

NoName057 (16), tutti i bersagli italiani degli attacchi DDoS rivendicati dal gruppo filo-russo



Dopo le contestate dichiarazioni della Russia sul Presidente italiano Mattarella, le reazioni non si sono fatte attendere neanche sul fronte digitale: negli ultimi giorni molte agenzie ed enti pubblici nazionali sono stati colpiti da attacchi informatici, rivendicati dal *cyber group* filo-russo NoName057 (16).

Attacchi informatici filo-russi all'Italia: origini e conseguenze

Il *casus belli* risalirebbe allo scorso 5 febbraio, quando il Presidente della Repubblica, in un discorso pubblico presso l'Università di Marsiglia, aveva paragonato l'offensiva di Mosca in Ucraina alle *"guerre di conquista"* condotte dal Terzo Reich nell'Europa del secolo scorso.

Per tutta risposta, alcuni giorni dopo, la portavoce del ministero degli Esteri russo Maria Zakharova ha dichiarato che un simile paragone *"non potrà rimanere senza conseguenze"*.

A tali affermazioni, definite *"inopportune e fuori luogo"* dai rappresentanti del governo italiano, ha fatto seguito una serie di attacchi DDoS che il 17 febbraio ha iniziato a prendere di mira numerosi obiettivi di alto profilo istituzionale in Italia.

Finora, tra le realtà colpite spiccano:

- i **Ministeri** dello Sviluppo Economico e delle Infrastrutture e dei Trasporti;
- i **corpi armati** dei Carabinieri, della Guardia di Finanza e dell'Aeronautica Militare;
- gli **aeroporti** di Malpensa e Linate, i **porti** di Trieste e Taranto e l'agenzia Italia Energia Aerospaziale;
- alcune società che erogano **servizi idrici** o di **trasporto pubblico locale**, nonché l'Automobile club italiano (ACI);
- gli **istituti finanziari** Intesa Sanpaolo, Nexi e Mediobanca;
- diverse **industrie del comparto bellico**.

Motivate dagli attaccanti con la presunta “russofobia” del Capo di Stato italiano, le operazioni di NoName057 si sono limitate – come di consueto – a bloccare per qualche tempo l'accesso ai siti delle realtà colpite, senza conseguenze sulla sicurezza dei dati o delle infrastrutture.

NoName057 (16), dall'hacktivismo alla guerra ibrida

Il gruppo NoName057 (16) si è fatto conoscere nel 2022, poco dopo l'inizio dell'offensiva russa in Ucraina.

Da allora si è attribuito numerosi DDoS lanciati contro siti governativi e istituzionali ucraini, statunitensi ed europei: l'Italia è stata presa di mira a partire dal 2023, con una serie di attacchi rivolti a Ministeri e altri obiettivi minori, inclusa l'Agenzia dei Trasporti romana ATAC.

Nel Manifesto pubblicato al tempo sul canale Telegram, si ricordavano “ai nemici” le parole dell'eroe nazionale russo Alexander Nevsky: *“Whoever comes to us with a sword will perish by the sword!”*

Al netto dei riferimenti bellici, nell'attuale fase sembra che

i *threat actor* come NoName057 attribuiscano grande importanza alla comunicazione e operino in modo più coordinato che in passato, sebbene solitamente i membri si collochino in diversi Paesi (pochi mesi fa alcuni esponenti del gruppo sarebbero stati arrestati in Spagna).

Le attività di NoName057 (16), analogamente a quelle del gruppo Killnet, rientrano pertanto a pieno titolo nella terza era dell'hacktivismo, dove si osserva la trasformazione di un movimento originariamente decentralizzato – e tendenzialmente antigovernativo – in fenomeno organizzato e strategico.

Usando il “defacciamento” dei siti istituzionali di uno Stato a fini prevalentemente dimostrativi, l'organizzazione si colloca in un panorama di minacce sempre più ibride e diffuse: in questo scenario, è evidente come non basti implementare misure di sicurezza informatica per proteggere le infrastrutture digitali nazionali dal rischio di attacchi costanti e imprevedibili.

Le attività del gruppo NoName057 (16) e di altri simili attaccanti mostrano infatti una dimensione decisamente più politica che tecnologica, chiamando in causa – al fianco della cybersecurity – tutte le armi della diplomazia.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/noname05716-attacchi/>