

CASO DI STUDIO · CYBER

Salt Typhoon: quando lo spionaggio diventa sorveglianza globale

Una rete di telecomunicazioni non custodisce segreti propri: custodisce quelli di tutti gli altri. Il caso che trasforma lo spionaggio in una capacità planetaria di identificare e seguire le persone.

di Carmine Di Marino

Una rete di telecomunicazione non conserva informazioni proprie di grande valore, ma è il luogo attraverso cui transitano le informazioni di tutti gli altri. Il rapporto tra costo dell'operazione e volume del prodotto informativo è, in questo comparto, di alcuni ordini di grandezza superiore a quello di qualunque altro bersaglio. È la ragione per cui il caso Salt Typhoon, pur essendo «spionaggio puro», cambia natura strategica: la scala e il bersaglio ne fanno qualcosa di diverso da una campagna di furto industriale.

L'ironia dell'accesso legale

Vi è un'ironia istruttiva. Gli operatori delle democrazie liberali sono obbligati per legge a mantenere sistemi di intercettazione legale: architetture progettate per consentire, su provvedimento dell'autorità, l'accesso selettivo alle comunicazioni. Chi ne conquista il controllo eredita esattamente le capacità riservate all'autorità giudiziaria, senza il provvedimento. Non è un'ipotesi teorica: il precedente più noto è la compromissione, tra il 2004 e il 2005, del sistema di intercettazione legale di un operatore greco, con autori mai accertati. Ogni accesso eccezionale creato per finalità legittime è una superficie di attacco permanente.

I metadati contano più del contenuto

Per un servizio di intelligence i metadati — chi ha chiamato chi, quando, da dove, per quanto — sono spesso più preziosi del contenuto: strutturati, analizzabili in massa, non richiedono traduzione né decrittazione e producono direttamente il grafo delle relazioni e il modello di vita del bersaglio. Il contenuto dice cosa due persone si sono dette; i metadati dicono chi conosce chi — e questo, per il controspionaggio, è il dato che conta.

Che cosa dicono le fonti

Nell'autunno del 2024 emerge, prima per via giornalistica e poi con conferme istituzionali, la compromissione di più operatori di telecomunicazione statunitensi da parte di un attore designato Salt Typhoon, con un accesso che avrebbe interessato anche le infrastrutture di intercettazione legale. Il documento che consente di uscire dalla zona grigia — dove la fonte è il funzionario non identificato — è l'advisory congiunto AA25-239A del 27 agosto 2025, sottoscritto da più di dieci paesi. Esso rinuncia alla nomenclatura commerciale (riferendosi ad «attori APT») e, soprattutto,

collega l'attività a tre società cinesi indicate come fornitrici di prodotti e servizi cyber ai servizi di intelligence della RPC, comprese unità del PLA e del MSS: la conferma istituzionale del modello ad appalto. Il profilo tecnico è ordinario — vulnerabilità note, apparati di frontiera e di dorsale — e la distribuzione settoriale eccede le telecomunicazioni: governo, trasporti, ospitalità alberghiera, reti militari, in più paesi.

Tre giacimenti che, incrociati, ricostruiscono una persona

La combinazione settoriale non è casuale. Telecomunicazioni, trasporti e ospitalità non hanno nulla in comune sul piano industriale, ma tutto su quello informativo: sono i tre giacimenti che, incrociati, ricostruiscono movimenti e relazioni di una persona. La rete telefonica dice dove si trovava e con chi comunicava; i trasporti dove è andato; i sistemi alberghieri dove ha dormito e chi altro alloggiava nella stessa struttura la stessa notte. Tradotto: non spionaggio economico, ma controspionaggio su scala globale. Il caso si iscrive in una serie decennale — la violazione dell'ufficio del personale federale statunitense (2015), la catena alberghiera (2018), la centrale rischi creditizia (2017, con incriminazione di militari cinesi nel 2020). La tesi dell'aggregazione, secondo cui questi episodi popolerebbero un archivio unico, è un'inferenza forte e ampiamente condivisa, ma va qualificata come valutazione, non come fatto.

Salt e Volt: lo stesso accesso, due usi

Il confronto con Volt Typhoon è illuminante. La finalità diverge nettamente — Volt costruisce un'opzione da esercitare in crisi, Salt una capacità di raccolta permanente — e così il bersaglio. Ma le tecniche sono in continuità: entrambi privilegiano gli apparati di frontiera, sfruttano vulnerabilità note, operano con strumenti nativi e credenziali legittime, accettano la lentezza in cambio della permanenza. È il medesimo modello operativo. E qui sta il punto teoricamente decisivo: un router di dorsale compromesso serve tanto la raccolta quanto l'interdizione — dal medesimo accesso si può copiare il traffico o interromperlo. Quando il difensore rileva un'intrusione osserva un accesso, non un'intenzione; stabilire se si tratti di Salt o di Volt richiederebbe di conoscere una decisione che risiede a Pechino. Ne discende una conclusione onerosa ma inevitabile: ogni accesso persistente su infrastruttura critica va trattato come se fosse il peggiore dei due.

NOTA DI METODO

Sul modello ad appalto, la risposta occidentale rivela dove sta il punto debole cinese: non l'operatore, ma il fornitore. Le misure restrittive contro una delle tre società e la nomina pubblica delle altre sono un riconoscimento implicito che l'esternalizzazione, mentre dà scala e negabilità, espone la catena ad attribuzione e sanzione.

Fonti principali

CISA-NSA-FBI e partner internazionali, advisory congiunto AA25-239A, 27 agosto 2025.

U.S. Department of the Treasury (OFAC), misure su Sichuan Juxinhe Network Technology, 17 gennaio 2025.

V. Prevelakis, D. Spinellis, «The Athens Affair», IEEE Spectrum, luglio 2007.

United States v. Wu Zhiyong et al., N.D. Georgia, 10 febbraio 2020 (Equifax).