

Server italiani di banche e aziende hanno subito sabotaggi da parte di hacktivisti legati a Mosca

Nuovi attacchi informatici filorussi: coinvolti anche hacker palestinesi

MATTIA CIRILLI

Nuovi attacchi hacker hanno colpito l'Italia nella giornata di ieri. Ai recentissimi sabotaggi che hanno interessato la crew Noname057(16) si sono aggiunte anche le azioni coordinate del gruppo palestinese Alixsec. L'organizzazione sostiene anch'essa la causa

russe, ed è dunque plausibile un legame con i Noname057. Gli hacktivist filopalestinesi hanno nel mirino, in particolare, gli interessi israeliani e già da tempo portano avanti una cyber-guerra contro Tel Aviv. Da quello che si sa al momento, Alixsec fa parte di 'The Holy League', un collettivo di 70 organizzazioni di attivisti

che vanta rapporti con servizi segreti dei cosiddetti 'Stati canaglia' e che ha un profilo antioccidentale.

Siti nel mirino

Anche stavolta i responsabili degli attacchi informatici ai danni dei sistemi italiani sono i cyberterroristi

SERVER ITALIANI DI BANCHE E AZIENDE HANNO SUBITO SABOTAGGI DA PARTE DI HACKTIVISTI LEGATI A MOSCA

Nuovi attacchi informatici filorussi: coinvolti anche hacker palestinesi

del gruppo filorusso Noname057(16), che hanno rivendicato su Telegram i vari disagi procurati ai server nostrani. Coadiuvati stavolta dall'ancora poco noto gruppo palestinese Alixsec, hanno messo nel mirino i siti di banche, come Intesa San Paolo e Monte dei Paschi, i porti di Taranto e Trieste, e alcune aziende, tra cui Vulcainair, di cui si ha certezza assoluta del sabotaggio. L'Agenzia per la cybersicurezza nazionale si è messa fin da subito al lavoro. Sono stati infatti avvistati tempestivamente i soggetti colpiti, supportandoli nell'iter di ripristino delle funzionalità. Alcuni domini risultavano tuttavia intaccati in modo pesante dagli attacchi, che sono sempre di tipo Ddos, Distributed denial of service. Questo genere

di illecito viene ordito tramite Botnet ovvero reti di pc "zombie" infettati da malware, che possono essere risvegliati a comando dall'operatore e usati per vari scopi illegali.

Il precedente

Si tratta già della seconda ondata consecutiva dopo quella che ha colpito il Belpaese sabato, coinvolgendo i siti dei ministeri e delle istituzioni. Tra i server citati come attaccati erano inclusi i ministeri dello Sviluppo, degli Esteri, delle Infrastrutture e dei Trasporti, Consob, Carabinieri, Marina, Aeronautica e aziende del trasporto pubblico locale - l'Atac di Roma, l'Amat di Palermo, l'Amt di Genova. Stando alle varie dichiarazioni di sabato scorso, gli attacchi, partiti dal-

le 7 del mattino circa, avrebbero provocato disagi contenuti. Stavolta, invece, il bersaglio è stato costituito da banche e aziende, coordinandosi col succitato gruppo Alixsec, che ha sabotato i server di Olidata, Skillbill e Zucchetti Design. La concomitanza dei cyberattacchi con la presenza del presidente ucraino Volodymyr Zelensky in Italia non è affatto casuale, e adesso tocca vedere che cosa potrebbe succedere nei



prossimi giorni, visto che la Acn ha la possibilità di individuare gli obiettivi sotto attacco mentre il sabotaggio è ancora in corso. Per il Presidente di **Unimpresa** Giovanna Ferrara l'Italia non può permettersi di sottovalutare l'importanza della sicurezza informatica.

“Le istituzioni e le aziende devono considerare la cybersicurezza una priorità strategica, dotandosi degli strumenti necessari per prevenire e mitigare i rischi. Solo così si potrà proteggere il tessuto economico e sociale del Paese da attacchi che, nel prossimo futuro, saranno sempre più frequenti e devastanti”.