Attacchi cyber, alleanza fra gruppi di hacker filorussi: chi sono, cosa vogliono e come usano i «pc zombie» di Rinaldo Frignani

Dalle infrastrutture ai supermercati, un «salto di qualità» per creare il caos nel Vecchio Continente. Alle due sigle si è aggiunta anche quella dei «Z-Pentest»: gli Usa hanno messo su di loro una taglia fino a due milioni di euro (Fonte: https://roma.corriere.it/ 9 novembre 2026)



Il tunnel del Brennero preso di mira dagli hacker nei giorni scorsi

Hanno cambiato nome più volte, si sono uniti e poi divisi. Hanno agito sotto sigle differenti. Hanno disorientato chi dall'Occidente gli stava dando la caccia. E oggi cercano di creare il caos in Europa più di quanto abbiano mai fatto dal giorno dell'invasione russa dell'Ucraina. Un salto di qualità — almeno così sembra —, **mettendo da parte le abilità mostrate fino a un mese fa, per concentrarsi su attacchi diretti alle infrastrutture dei Paesi «nemici della Russia». Un'alleanza fra gruppi hacker ricollegabili al Cremlino,** secondo gli ultimi riscontri dell'intelligence europea, al netto delle smentite ripetute e categoriche di Mosca, che vede in prima linea adesso i «Noname057(16)» con gli «Everest». Gli esperti delle incursioni informatiche con la saturazione delle pagine web di ministeri e aziende usando il ddos — milioni di richieste d'accesso provenienti da pc zombie — insieme con la crew responsabile di ricatti ransomware a società pubbliche e private. Nata nel 2020, «Everest» ha debuttato in Italia l'anno successivo con l'estorsione alla Siae.

L'unione per la guerra ibrida e cognitiva

Il sospetto è che gli hacker che fino a oggi hanno sfruttato le fragilità dei sistemi informatici per infiltrarsi e chiedere riscatti — sbloccando a pagamento i file rubati e poi criptati — si siano messi a

disposizione della causa comune **per la guerra ibrida e cognitiva per colpire l'Europa.** Il gruppo è infatti quello accusato di aver preso di mira il supertunnel del Brennero il 17 ottobre scorso, **ma a luglio si era già fatto vivo in Svizzera contro la Stadler Rail:** al costruttore ferroviario del Canton Turgovia aveva chiesto un riscatto di 10 milioni di franchi. Nel 2025 però sempre «Everest» ha rivendicato l'attacco contro la Svenska Kraftnät, il gestore della rete elettrica svedese.

I prossimi obiettivi: reti idriche ed elettriche

Dal canto loro i «Noname», **solo in Italia coinvolti in più di 350 incursioni**, hanno rivendicato giorni fa — sempre che siano davvero loro —l 'offensiva contro la grande distribuzione alimentare in diversi Paesi europei, con la manomissione a distanza di centinaia di celle frigorifere dei supermercati e la perdita di prodotti per decine di milioni di euro. In passato avevano attaccato con il ddos creando per lo più disagi, senza causare però gravi danni materiali. **Adesso invece è successo.** E — come hanno confermato assumendosi la responsabilità dell'azione — **non avrebbero intenzione di fermarsi:** «Ancora una volta abbiamo dimostrato il vero livello della maturità digitale occidentale. Tenete d'occhio le nostre azioni sulla scena globale». Nel mirino ora ci sarebbero reti idriche ed elettriche.

Le minacce a Mattarella e la taglia sui poliziotti

Un radicale cambio di linea del gruppo attivo dal marzo 2022, che ha creato un franchising sulla piattaforma «DDosia» ricompensando gli affiliati, e che nel 2025 ha perfino minacciato **il presidente della Repubblica Sergio Mattarella, avvalorato oggi dalla lista,** con tanto di taglia per chi fornisce informazioni utili e private, che gli hacker hanno pubblicato a ottobre sul dark web dei nomi degli investigatori italiani e tedeschi — insieme con quello del ministro degli Esteri Antonio Tajani — protagonisti dell'operazione «Eastwood», con la quale è stato inferto un duro colpo proprio ai «Noname».

I blitz informatici contro le aziende Usa

Insomma, al netto della raffica di falsi allarmi aerei della settimana scorsa, tutti in orario ufficio e interrotti nel weekend, la minaccia appare più forte e concreta. Tanto che alle due sigle dei supermercati se n'è aggiunta un'altra: i «Z-Pentest», **ex «Cyber Army of Russia Reborn»**, ritenuti dagli investigatori statunitensi collegati al «Centro tecnologie speciali» dei servizi di intelligence russi (Gru) e responsabili di azioni contro le infrastrutture critiche Usa dalla fine del 2023. Anche di «numerosi attacchi malevoli contro le aziende idriche in **Indiana, New Jersey e Texas**» e di una fuga di ammoniaca con distruzione di tonnellate di carne **in uno stabilimento di Los Angeles.** Come oggi in Europa. Il «Reward for Justice» ha promesso fino a due milioni di dollari a chi fornisca «informazioni che portino all'identificazione o alla localizzazione di qualsiasi persona che, agendo su indicazione o sotto il controllo di un governo straniero, **partecipi ad attività informatiche**

dannose contro le infrastrutture critiche statunitensi». Nella comunicazione si fanno i nomi di Yuliya Pankratova, Denis Degtyarenko, e del misterioso agente «Cyber_1ce_Killer».