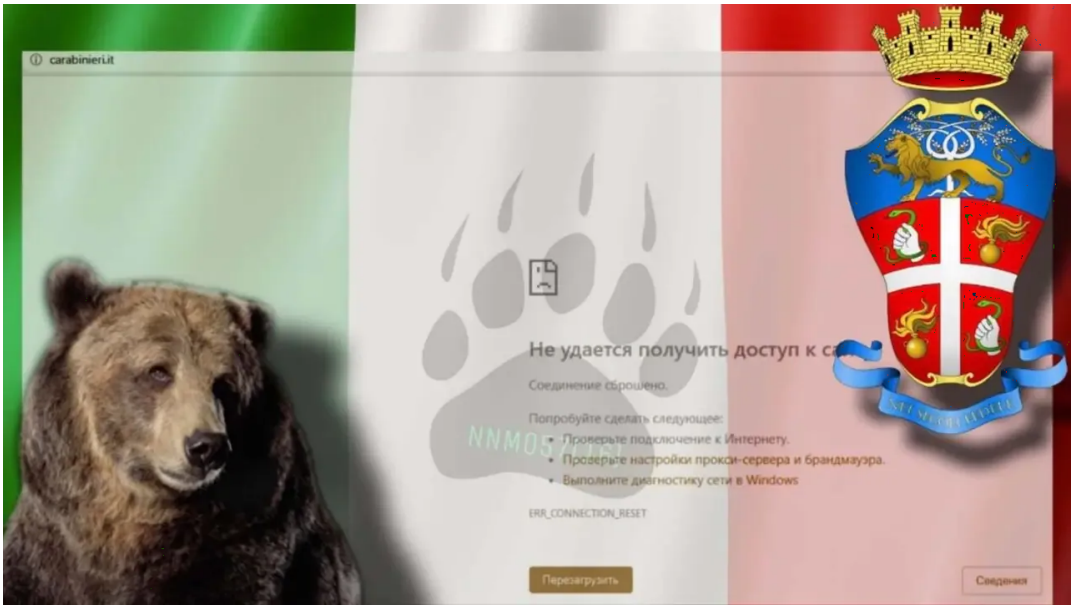


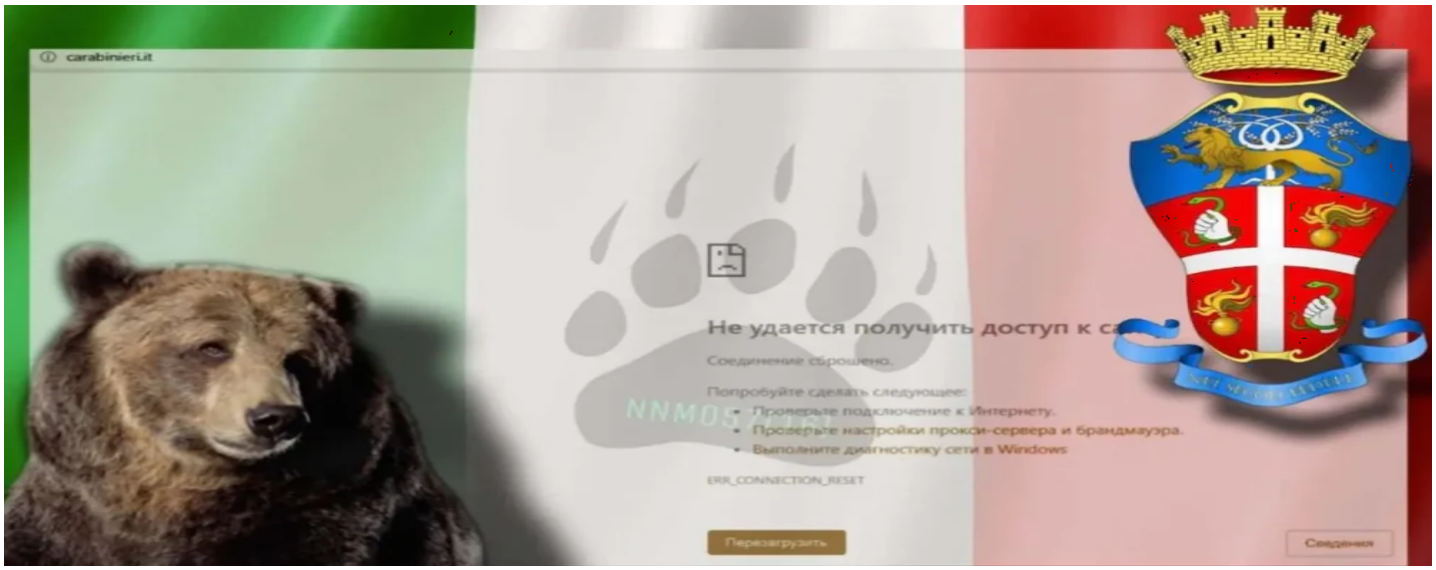
NoName057: l’impressionante offensiva cyber contro l’Italia

Pubblicato il 24/02/2025

Negli ultimi giorni, l’Italia è stata teatro di una serie di attacchi informatici che hanno coinvolto numerosi settori, mettendo in luce la vulnerabilità delle infrastrutture digitali nazionali. Il gruppo hacker filorusso NoName057(16), attivo dal marzo 2022, ha intensificato le sue operazioni contro siti istituzionali e aziende di rilievo, sfruttando la tecnica del **Distributed Denial of Service (DDoS)** per rendere inaccessibili piattaforme strategiche.

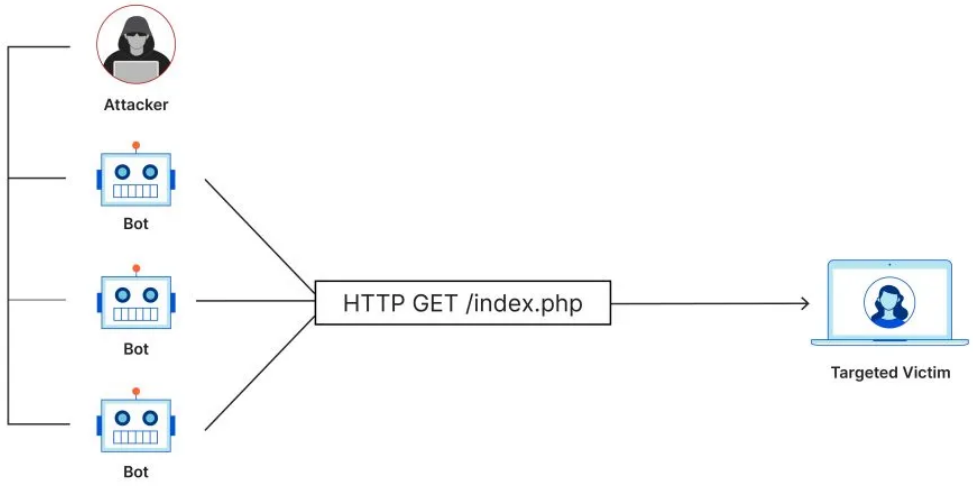
NoName057 attacca istituzioni e aziende

Gli attacchi, condotti per sette giorni consecutivi, hanno preso di mira il settore governativo, i trasporti e il comparto bancario. In particolare, sono stati colpiti i siti dei **ministeri degli Esteri, delle Imprese e della Difesa,** insieme a quelli dell'Aeronautica militare e al sito personale della presidente del Consiglio, Giorgia Meloni. Nei giorni scorsi, altre realtà importanti come **Leonardo, Banca d'Italia, l'Autorità dei trasporti, Edison, Fininvest e Parmalat** hanno subito attacchi analoghi, e addirittura il porto di Genova è stato bersaglio di un attacco venerdì scorso. Questi attacchi hanno provocato blackout temporanei, causando disservizi significativi agli utenti e interruzioni nel regolare svolgimento dei servizi digitali.



DDOS: Modus Operandi

La strategia adottata da NoName057(16) si basa sull’impiego di botnet, ovvero reti di dispositivi compromessi – computer, server, router e dispositivi IoT – controllati da remoto per sommergere i siti web con un flusso massiccio di richieste. Un elemento distintivo di questo modus operandi è l’utilizzo della piattaforma DDosia, che consente ai simpatizzanti di contribuire alle operazioni in cambio di ricompense finanziarie. Questa forma di "crowdsourcing" del crimine informatico ha ampliato la portata dell’offensiva, causando problemi non solo in Italia, ma anche in altri Paesi europei.



Possibili motivazioni degli attacchi

Secondo le dichiarazioni rilasciate sul canale Telegram del gruppo, gli attacchi sono una risposta diretta alle recenti affermazioni del **Presidente della Repubblica Sergio Mattarella**. Durante un intervento all’Università di Marsiglia, il capo dello Stato aveva paragonato le azioni della Russia all’espansionismo nazista, provocando una reazione furiosa da parte degli hacker. In questo contesto, il collettivo ha definito la propria offensiva come una “punizione per l’Italia”, in risposta alle posizioni politiche espresse dal presidente. La tensione è ulteriormente aumentata quando, questa mattina, **la portavoce del ministero degli Esteri russo, Maria Zakharova**, ha dichiarato che le parole di Mattarella “non resteranno senza conseguenze”, sottolineando come le affermazioni possano scatenare reazioni a livello internazionale.

Come ridurre gli attacchi

Per fronteggiare questa minaccia, le autorità italiane hanno adottato sistemi di monitoraggio avanzati e implementato misure di mitigazione del traffico malevolo. Tecniche come il rate limiting, che limita il numero di richieste accettate in un intervallo temporale, e l'impiego di servizi anti-DDoS come indicati dalla dall'Agenzia per la Cybersecurity nazionale (ACN) hanno contribuito a ridurre l'impatto degli attacchi. Tuttavia, la continua evoluzione delle minacce informatiche richiede un costante aggiornamento della cyber intelligence e una collaborazione stretta con partner internazionali.

In conclusione, l'offensiva di NoName057(16) non rappresenta una sfida tecnica per la sicurezza digitale italiana, ma anche un segnale delle crescenti tensioni geopolitiche. In un'epoca in cui le armi digitali assumono un ruolo sempre più centrale, **è fondamentale rafforzare le difese cibernetiche** e promuovere una cooperazione internazionale per contrastare efficacemente il crimine informatico e garantire la protezione delle infrastrutture critiche.

IN CASO DI INCIDENTE

CONTATTA CSIRT ITALIA

Link notizia: https://www.ilsole24ore.com/art/il-collettivo-hacker-pro-russia-noname057-attacca-l-italia-cosa-c-e-dietro-cortina-fumogena-AGcLt5zC