

## ATTACCO INFORMATICO ALLA REGIONE: L'HACKER CHICCARELLI, "E' ATTO DI GUERRA, DIFFICILE DIFENDERSI"

27 Febbraio 2025



L'AQUILA – “Le Pubbliche amministrazioni si stanno muovendo sulla cybersicurezza, ma c’è un gap di 15 anni da recuperare. Contro attacchi hacker come quello subito ieri dalla Regione Abruzzo è comunque difficile difendersi”.

Parola di Stefano Chiccarelli, hacker “buono” di professione, pescarese amministratore delegato dell’azienda RJ45LAB, che di mestiere, tra le cose, forza le reti informatiche di imprese ed enti proprio per metterle alla prova e aiutarle così ad alzare le difese informatiche.

Sentito da Abruzzoweb, spiega: “Nel 2023 la Asl dell’Aquila subì un attacco intrusivo ransomware, quindi profondo e mirato a prelevare dati e documenti per poi chiedere un riscatto. Furono sfruttate carenze nella rete. Quanto accaduto ieri, invece, è tutt’altra storia: la Regione ha subito un attacco più facile da realizzare, meno grave per i suoi effetti diretti. Si tratta però di un vero e proprio atto di guerra cybernetica, un bombardamento che invece di essere fatto con proiettili veri viene realizzato con tanti piccoli segnali informatici. Del resto l’Italia è sotto attacco dal gruppo hacker NoName da dieci giorni. Qualcuno dice che siano riconducibili alla Russia, ma in questi casi non lo si può mai dire con certezza. Il vero scopo è la propaganda politica, mettere sotto pressione un Paese”.

Quindi nel dettaglio: “Si chiama attacco DDoSS (Distributed Denial of Service), prevede che migliaia o addirittura milioni di device compromessi – dai pc agli smartphone, fino ai router e a ogni possibile apparecchio collegato ad internet – di ignare persone, all’improvviso inviano tutti insieme richieste a uno specifico sito web, saturando la sua banda e le risorse computazionali dei server”.

In altre parole, quanto accaduto è simile a quanto avviene per esempio in occasione dei “click day” per l’acquisto dei biglietti per il concerto di una star internazionale: troppi utenti entrano nello stesso momento in un sito web, mandandolo in tilt.

Come difendersi? “Purtroppo non si può fare molto. Anche se la Telco (l’operatore che fornisce la banda del sito web)

dovesse prevedere una difesa dagli attacchi DDoSS, questa potrebbe essere comunque aggirabile. Faccio un esempio: magari la misura di sicurezza si aziona bloccando un traffico anomalo di utenti dall'estero e rende inaccessibile il sito, ma per gli hacker basta usare pc presenti in Italia per aggirare il problema e mettere a segno il bombardamento. Se invece la Telco blocca il sito quando c'è traffico eccezionale dall'Italia comunque provoca disagi agli utenti veri".