardia Nazionale, potenzialmente utilizzabili per colpire altre unità statali e le loro controparti di sicurezza informatica.

Cronologia dell’incidente

- **Marzo 2024 – Dicembre 2024:** Salt Typhoon si insedia silenziosamente nella rete della Guardia Nazionale di uno Stato federale USA, sfruttando vulnerabilità note o credenziali rubate per ottenere accesso iniziale. Durante l’intrusione il gruppo esfiltra file di configurazione di rete, diagrammi e credenziali di amministratore. Contemporaneamente (gennaio–marzo 2024)

utilizza tali informazioni per attaccare almeno altre due agenzie statali, sfruttando dispositivi con vulnerabilità note.

- **Dicembre 2024:** Si ritiene che l'intrusione si concluda o venga scoperta. Non sono note pubblicazioni immediate, ma i militari statali iniziano indagini interne.
- **11 giugno 2025:** Il Dipartimento della Sicurezza Interna (DHS) redige una nota riservata (intelligence memo) che riassume l'incidente. Il documento, acquisito tramite FOIA dal gruppo *Property of the People*, viene reso pubblico a metà luglio 2025.
- **15–17 luglio 2025:** Media statunitensi (Reuters, NBC News, Federal News Network, BleepingComputer, Wired, ecc.) riportano l'accaduto. Reuters sottolinea che il DHS e il Dipartimento della Difesa hanno confermato la compromissione prolungata (marzo–dicembre 2024) di una rete della Guardia Nazionale, con furto di dati critici. La National Guard Bureau ammette l'attacco (pur senza rivelare dettagli precisi), dichiarando che non ha impedito le operazioni e che l'indagine prosegue.

Tecniche e vettori di attacco utilizzati

L'analisi di intelligence indica che Salt Typhoon ha sfruttato principalmente vulnerabilità note e credenziali legittime per infiltrarsi nella rete della Guardia Nazionale. Sebbene il memo DHS non precisi l'esatto vettore iniziale, si ritiene plausibile l'uso di exploit pubblici su dispositivi di rete (router Cisco, firewall, VPN) o di credenziali rubate. Ad esempio, in passato il gruppo ha abusato di una falla critica del servizio Cisco Smart Install (CVE-2018-0171) e di altre vulnerabilità Cisco IOS/XE. In un noto caso, Salt Typhoon ha ottenuto inizialmente l'accesso a un dispositivo Cisco sfruttando CVE-2018-0171; in altre situazioni ha semplicemente utilizzato credenziali valide ottenute altrove.

Una volta dentro il perimetro, gli aggressori hanno usato tecniche living-off-the-land e movimenti laterali per espandere il controllo. In particolare, hanno stabilito connessioni SSH tra dispositivi di rete compromessi usando account creati modificando i file di sistema (/etc/shadow, /etc/passwd). Sono state aggiunte chiavi SSH autorizzate e creati account di servizio sui dispositivi Linux (MITRE ATT&CK T1098, T1136). Per eludere le difese, il gruppo ha ripetutamente modificato l'indirizzo dell'interfaccia loopback su switch Cisco compromessi, usando quel loopback come sorgente per SSH verso altri dispositivi e aggirando così le ACL impostate. Ha inoltre ripulito i log (.bash_history, auth.log, wtmp, btmp) per cancellare tracce delle sue attività (Indicator Removal, T1070).

Dal punto di vista MITRE ATT&CK, le tecniche osservate includono l'uso di credenziali rubate (T1078 – Valid Accounts), la raccolta di file di configurazione di rete (T1602 – Data from Configuration Repository) e la ricognizione di topologie di rete (T1590.004). Per l'esfiltrazione i criminali hanno trasferito i dati tramite protocolli non cifrati come FTP o TFTP (Exfiltration over Alternative Protocols T1048.003).

In alcuni casi è stato usato il tool custom *JumbledPath*, che esegue catture di pacchetti su dispositivi remoti e ne invia in forma compressa e crittografata i risultati via catena di salto. In sostanza il gruppo ha sfruttato credenziali legittime e configurazioni esposte per avvicinarsi alle risorse sensibili, senza introdurre malware complessi sugli end-point: ad esempio, ha utilizzato strumenti di sistema come **tcpdump**, Cisco Embedded Packet Capture (EPC) e **Tpacap** per intercettare il traffico di rete, e ha spostato il traffico catturato via FTP/TFTP all'esterno dell'ambiente target.

Strumenti e infrastrutture impiegati

Salt Typhoon ha fatto ampio uso di infrastrutture di rete compromesse come **ponti** fra diverse reti. I dispositivi crittografici utilizzati nel settore (router, switch, modem di segmenti sensibili) sono stati trasformati in *jump host* internetworking. Ad esempio, Cisco Nexus con funzionalità *guestshell* Linux sono stati riconfigurati come punti di salto in catena (vedi immagine sottostante). Nell'immagine il tool custom **JumbledPath**, compilato come binario ELF x86-64, cattura pacchetti su un dispositivo di rete remoto attraverso un altro dispositivo "di salto" dell'attore, comprimendo e cifrando i dati esfiltrati: questo permette di occultare la fonte e di attraversare segmenti non altrimenti routabili.

Oltre a JumbledPath, Salt Typhoon ha impiegato tool sia custom sia di amministrazione standard: in campagne precedenti il gruppo ha usato tecnologie Windows native (PowerShell, WMI, PsExec) e utility per la gestione remota, ma qui l'enfasi è rimasta sulle componenti *network*. I dispositivi di rete compromessi eseguivano script SSH e comandi come **snmpwalk** e **tftp** per raccogliere configurazioni e credenziali. Gli indicatori di compromissione pubblicati includono anche indirizzi IP collegati agli exploit delle vulnerabilità citate.

L'infrastruttura di comando e controllo (C2) e di raccolta dati include server FTP/TFTP esterni controllati dagli aggressori, dove venivano caricati i file estratti. Benché non siano stati resi noti domini specifici, il memo DHS elenca alcuni indirizzi IP usati dal gruppo. In sintesi, Salt Typhoon ha trasformato le reti legacy della Guardia Nazionale (spesso basate su hardware Cisco con vecchi sistemi operativi di rete) in una struttura di puntellamento laterale, utilizzando account amministrativi creati ad hoc e meccanismi di logging interno ai dispositivi (EPC, loopback) per spostarsi e

mantenere la persistenza.

Obiettivi e impatti dell’attacco

L’obiettivo primario di Salt Typhoon sembra essere stato il **cyber-spionaggio strategico**. Rubando configurazioni di rete, credenziali e diagrammi di rete, gli hacker hanno acquisito una mappa dettagliata dell’architettura di difesa cibernetica statale e collegata alla National Guard. Secondo gli analisti, questi dati possono “agevolare successivi attacchi Salt Typhoon” anche verso altre unità della Guardia Nazionale in altri Stati.

In particolare, la compromissione poteva dare a Pechino informazioni sui legami tra le reti statali e la Guardia Nazionale, inclusi i sistemi di intelligence sulle minacce condivise (fusion centers statali). L’analisi del memo evidenzia il furto di PII di militari (nominativi, mappe di posizionamento geografico di asset militari, credenziali interne), elementi che potenzialmente possono essere usati per targeting mirati in scenari futuri.

L’impatto potenziale è grave anche dal punto di vista della sicurezza nazionale collettiva: Salt Typhoon avrebbe potuto “minare gli sforzi della Guardia Nazionale per proteggere l’infrastruttura critica americana”.

L’esposizione di topologie di rete e accessi amministrativi rende più facile per gli attaccanti cinesi colpire backdoor in ulteriori reti governative o civili, superando i confini statali. Inoltre, come ha osservato la stampa specializzata, il fatto che Salt Typhoon abbia violato sistemi telecom per intercettare dati di comunicazione (inclusi conversazioni di politici come Trump e Vance) lascia intendere un’agenda di intelligence estesa anche al settore della difesa militare.

In pratica, gli Stati Uniti hanno valutato l’intrusione come un’espansione delle campagne di spionaggio cinesi:

un’occasione in cui i dati ottenuti possono “facilitare l’hacking di altre unità della National Guard” e “dei loro partner di cybersecurity statali”, configurando così un significativo rischio strategico.

Risposta delle autorità statunitensi

Dopo la diffusione del memo DHS, le agenzie governative hanno riconosciuto la gravità del fenomeno, pur rimanendo vaghe nei dettagli pubblici. La **Guardia Nazionale** (National Guard Bureau) ha confermato l’attacco a NBC News, assicurando che «l’attacco non ha impedito alla Guardia di portare a termine le proprie missioni» e che l’indagine è in corso. A livello federale, non è stato emesso alcun bollettino pubblico specifico sulla violazione della Guardia Nazionale, ma il caso si colloca nel più ampio contesto delle contromisure anti-cinesi.

La **CISA** (agenzia governativa per la sicurezza cibernetica) e l’**FBI** avevano già da tempo iniziato a contrastare Salt Typhoon. Nel dicembre 2024 CISA, NSA e FBI hanno pubblicato linee guida rivolte al settore delle telecomunicazioni per individuare e mitigare la minaccia Salt Typhoon. Nel frattempo, l’FBI ha chiesto pubblicamente collaborazione per raccogliere informazioni sul gruppo: nell’aprile 2025 ha diffuso un avviso (IC3 Alert) con una taglia di 10 milioni di dollari per chi segnali i membri del Salt Typhoon, evidenziando come la campagna di Salt Typhoon sia «probabilmente più ampia» di quanto inizialmente noto.

Sul fronte legislativo, alcuni senatori hanno esercitato pressione perché la CISA migliori la resilienza del settore delle telecomunicazioni. Per quanto riguarda l’escalation militare, i vertici della sicurezza informatica del Pentagono raccomandano a tutte le forze armate di operare «assumendo i propri network già compromessi» e di coordinare la difesa

informatica degli Stati federali, dato il ruolo ibrido della Guardia Nazionale come collegamento tra agenzie federali e autorità statali. In sintesi, la risposta US è stata: indagine continuata congiunta (DHS, DOD, FBI, NSA), emissione di linee guida di settore (CISA/NSA/FBI) e richiesta di informazioni al pubblico (FBI), ponendo l'accento sulla cooperazione pubblico-privato per «alzare il costo per l'attaccante».

Collegamenti con campagne di spionaggio precedenti

L'intrusione della Guardia Nazionale si inquadra nella più ampia serie di operazioni *"Typhoon"* condotte da attori cinesi. Salt Typhoon è lo stesso gruppo (anche detto Earth Estries, FamousSparrow, UNC2286) responsabile dell'attacco dimostrato nel 2024 contro nove grandi operatori telecom americani. In quella campagna, il gruppo ha sottratto enormi quantità di metadati delle comunicazioni telefoniche di oltre un milione di utenti, compresi funzionari di alto profilo, e ha compromesso i sistemi impiegati nelle intercettazioni legali (CALEA) delle agenzie USA.

Salt Typhoon opera in tandem con altri gruppi Chinese APT, come Volt Typhoon (che cercava posizionamenti su infrastrutture critiche per un ipotetico conflitto) e Flax Typhoon (coinvolto in botnet e contrattacchi FBI). Il fatto che il gruppo sia focalizzato su infrastrutture di comunicazione – siano esse reti civili o militari – sottolinea un obiettivo strategico di raccolta di intelligence.

In particolare, la vicenda recente conferma il timore che i compromessi delle reti 5G e delle telecom possano connettersi alla minaccia verso sistemi di difesa militare: secondo The Record, gli sforzi americani nel 2025 hanno costretto i gruppi Typhoon a rivedere le loro tattiche di persistenza, ma non hanno distrutto completamente le loro capacità offensive. In conclusione, l'attacco alla National Guard rappresenta

un’estensione naturale delle precedenti campagne cinesi di cyber-spionaggio contro gli Stati Uniti, ribadendo come la rete di Salt Typhoon sia parte di un ecosistema nazionale cinese che combina attori statali e privati nel panorama internazionale.

Fonti:

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/gruppo-salt-typhoon/