LA NUOVA BUSSOLA QUOTIDIANA
Direttore Riccardo Cascioli
FATTI PER LA VERITÀ

hacker

È in corso la guerra cibernetica, sovranità a rischio

ATTUALITà 07_02_2023

Ruben Razzante

Quanto accaduto domenica non deve terrorizzare ma non va neppure sottovalutato. Il massiccio attacco hacker che ha coinvolto mezzo mondo e che in Italia è stato segnalato dall'Agenzia per la cybersecurity nazionale (Acn) ha mandato in tilt numerosi server e siti

web italiani e di altri Stati, che sono risultati inaccessibili a causa di un ransomware globale. Si tratta di un attacco venuto alla luce nel giorno in cui la rete Tim è andata in down lasciando milioni di utenti senza internet e provocando disservizi anche ai bancomat.

Una massiccia offensiva scatenata dagli hacker in tutto il mondo, la cui portata e le cui conseguenze sono ancora tutte da delineare. Sulla rete Tim era stato rilevato un problema di interconnessione al flusso dati su rete internazionale, che ha generato un impatto anche in Italia. Durante la giornata si sono susseguite segnalazioni degli utenti per i disservizi ad internet e ai bancomat, tanto che sia l'hastag #timdown sia quello sugli sportelli automatici sono andati in tendenza su Twitter.

La gravità della situazione è stata confermata dal vertice convocato ieri a Palazzo Chigi per fare un primo bilancio dei danni provocati e mettere in campo le adeguate contromisure. Proprio nelle scorse settimane, tra l'altro, la premier Giorgia Meloni aveva fatto in Consiglio dei ministri un'informativa sulla necessità di contrastare la vulnerabilità della rete. Dunque le falle in alcuni sistemi informatici erano già note e la necessità di aggiornare i software è stata forse sottovalutata da imprese e pubbliche amministrazioni, alcune delle quali non sanno neppure di essere sotto attacco. Il Computer security incident response team Italia, l'organismo cui spetta il monitoraggio degli incidenti e l'intervento in caso di attacchi, ha scoperto che gli hacker sono entrati in azione attraverso un ransomware già in circolazione che ha compromesso decine di sistemi.

L'attacco ha preso di mira i server VMware ESXi. La vulnerabilità sfruttata dagli hacker è già stata corretta in passato dal produttore ma, come ha evidenziato Acn – l'Agenzia per la cybersicurezza nazionale – «non tutti coloro che usano i sistemi attualmente interessati l'hanno risolta» e i server presi di mira, se privi delle correzioni adeguate, «possono aprire le porte agli hacker impegnati a sfruttarla in queste ore dopo la forte crescita di attacchi registrata nel weekend». I primi ad accorgersi dell'attacco sono stati i francesi, probabilmente per via dell'ampio numero di infezioni registrato sui sistemi di alcuni provider in quel Paese. Successivamente l'ondata di attacchi si è spostata su altri Paesi tra cui l'Italia.

Al momento i server compromessi sono qualche migliaio in tutto il mondo, dalla Francia alla Finlandia, dal Canada agli Stati Uniti fino appunto all'Italia dove, stando a quanto accertato finora, decine di realtà hanno già riscontrato l'attività malevola nei loro confronti. E il numero, dicono gli analisti, è destinato ad aumentare. I settori più colpiti sembrano essere quello bancario e sanitario, che sono tra i più strategici per il

funzionamento dell'economia e la vita degli Stati. Probabilmente c'è una regia ed è in atto una guerra cibernetica dai contorni ancora nebulosi. Non è facile infatti delinearne le finalità e, soprattutto, si fa fatica a individuare una precisa regia di questi attacchi.

Il ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione e minacciando, in caso di mancato versamento del riscatto, la definitiva distruzione dei dati bloccati. C'è chi, come Corrado Giustozzi, esperto di cybersicurezza, ha proposto di stroncare sul nascere ogni minaccia di questo tipo e di introdurre una normativa ad hoc che impedisca alle aziende di pagare riscatti per riavere i dati, proprio come succedeva per i sequestri di persona negli anni settanta. Considerata la transnazionalità della Rete, è ipotizzabile una riforma legislativa del genere? I dubbi sono più che legittimi.

Palazzo Chigi, pur precisando che «nessuna istituzione o azienda primaria che opera in settori critici per la sicurezza nazionale è stata colpita» dall'attacco hacker di domenica scorsa, si esprime in maniera abbastanza critica verso le aziende che non hanno fatto aggiornamenti ai loro software, visto che la falla sfruttata dal ransomware era conosciuta almeno dal febbraio 2021. «L'aggressione informatica era stata individuata da Acn come ipoteticamente possibile fin dal febbraio 2021, e a tal fine l'Agenzia aveva allertato tutti i soggetti sensibili affinché adottassero le necessarie misure di protezione. Taluni dei destinatari dell'avviso hanno tenuto in debita considerazione l'avvertimento, altri no e purtroppo oggi ne pagano le conseguenze», fanno sapere dall'Agenzia.

Ora l'Agenzia per la cybersicurezza nazionale si metterà al lavoro insieme alla polizia postale per capire meglio i soggetti più vulnerabili, ma l'impressione è che si tratta di atti intimidatori, di minacce, forse avvertimenti a qualcuno. Non si può escludere, cioè, che la guerra cibernetica dispieghi tutte le sue potenzialità nel prossimo futuro, diventando il nuovo teatro dello scontro tra superpotenze. Di qui la necessità di procedere con nuovi massicci investimenti in cybersecurity per tentare di blindare l'integrità della rete, sperando che ciò possa bastare e che non sia già troppo tardi.