L’Iran adotta la strategia del caos anche nel cyberspazio

Pubblicato il 16/03/2026

Un report di Maticmind segnala un’intensificazione delle attività cyber legate a Teheran: oltre 600 rivendicazioni in una settimana. Non solo sabotaggio, ma soprattutto pressione psicologica, infiltrazione e spionaggio strategico.

La guerra tra Iran, Israele e Stati Uniti non si combatte soltanto nei cieli del Medio Oriente. Da tempo, infatti, un secondo fronte si è aperto con crescente intensità nel cyberspazio, dove Teheran sembra muoversi secondo una logica precisa: seminare caos, aumentare la pressione sugli avversari e costruire strumenti di coercizione da usare nel tempo.

A fotografare questa escalation è un report di **Maticmind**, società italiana del gruppo Zenita specializzata in sicurezza informatica. Secondo l’analisi, negli ultimi sette giorni si è registrata una crescita significativa dell’attività cybercriminale riconducibile all’Iran: **oltre 600 rivendicazioni di attacco**, con un **picco superiore alle 50 al giorno**, attribuite a **47 diversi attori** e rivolte contro obiettivi sensibili in **11 Paesi**.

Tra i bersagli più colpiti figurano **Israele e Stati Uniti**, seguiti da **Arabia Saudita, Giordania e Kuwait**. Ma il raggio d'azione sembra allargarsi anche oltre il Medio Oriente. Nel mirino sarebbero finiti anche il **Canada**, per via del sostegno politico espresso a Washington e Tel Aviv, e altri Paesi **europei e NATO** con posizioni pubbliche considerate allineate agli interessi occidentali.

L'Iran adotta la strategia del caos anche nel cyberspazio

La logica della Jang-e-Ashub

Alla base di questa offensiva c'è quella che Maticmind definisce **"Jang-e-Ashub"**, ovvero " guerra e caos". Non si tratta, secondo il report, di una strategia pensata per vincere un conflitto con un singolo colpo decisivo, ma piuttosto di una forma di pressione continua, psicologica e negoziale.

Il modello si sviluppa in più fasi. La prima è quella degli attacchi dimostrativi, come i **wiper** contro obiettivi israeliani o sauditi, utili a mostrare la capacità di risposta iraniana senza arrivare a uno scontro militare diretto. A questa segue una fase di amplificazione della minaccia, in cui si alimenta la percezione di un attacco imminente e si cerca di destabilizzare l'avversario.

L'ultimo passaggio è il più delicato: l'infiltrazione silenziosa dei sistemi informatici dei Paesi colpiti per ottenere **accessi persistenti e dormienti**, da attivare al momento opportuno. In questo modo il cyber diventa una leva di pressione indiretta, uno strumento da usare nei momenti di maggiore tensione politica o militare.

Per le organizzazioni europee, osserva Maticmind, il rischio più immediato non sarebbe tanto quello di un blackout improvviso, quanto piuttosto quello di uno **spionaggio prolungato** e dell'esposizione della **supply chain cloud**.

Più spionaggio che distruzione

Dietro il rumore delle rivendicazioni e l'impatto mediatico degli attacchi, l'obiettivo principale sembra essere uno solo: **raccogliere informazioni strategiche**.

Gruppi vicini a Teheran come **APT34, MuddyWater** o **Charming Kitten** sono stati più volte associati a operazioni persistenti all'interno di reti governative, energetiche e militari in vari Paesi del Medio Oriente. In molti casi, questi attori hanno mantenuto l'accesso alle infrastrutture compromesse per mesi, se non anni, con l'obiettivo di sottrarre dati sensibili relativi a capacità militari, negoziati diplomatici e asset tecnologici strategici.

Il tratto distintivo dell'approccio iraniano, sottolinea il report, è proprio questa gradualità: accessi silenziosi, raccolta di informazioni, consolidamento della presenza e costruzione di margini di pressione da spendere quando il contesto lo rende utile.

Più che una super arma capace di produrre effetti spettacolari e immediati, il cyber iraniano appare dunque come uno **strumento di influenza strategica**: meno visibile di un missile, ma potenzialmente altrettanto efficace nel logorare un avversario, minarne la fiducia e aumentare il costo politico del confronto.

L'Iran adotta la strategia del caos anche nel cyberspazio

Un fronte sempre più centrale

In questo scenario, il cyberspazio si conferma sempre più come un terreno di scontro cruciale. Non solo per la possibilità di colpire infrastrutture e sistemi sensibili, ma soprattutto perché consente di esercitare pressione continua senza oltrepassare apertamente la soglia della guerra convenzionale.

È in questa zona grigia, fatta di sabotaggi limitati, infiltrazioni, propaganda e spionaggio, che l'Iran sembra voler giocare una parte decisiva della sua partita regionale e internazionale. Una partita in cui il caos non è un effetto collaterale, ma una strategia deliberata.

Link notizia: https://www.ansa.it/canale_tecnologia/notizie/tecnologia/2026/03/12/iran-maticmind-zenita-group-oltre-600-attacchi-cyber-in-7-giorni_f42bcbce-a8e5-4f9c-8675-42ef956e6b00.html