

CYBER SICUREZZA: MASSICCIO ATTACCO HACKER IN CORSO, COMPROMESSI MIGLIAIA DI SERVER

6 Febbraio 2023



L'AQUILA - E' un attacco massiccio quello scatenato dagli hacker in tutto il mondo, Italia compresa, la cui portata e, soprattutto, le cui conseguenze sono ancora tutte da chiarire.

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. Sia l'azienda sia la polizia postale hanno però escluso che il problema sia dovuto ad un attacco dei pirati informatici.

Ma che si tratti di una cosa seria lo conferma il vertice convocato da palazzo Chigi per fare un primo bilancio dei danni provocati e mettere in campo le adeguate contromisure. All'incontro ci saranno il sottosegretario Alfredo Mantovano, il direttore dell'Agenzia Roberto Baldoni e la direttrice del Dis, il Dipartimento informazioni e sicurezza, Elisabetta Belloni.

Già nelle scorse settimane, tra l'altro, la premier Giorgia Meloni aveva fatto in Cdm un'informativa proprio sulla necessità di contrastare la vulnerabilità dei sistemi informatici.

L'allarme è arrivato nel pomeriggio dall'Agenzia per la cybersicurezza nazionale: 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 già "compromesso" decine di sistemi. Non solo: gli esperti dell'Agenzia guidata da Roberto Baldoni sono riusciti ad allertare diversi soggetti - istituzioni, aziende pubbliche e private - i cui sistemi risultano esposti e dunque vulnerabili agli attacchi ma "rimangono ancora alcuni sistemi esposti, non compromessi, dei quali non è stato possibile risalire al soggetto proprietario".

Significa, in sostanza, che decine di aziende non sanno neanche di essere sotto attacco ma dovrebbero "immediatamente" aggiornare i loro sistemi. "L'attacco - ha detto il ministro delle Imprese e del Made in Italy Adolfo Urso - ci rafforza nella convinzione che sulla rete e in generale sulla cyber sia importante garantire il massimo livello di sicurezza".

Sulla rete di Tim, invece, fin dalle prime ore della mattina era stato rilevato un problema di interconnessione al flusso dati su

rete internazionale, che – ha spiegato l'azienda – ha generato un impatto anche in Italia.

Il problema è stato risolto nell'arco della stessa giornata, durante la quale si sono susseguite segnalazioni degli utenti per i disservizi ad internet e ai bancomat, tanto che sia l'hashtag #timdown sia quello sugli sportelli automatici sono andati in tendenza su Twitter. Tra gli esperti che si occupano di cybersicurezza, però, è anche circolata l'ipotesi che si sia verificato un problema sui router di Sparkle, la società di Tim che gestisce tra l'altro i cavi in fibra ottica, che potrebbe essere collegato all'attacco. Sul punto al momento sarebbero ancora in corso una serie di analisi approfondite.

L'attacco individuato dall'Agenzia ha invece preso di mira i server 'VMware ESXi': gli autori hanno sfruttato una vulnerabilità che era stata già individuata e risolta nel febbraio 2021 da VMware, ma – spiegano gli esperti – non tutti hanno applicato la correzione indicata dall'azienda e dunque sono rimasti col 'buco' senza toppa che è stato sfruttato in questa ondata di attacchi per entrare.

Ed 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. Lo sfruttamento della vulnerabilità, spiega infatti l'Agenzia, "consente in una fase successiva di portare attacchi ransomware che cifrano i sistemi colpiti rendendoli inutilizzabili fino al pagamento di un riscatto per avere la chiave di decifrazione".

Chi sembra lasciarsi alle spalle invece l'attacco hacker subito lo scorso 2 febbraio, sferrato dal gruppo ransomware 'Black Basta', è l'azienda energetica romana di Acea, la quale ha annunciato di aver ripristinato la funzionalità dei propri sistemi informatici. I siti internet del Gruppo e delle piattaforme online per la gestione degli aspetti commerciali delle forniture di acqua, elettricità e gas risultano operativi, così come per i clienti il servizio di contact center delle società del Gruppo, tra cui Acea Ato 2, Areti e Acea Energia.