

Il fronte civile della guerra cibernetica tra Iran e Israele

La Repubblica islamica è rimasta senza benzina mentre a migliaia di residenti di Tel Aviv stati sottratti i dati "Noi cittadini comuni vittime dello scontro" di Farnaz Fassihi e Ronen Bergman

Da qualche tempo in Iran e in Israele milioni di persone comuni si trovano prese di mira dal fuoco incrociato di una guerra cibernetica tra i loro Paesi. A Teheran un dentista ha guidato per ore in cerca di benzina, mettendosi in coda in quattro stazioni di servizio prima di tornare a casa con il serbatoio vuoto. A Tel Aviv un noto giornalista è stato preso dal panico quando i particolari della sua vita intima sono stati caricati sui social insieme a quelli di centinaia di migliaia di altre persone, sottratti da un sito di incontri per Lgbtq. Da anni Israele e Iran sono invischiati in una guerra occulta a tutto campo, per terra, mare, aria e online ma, in genere, finora erano state prese di mira soltanto persone collegate a forze armate e governo. Adesso, invece, la guerra ha iniziato a bersagliare su ampia scala anche i civili.

Nelle ultime settimane, un attacco cibernetico al sistema nazionale iraniano di distribuzione del carburante ha paralizzato le 4.300 stazioni di servizio del Paese e sono occorsi 12 giorni per ripristinare del tutto i rifornimenti. L'attacco è stato attribuito a Israele da due funzionari delle Difesa Usa. A quell'attacco ha fatto seguito, alcuni giorni dopo, una serie di attacchi cibernetici in Israele attribuiti all'Iran contro una struttura sanitaria e un sito di appuntamenti per la comunità Lgbtq. «Forse, c'è un conflitto in corso tra Israele e Iran, ma dalla ristretta prospettiva di noi civi-

li siamo considerati alla stregua di prigionieri, presi in mezzo e indifesi», dice Beni Kvodi, 52 anni, redattore di una radio israeliana.

Entrambi i Paesi sembrano voler colpire i civili per far pervenire messaggi precisi ai rispettivi governi. L'attacco al sistema di distribuzione del carburante in Iran si è verificato il 26 ottobre, in prossimità del secondo anniversario delle proteste antigovernative su larga scala innescate da un brusco aumento del prezzo della benzina. All'epoca il governo reagì con una brutale repressione che secondo Amnesty International provocò la morte di oltre 300 persone. L'attacco cibernetico è sembrato finalizzato a innescare un'altra ondata di disordini antigovernativi. Le stazioni di servizio hanno smesso di funzionare all'improvviso e un messaggio digitale ha invitato i clienti a lamentarsi con la Guida suprema iraniana, l'ayatollah Ali Khamenei, del cui ufficio è stato diffuso il numero di telefono diretto. Gli hacker hanno assunto il controllo delle insegne pubblicitarie di città come Teheran e Isfahan, sostituendo alle réclame la domanda «Khamenei, dov'è la mia benzina?».

Per ripristinare il servizio, il ministero ha dovuto inviare tecnici in tutte le stazioni di rifornimento del Paese. Una volta resettate le pompe, però, la maggior parte delle stazioni di servizio ha potuto vendere soltanto carburante non sovvenzionato, il cui prezzo è doppio rispetto a quello sovvenzionato. Sono occorse due settimane per ripristinare la rete dei sussidi che permette di rifornirsi di 60 litri al mese a metà prezzo. L'attacco potrebbe anche essere stato più grave.

Un manager di spicco del ministero del Petrolio, a conoscenza delle indagini, ha rivelato – chiedendo di restare anonimo – che gli hacker avevano assunto il controllo anche dei serbatoi di stoccaggio del carbu-

rante del ministero e che potrebbero aver avuto accesso a informazioni sulla vendita internazionale di petrolio, segreto di Stato che potrebbe portare alla luce le modalità con le quali l'Iran evade le sanzioni.

Quattro giorni dopo che le pompe di benzina in Iran avevano smesso di funzionare, gli hacker sono riusciti a penetrare nel database di "Atraf", un sito israeliano di appuntamenti, e ad accedere ai file medici del Machon Mor Medical Institute, network di ospedali privati in Israele. I file sottratti in entrambi gli hackeraggi e comprendenti informazioni riservate su circa 1,5 milioni di israeliani, pari al 16% della popolazione del Paese, sono stati postati su un canale dell'app di messaggistica Telegram. Il governo israeliano ha chiesto di oscurare immediatamente il canale, come è avvenuto, ma gli hacker – un piccolo gruppo denominato Black Shadow – ha postato tutto il materiale su un altro canale e ha continuato a farlo ogni volta che le informazioni sottratte e pubblicate erano rimosse. Il gruppo ha postato anche alcuni file sottratti alla compagnia israeliana di assicurazioni Shirbit, hackerata nel dicembre scorso, che copre i dipendenti del ministero israeliano della Difesa.

Né Israele né Iran hanno rivendicato in modo ufficiale gli ultimi attacchi cibernetici, né hanno formulato accuse formali. I funzionari israeliani si sono rifiutati di accusare pubblicamente l'Iran, mentre i funzionari iraniani hanno addebitato l'attacco alle loro stazioni di servi-



zio a un Paese straniero non meglio identificato. «Stiamo vivendo una fase pericolosa», ha detto lunedì in una chat su Clubhouse Maysam Behravesh, ex capo analista per il ministero dell'intelligence iraniano. «Ci sarà una nuova serie di attacchi cibernetici su vasta scala contro le nostre infrastrutture. Siamo a un solo passo da uno scontro militare vero e proprio».

– Traduzione di Anna Bissanti

© 2021 THE NEW YORK TIMES

I numeri

1,5

Gli abitanti

Un attacco iraniano ha sottratto i dati di 1,5 milioni di israeliani: il 16% degli abitanti

12

I giorni

Ci sono voluti 12 giorni per ripristinare i rifornimenti di benzina in Iran dopo un cyberattacco israeliano



Il messaggio degli hacker

Il 26 ottobre hacker israeliani hanno colpito le stazioni di servizio in Iran e sostituito messaggi pubblicitari con: "Khamenei, dov'è la mia benzina?". A lato, Raisi visita una pompa di servizio

DATA STAMPA



ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - 2994