Europa sotto attacco cyber, chi sono i «Noname» e i loro alleati hacker. «Voi non avete ancora capito come difendervi da noi» di Rinaldo Frignani

Oltre alla crew che ha rivendicato le azioni contro i supermercati anche in Italia, ci sono altri gruppi filorussi che sono comparsi negli ultimi tempi: dal «Male State» a «Z-Pentest», da «Everest» alle bande vicine ai servizi segreti

(Fonte: https://roma.corriere.it/ 8 novembre 2026)



«Incidenti come questi hanno colpito centinaia di località in tutta Europa, eppure non hanno imparato dai loro errori. Ancora una volta abbiamo dimostrato il vero costo della maturità digitale occidentale. Quindi tenete d'occhio le nostre azioni sulla scena globale». Dalla saturazione dei sistemi informatici di istituzioni e aziende prese di mira, usando il ddos con milioni di richieste d'accesso provenienti da pc zombie in tutto il mondo, all'attacco diretto alla grande distribuzione alimentare europea. **Annunciando però di saper colpire in futuro la rete idrica e quella elettrica.**

Gli hacker filorussi «**Noname057(16)**» insieme con gli alleati della «**Z-Pentest**» hanno alzato il tiro proprio nei giorni scorsi dimostrando, se la loro rivendicazione dovesse essere confermata dalle indagini, di saper andare anche oltre la semplice azione dimostrativa che causa disagi.

Sono loro in cima alle crew che, **al netto delle smentite ripetute e categoriche di Mosca, sono fortemente sospettate di aver dato vita** a una nuova e più concreta campagna anti-occidentale, dopo aver già organizzato più di 350 incursioni informatiche solo contro l'Italia dall'invasione russa dell'Ucraina. Un rischio costante tanto che martedì il ministro dell'Interno Matteo Piantedosi ha convocato il Comitato nazionale per l'ordine e la sicurezza pubblica al Viminale per fare il punto

sugli attacchi cyber al nostro Paese in un panorama dove sono gli investigatori europei in generale a chiamare in causa la Russia.

I leader ricercati dalla Germania

L'operazione «Eastwood» dello scorso anno portata a termine dalle polizie europee, anche quella italiana, ha svelato un primo livello del gruppo hacker con oltre mille contatti che sono stati identificati. Al vertice della crew anche cinque persone attualmente ricercate da Europol e dalla polizia tedesca. Si tratta di Olga Evstratova, Mihail Evgeyevich Burlakov, Andrey Stanislavovich Avrosimow, Maxim Lupin e Andrey Muravyov, **considerati gli organizzatori delle pagine dei «Noname»** su Telegram nonché delle **incursioni informatiche**. A dargli la caccia sono soprattutto pm e poliziotti di Francoforte che infatti sono stati inseriti nella lista del «tribunale» degli hacker insieme con quelli italiani (il procuratore capo di Roma Francesco Lo Voi e il direttore della polizia postale Ivano Gabrielli) che cerca informazioni su di loro dietro il pagamento di una taglia.

Il manifesto e il comandante

Il manifesto del gruppo, nato a marzo 2022, un mese dopo l'invasione, è stato inizialmente un messaggio contro i rivali ucraini con il motto del comandante russo Aleksandr Nevskij: **«Chiunque venga da noi con una spada, perirà di spada!»,** ma poi le loro azioni - soprattutto ddos, come detto - si sono allargate ai «nemici della Russia» colpiti da azioni cibernetiche ripetute. Da Telegram la crew si è poi spostata su GitHub con la piattaforma «**DDosia**», per sferrare attacchi in franchising e dietro compenso. **Dai riscontri investigativi sono alleati di altri gruppi come «Killnet», «Xaknet» e appunto «Z-Pentest».** Nel febbraio 2025 hanno preso di mira il presidente della Repubblica Sergio Mattarella: «Ha paragonato la Russia al Terzo Reich, provocando una dura reazione da parte del ministero degli Esteri russo. Mosca ha già promesso che tali dichiarazioni non resteranno senza conseguenze».

La taglia degli americani contro il «Cyber Army» russo

Ma se oggi i «**Noname**» propogono taglie sui leader occidentali, già negli anni passati il governo americano - con il Reward for Justice - aveva promesso fino a 2 milioni di dollari «per 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 in violazione del Computer Fraud and Abuse Act». **L'obiettivo erano gli hacker del «Cyber Army of Russia Reborn», noto anche come «Z-Pentest»**, ritenuto dagli investigatori Usa collegati al «Centro Tecnologie Speciali» dei servizi di intelligence russi Gru, e responsabili di attacchi alle infrastrutture critiche Usa dalla fine del 2023. Anche «numerosi attacchi informatici malevoli contro le aziende idriche in Indiana, New Jersey e Texas», proprio come si teme oggi in Europa.

Nel novembre di due anni fa hanno hackerato un impianto di lavorazione della carne nella contea di Los Angeles, danneggiando migliaia di chili di carne e provocando una fuga di ammoniaca, che ha costretto all'evacuazione dell'impianto per diverse ore. All'epoca i leader del gruppo ricercati erano Yuliya Pankratova, nick name YUliYA, e Denis Degtyarenko, detto Dena.

L'alleanza con «Everest» specializzata in riscatti ferroviari

Ma l'altra sigla ricomparsa di recente è quella di «**Everest**», nata nel 2020 e specializzata però in ricatti di tipo ransomware. In Italia il suo debutto è stato con **l'estorsione ai danni della Siae nel 2021,** ma ce ne sarebbero stati molti altri sempre ai danni di enti e aziende importanti. Adesso il sospetto è che gli hacker che chiedono riscatti per sbloccare informazioni riservate rubate e **poi cifrate da rivendere sul dark web** si siano messi a disposizione della causa legata alla guerra ibrida in atto per colpire l'Europa tutti insieme.

Adesso «**Everest**» **è accusata di aver preso di mira il supertunnel del Brennero con l'attacco informatico del 17 ottobre scorso.** A luglio tuttavia lo stesso gruppo si è fatto vivo in Svizzera prendendo di mira la Stadler Rail chiedendo al costruttore ferroviario turgoviese un riscatto di 10 milioni di franchi. Nel 2025 ha rivendicato un attacco contro Svenska kraftnät, il gestore della rete elettrica svedese.

La siglia del «Male State» sfruttata negli allarmi bomba aerei

Più defilata, almeno stando alla smentita di un suo coinvolgimento negli allarmi bomba sugli aerei in mezza Europa della settimana scorsa, la posizione del «Male State», lo Stato maschile russo, associazione peraltro messa al bando **dagli stessi giudici di Mosca** per istigazione all'odio contro le donne. Il sospetto in questo caso è che in realtà il nome del gruppo sia stato sfruttato da altri per gettare nel panico di viaggiatori che utilizzano il trasporto aereo, le compagnie e le industrie collegate.

Il «**Muzhskoye gosudarstvo**», **movimento estremista russo, ultranazionalista, razzista, omofobo e misogino** fondato dieci anni fa da Vladislav Pozdnyakov, l'ideologo del **nazional-patriarcato,** condannato nel 2018 e tre anni dopo dichiarato fuorilegge dalla magistratura, mentre il canale social «VKontakte» aveva già bloccato i suoi profili.

I gruppi che danno anche la caccia ai dissidenti

Ma la galassia delle sigle hacker filorusse è immensa, composta da gruppi che scompaiono, si aggregano e poi ricompaiono sotto altri nomi. Ce ne sono alcuni che agiscono in proprio e altri che invece sembrano rispondere a ordini statuali, **anche se le indagini su questo punto sono ancora in corso.** Altri ancora, come detto, sarebbero collegati ai servizi di sicurezza russi. Come l'«**Apt44**», che concentra le sue attività in particolare contro l'Ucraina mentre quelli più datati sono ancora oggi «**Cozy Bear**» e «**Fancy Bear**», quest'ultimo impegnato anche nella caccia ai dissidenti.