

CASO DI STUDIO · CYBER

Volt Typhoon: che cosa significa avere un intruso che non ruba nulla

Nel 2023 le agenzie occidentali rivelano un attore cinese annidato nelle infrastrutture critiche americane. Non esfiltra dati. E proprio per questo è il caso più istruttivo della cyber-intelligence recente.

di Carmine Di Marino

Compromettere l'impianto idrico di una municipalità statunitense, o la rete elettrica di un'isola del Pacifico, non frutta proprietà intellettuale né dati industriali. Se quell'attività si osserva, la sua finalità dev'essere altra. È questo il residuo che Volt Typhoon trasforma in oggetto autonomo di analisi, costringendo a una domanda scomoda: che cosa fa un servizio di intelligence quando ottiene un accesso e non lo usa per raccogliere?

I fatti

Il 24 maggio 2023 Microsoft Threat Intelligence pubblica un rapporto su un attore designato Volt Typhoon, attivo contro infrastrutture critiche statunitensi con particolare concentrazione su Guam, attribuendolo a un soggetto sponsorizzato dallo Stato cinese; lo stesso giorno NSA, CISA, FBI e i partner Five Eyes diffondono un advisory congiunto. Il documento di riferimento arriva il 7 febbraio 2024 (AA24-038A): i comparti colpiti sono comunicazioni, energia, trasporti e sistemi idrici, e — punto qualificante — gli attori cercano di pre-posizionarsi sulle reti per rendere possibili attacchi disruptivi o distruttivi nell'eventualità di una crisi o di un conflitto con gli Stati Uniti. In alcune reti l'accesso era stato mantenuto per almeno cinque anni. Nel gennaio 2024, Dipartimento di Giustizia e FBI disarticolano la KV Botnet, una rete di router domestici a fine vita usata per mascherare le operazioni.

Un intruso che non lascia tracce di malware

Il tratto distintivo di Volt Typhoon è che non impiega malware proprietario. La tecnica prevalente, il *living off the land*, consiste nell'usare esclusivamente strumenti già presenti nel sistema-bersaglio: l'accesso iniziale sfrutta vulnerabilità note di apparati di rete esposti su Internet — firewall, concentratori VPN, dispositivi di frontiera, spesso a fine vita; la persistenza è affidata alle credenziali estratte, non a un impianto; il traffico è instradato attraverso apparati domestici compromessi per apparire locale. La conseguenza difensiva è dirimente: un'architettura fondata sul riconoscere «ciò che è malevolo» è cieca, perché non vi è nulla di malevolo da riconoscere. A distinguere l'intruso non è l'atto, ma il contesto — e questo richiede una linea di base comportamentale, log centralizzati e la capacità di interrogarli.

Dal cyber espionage al pre-positioning

Si giunge al nucleo concettuale del caso. Il *pre-positioning* designa l'acquisizione e il mantenimento di un accesso senza che venga impiegato — né per raccogliere né per produrre effetti — nell'attesa di una contingenza futura: non è raccolta e non è attacco, è la costituzione di un'opzione. La selezione dei bersagli è la principale prova dell'intenzione. La concentrazione su Guam — sede della base aerea di Andersen e di una base navale, perno logistico della proiezione di forza nel Pacifico occidentale — è l'indicatore più eloquente: un'isola priva di industria tecnologica non è un bersaglio plausibile per lo spionaggio economico, ma è coerente con la preparazione di un'opzione militare.

Un giudizio, non un fatto

Per stabilire quale ipotesi le evidenze sostengano conviene applicare il metodo delle ipotesi concorrenti. Tre le ipotesi: spionaggio ordinario (H1), *pre-positioning* per una contingenza militare (H2), mantenimento generico di accessi (H3). La selezione dei bersagli è incompatibile con H1; l'accettazione del costo del *living off the land* milita contro H1; la durata dell'accesso senza utilizzo è compatibile con H2 e H3; l'assenza di payload distruttivi impiantati è argomento contro H2 nella sua forma forte. Il giudizio — valutazione analitica a confidenza medio-alta, non fatto — è che sia meglio sostenuta una versione debole di H2: la costruzione di un'opzione di interdizione mantenuta al livello dell'accesso, non del pre-impianto dell'effetto.

Il paradosso della deterrenza

Ne discende un paradosso. Se il *pre-positioning* deve dissuadere, deve essere noto all'avversario; ma appena noto viene rimosso, e l'opzione svanisce. La deterrenza cibernetica soffre così di una contraddizione che quella nucleare non conosce: là la capacità è ostentabile senza essere consumata, qui l'ostentazione la distrugge. La stessa sequenza divulgativa del 2023-2024 può leggersi come una mossa: l'annuncio all'avversario che l'opzione è stata individuata e che il suo valore è in erosione. Quanto al ricorrente riferimento a una finestra attorno al 2027, va ricordato che l'affermazione originaria riguardava la *capacità* militare cinese, non l'*intenzione* politica: confondere le due è un errore classico dell'analisi.

La contro-analisi cinese

Il caso è istruttivo anche perché Pechino non si è limitata a smentire: nel 2024 il CVERC ha pubblicato tre rapporti che negano l'esistenza stessa di Volt Typhoon come attore statale cinese, parlando di disinformazione statunitense e di attività criminale comune. Il trattamento corretto non è né l'adesione né il rigetto sommario. Le due società private citate a sostegno hanno dichiarato che la propria ricerca era stata travisata, e i rapporti cinesi non producono indicatori tecnici verificabili in proprio. Va però concesso un punto: il rilievo secondo cui l'attribuzione occidentale poggia su fonti private, telemetria non ispezionabile e valutazioni istituzionali che non espongono la base probatoria è, in sé, fondato — ed è il medesimo rilievo che un analista occidentale dovrebbe formulare in autonomia.

La risposta è la resilienza

Contro il pre-positioning, la deterrenza per punizione sconta attribuzione tardiva, rischio di escalation e asimmetria delle superfici esposte. La leva realmente disponibile è la deterrenza per negazione, che coincide con la resilienza: ridondanza, segmentazione, capacità di operare in condizioni degradate, tempi di ripristino provati. È la conclusione, poco spettacolare, che il caso impone: la difesa non è la controffensiva, è la capacità di funzionare quando l'opzione avversaria viene esercitata.

NOTA DI METODO

Cinque livelli di prudenza attraversano questo caso: la presenza in una rete è un indicatore, non un allarme di attacco imminente; l'evidenza più diagnostica è quella negativa (l'assenza di esfiltrazione); l'attribuzione è un giudizio articolato, non un fatto; la finalità è un'ipotesi calibrata, non una certezza; e rendere pubblico un accesso avversario è esso stesso una decisione di intelligence, con un costo e un beneficio.

Fonti principali

Microsoft Threat Intelligence, «Volt Typhoon targets US critical infrastructure...», 24 maggio 2023.

NSA-CISA-FBI e partner, advisory congiunto AA23-144A, 24 maggio 2023.

CISA-NSA-FBI e partner, advisory congiunto AA24-038A, 7 febbraio 2024.

U.S. Department of Justice, operazione contro la KV Botnet, 31 gennaio 2024.

R. J. Heuer Jr., Psychology of Intelligence Analysis, CIA, 1999 (cap. 8, ipotesi concorrenti).

CVERC, rapporti «Volt Typhoon» I-III, 2024 (fonte di parte; tesi contestate dalle società citate).