Primo piano

Gli aerei dopo i freezer e il sangue La strategia ibrida della tensione

L'analisi Azione coordinata, ben organizzata e gestita da un gruppo unico. I sospetti su un'entità statuale
Frequenza e continuità gli elementi per colpire l'opinione pubblica: «Vogliono testare le nostre difese»

Fausto Biloslavo

Due milioni di attacchi cyber in 24 ore, ma il grosso serve a confondere e saturare le difese. Il bersaglio primario è una centrale elettrica o la banca nazionale, che viene paralizzato in poco tempo. Non è fantascienza, ma realtà a Taiwan sotto costante minaccia cyber cinese. L'escalation di attacchi ibridi in Europa arriverà a questo livello? Dai siti governativi hackerati siamo passati ai refrigeratori degli alimentari, alle riserve di sangue francese fino alle mail-bomba sui voli civili. I falsi allarmi, che hanno fatto alzare i caccia o costretto i voli ad atterraggi di emergenza in basi militari, hanno coinvolto 31 aerei solo nei primi 5 giorni di novembre (5mila passeggeri). La media storica è di 2 voli al mese. La frequenza e continuità su bersagli diversi dimostra che l'azione è coordinata, ben organizzata e parte da un gruppo che potrebbe avere alle spalle «un'entità statuale», come teme la nostra intelligence. I russi sono i primi indiziati, ma non si possono escludere operazioni *false flag*, sotto falsa bandiera, per dare la colpa al nemico. L'unica certezza è che siamo di fronte a una strategia della tensione senza armi e morti, per ora, capace di instillare paura oltre a insicurezza nell'opinione pubblica con l'obiettivo di scatenare il caos. «Scenari che stanno progredendo velocemente, ma già tutti previsti nei documenti della Nato sulla minaccia ibrida e la guerra cognitiva - spiega una fonte militare del *Giornale* - Scritto nero su bianco e confermato da quello che sta accadendo con un'accelerazione preoccupante negli ultimi giorni».

Azioni a costi bassi ma con effetti devastanti Nessuna rete civile sembra al sicuro al 100%

Il bersaglio grosso è l'opinione pubblica, ma non l'unico: «Colpiscono la nostra volontà di difesa e vogliono testarla. Con i falsi allarme bomba sugli aerei in mezza Europa mettono alla prova e controllano la reazione ed i tempi dell'Alleanza atlantica». Per le mail bomba il costo è zero ed il testo delirante dei messaggi minacciosi richiama il Muzhskoye gosudarstvo, un gruppo sovranista, maschilista e ultra nazionalista messo fuori legge in Russia. Adesso si fa chiamare Male legion e si concentra sulla guerra in Ucraina. Il 13 luglio le intelligence occidentali, compresa la nostra, hanno lanciato l'allarme su un piano di attacchi cyber dei servizi russi. Si indicava il Centro 16 del Servizio federale per la sicurezza, l'Fsb erede del sovietico Kgb, che aveva nel mirino una lista di bersagli «critici» in Europa. Per l'offensiva cyber l'Fsb avrebbe assoldato gruppi hacker come Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard e Static Tundra. «Non è chiaro se gli autori di questi attacchi siano criminali informatici o soggetti mossi da altre finalità, ma finora non abbiamo riscontrato elementi che indichino una motivazione economica», spiega Rafe Pilling, di Sophos, importante società di sicurezza informatica. «L'immagine dei frigoriferi vuoti nei supermercati - aggiunge - ha un forte impatto psicologico in quanto può far percepire un attacco informatico di portata relativamente limitata come una crisi sociale molto più ampia». Nessuna bomba, ma tanta paura è la strategia dei falsi allarmi sui voli.

La pista più ovvia punta a Mosca e le intelligence europee sono arrivate a una conclusione sugli ultimi attacchi hacker. «Ma non è chiaro se sia un gruppo che agisce in maniera autonoma o eterodiretto da entità statali», spiega un'altra fonte del *Giornale* che segue la crisi. Però osserva che «mezza Europa si sente in guerra con la Russia. Operazioni *false flag* non si possono escludere a priori». Attacchi sotto falsa bandiera per incolpare il nemico, come il sabotaggio ai gasdotti Nord Stream del 2022. Russi o meno per difenderci dalle offensive informatiche dovremmo lanciare attacchi, che non possiamo fare, di tipo preventivo. Nessuna rete «civile» è sicura al 100% e l'escalation rischia di aumentare: «Pensate cosa accadrebbe - spiega una fonte - se gli enti che devono erogare le pensioni venissero hackerati a fine mese lasciando senza soldi gli anziani».



Caos nei cieli Passeggeri guardano un tabellone degli arrivi e delle partenze all'aeroporto di Sofia, in Bulgaria, dove tre voli Ryanair sono stati oggetto di segnalazioni