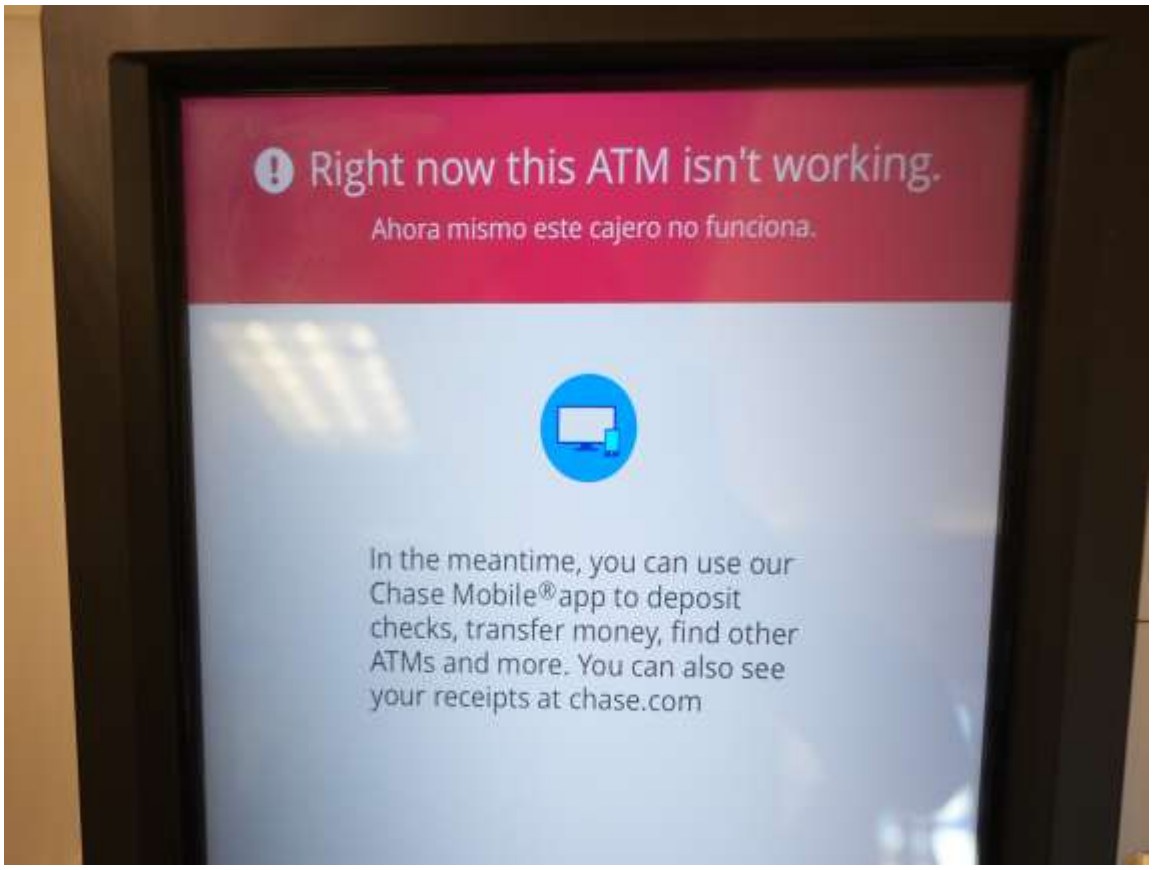
Blackout e cyber attacchi, che cosa sta succedendo? Le paure apocalittiche del «bugmagedddon» e le tre ipotesi di Paolo Ottolina

Da Microsoft alla Nsa, fino ad Apple: una settimana di guasti senza precedenti alimenta i sospetti di attacchi coordinati. La Casa Bianca esclude un'offensiva, mentre Google e Fbi documentano una nuova generazione di hacker che utilizzano agenti AI autonomi
(Fonte: https://www.corriere.it/ 18 novembre 2026)



In meno di una settimana, tra il 12 e il 17 novembre, una raffica di blackout informatici ha colpito gli Stati Uniti e non solo. Prima Microsoft, con Outlook, Teams e altri servizi inutilizzabili per oltre 24 ore. Poi, venerdì 13, il blocco nazionale dei decolli ordinato dalla Federal Aviation Administration, l'ente che gestisce il traffico aereo americano. Lunedì 16 è toccato ai sistemi bancari, JPMorgan Chase in testa (oltre a un problema tecnico che ha fermato per oltre un'ora i voli United Airlines). Martedì 17 sono arrivate le notizie dell'interruzione di una rete riservata della Nsa, l'agenzia di intelligence americana, e del blackout di diversi servizi Apple, tra cui iCloud, App Store e Apple Music.
E prima gli episodi dei frigo hackerati a distanza e del maxi-furto a Binance. In Italia si sono aggiunte le offensive, meno sofisticate ma persino più impattanti in termini di disagi concreti, delle mail minatorie ad aerei e scuole (e le minacce a figure delle istituzioni come Tajani).
Che cosa sta succedendo davvero? Le principali ipotesi sul tappeto - dicono esperti come Kate Klonick, docente di diritto e tecnologia alla St. John's University di New York - sono tre e vanno da uno scenario serio ma confortante, ad altri decisamente più negativi.

L'ipotesi più benigna

L'amministrazione Trump esclude, almeno per ora, un'operazione coordinata. Da Manila, dove accompagna il presidente nel suo viaggio asiatico, il segretario di Stato Marco Rubio ha riconosciuto che la sequenza di disservizi sta rendendo «nervosi e ansiosi» molti americani, promettendo trasparenza. Ma ha anche assicurato: «Non abbiamo alcuna prova, indicazione o ragione per credere che questi incidenti siano collegati tra loro». Nessun elemento, ha aggiunto, permette di attribuirli ad hacker, criminali o potenze straniere. Rubio ha però aperto alla possibilità di un ruolo indiretto dell'intelligenza artificiale: «A volte, quando si interviene per correggere un sistema perché è stata individuata una vulnerabilità, si crea un'interruzione temporanea del suo funzionamento».

Una ricostruzione più dettagliata arriva dal **Washington Sun** ed è stata ripresa anche da Reuters e Axios. Secondo tre fonti a conoscenza di colloqui riservati, dirigenti di Wall Street e funzionari della Nsa avrebbero spiegato ai membri del Congresso che alcune interruzioni sono state provocate proprio dalla corsa a correggere vulnerabilità scoperte con l'AI. «Questi modelli stanno individuando vulnerabilità enormi, aumentando l'urgenza di intervenire», ha raccontato un funzionario parlamentare. Le aziende starebbero distribuendo più aggiornamenti contemporaneamente di quanti i loro sistemi riescano a sopportare.

C'è persino una parola per descrivere il rischio che tutti cercano di scongiurare: «bugmageddon», una sorta di Apocalisse dei bug. Uno scenario in cui gli hacker, grazie all'accelerazione fornita dall'AI, scoprono e sfruttano le falle dei programmi prima che chi li gestisce riesca a correggerle.

Il direttore dell'intelligence nazionale Jay Clayton ha collegato il guasto della Nsa ad aggiornamenti per una vulnerabilità del linguaggio Php scoperta con l'AI (anche il down di iCloud di Apple è stato attribuito a un aggiornamento). Il segretario alla Sicurezza interna Markwayne Mullin ha offerto una spiegazione più generale: «Stanno sovrapponendo nuove tecnologie a sistemi informatici davvero vecchi, e questo sembra sovraccaricarli».

A complicare le cose potrebbe esserci anche il cosiddetto *vibe coding,* ovvero codice prodotto rapidamente con l'AI, a volte senza le necessarie competenze o la dovuta supervisione. E per di più inserito in infrastrutture costruite decenni fa, in un mondo del lavoro in cui licenziamenti e pensionamenti hanno ridotto il numero di ingegneri che conoscono davvero quei sistemi. Una combinazione potenzialmente pericolosa, anche se non è dimostrato che il codice generato dall'AI abbia causato i blackout. Microsoft, per esempio, ha ricondotto il proprio guasto a un difetto software introdotto mesi fa, aggravato dal sovraccarico dei server.

L'ipotesi degli hacker di Stato

Una seconda spiegazione, più inquietante, è che dietro i blackout ci siano potenze straniere impegnate in operazioni di sabotaggio. Le prove di un disegno comune non esistono, ma alcuni attacchi sono già stati attribuiti da fonti ufficiali a Stati nemici.

Il 9 novembre, il ministro degli Esteri francese Jean-Noël Barrot ha attribuito ai Guardiani della

Rivoluzione iraniani gli attacchi ai frigoriferi e congelatori di circa 700 supermercati francesi avvenuti in ottobre (episodi analoghi si sono ripetuti più di recente in diversi Paesi europei, **Italia inclusa**).
C'è poi la Corea del Nord, alla quale l'Fbi attribuisce **il colossale furto di criptovalute ai danni di Binance del 29 ottobre**: oltre 6 miliardi di dollari, la più grande sottrazione di criptovalute mai registrata. Il gruppo responsabile viene identificato con il nome TraderTraitor.

Gli sciami di hacker guidati dall'AI

La terza ipotesi, forse la più inquietante, riguarda attacchi condotti da sciami di agenti AI autonomi. Programmi capaci di collaborare, esplorare reti informatiche, individuare vulnerabilità e attaccarle con un intervento umano minimo. Sappiamo che alcuni episodi, di limitata portata concreta ma dalla grande eco mediatica, **sono avvenuti quest'estate**.
Pochi giorni fa, però, l'Fbi ha pubblicato un'allerta su Artex, piattaforma nata per verificare la sicurezza dei sistemi informatici e successivamente sfruttata dai criminali. Può coordinare diversi agenti AI e automatizzare buona parte di un'intrusione. In alcuni casi, secondo l'Fbi, il passaggio dall'individuazione del bersaglio all'accesso a sistemi privilegiati richiede meno di tre ore. Artex è stata utilizzata, ad esempio, in un attacco contro ConnectWise Cloud Backup, un servizio che permette alle aziende di salvare copie di sicurezza dei propri dati; sfruttando questa violazione, gli hacker hanno tentato di accedere ai sistemi Microsoft 365 di oltre 2.250 aziende che utilizzavano il servizio.
Due giorni fa, un **rapporto del Google Threat Intelligence Group** ha documentato un'evoluzione ulteriore: «Gli hacker ora usano i grandi modelli linguistici per analizzare continuamente gli aggiornamenti software, individuare le vulnerabilità appena corrette e costruire attacchi prima che le aziende possano applicare la correzione, il tutto senza intervento umano», scrivono con grande chiarezza gli esperti dell'azienda di Mountain View. Secondo Google, strumenti del genere stanno riducendo drasticamente il tempo a disposizione delle aziende per proteggersi.

La profezia dell'Apocalisse digitale

Al di fuori di queste tre ipotesi, tutte portatrici almeno di un pezzetto di verità, vi è un livello più estremo: quello delle teorie del complotto vere e proprie, alimentate sui social dalla successione apparentemente infinita e poco spiegabile dei guasti.
Marjorie Taylor Greene, ex deputata repubblicana, già fedelissima di Trump e nota per aver sostenuto numerose teorie complottiste, ha twittato: «*Sembra l'inizio del Covid. Stessa atmosfera*».
Non è una posizione isolata, anzi.
Secondo una voce diffusasi su X, TikTok e negli ambienti del dark web, proprio ieri, il 17 novembre, sarebbe dovuto cominciare un attacco informatico mondiale: conti correnti azzerati, banche paralizzate e Internet spento per tre mesi, il mondo gettato nel caos mentre una superintelligenza artificiale si sarebbe messa al lavoro per riparare le vulnerabilità della rete.

Sono circolati persino video manipolati nei quali Donald Trump sembrava annunciare un blackout nazionale di 90 giorni. I *fact-checker* di PolitiFact hanno rintracciato il filmato originale, registrato il 9 novembre: il presidente non aveva detto nulla del genere.

Ma la teoria, come spesso accade ai complottismi, mescolava fantasie ed elementi autentici. Il primo era il test nazionale del sistema americano di allerta d'emergenza, programmato dalla Fema proprio per il 17 novembre, che prevedeva l'interruzione temporanea delle trasmissioni radio e tv per diffondere un messaggio di prova. Il secondo era Fortress America, un programma annunciato dal Pentagono il 30 settembre per rendere le principali basi militari capaci di funzionare autonomamente, anche per 90 giorni, in caso di blackout elettrico (piani simili sono stati disposti da moltissimi governi e istituzioni, Unione europea inclusa).

Il 17 novembre è passato e l'apocalisse non è cominciata. Ma le previsioni sull'imminente fine del mondo non sono destinate a sparire.