Usa, agenzia della sicurezza in tilt Attacco ad Apple e 178 aziende

Il canale di comunicazione riservato dell'Nsa è rimasto bloccato a lungo Disservizi per la big tech della «mela» Allerta Fbi: gli hacker sfruttano l'IA

L'EMERGENZA

Un allarme dopo l'altro. «Una rete di comunicazioni altamente classificata per la sicurezza nazionale degli Stati Uniti è andata in tilt». Quando in Italia è il tardo pomeriggio, la Cnn rilancia, come esclusiva, questa notizia che interessa l'Nsa (National Security Agency), l'agenzia che si occupa di sicurezza informatica. L'attenzione non può che essere altissima visto che questo nuovo disservizio - definiamolo così per ora - arriva il giorno dopo il malfunzionamento di numerose app bancarie americane, mentre in precedenza c'era stato il clamoroso blackout del sistema del controllo del traffico aereo che per quattro ore aveva impedito ogni decollo e atterraggio. Ma andando più indietro, c'era stato il lungo stop dei servizi Microsoft il cui picco era durato oltre venti ore, ma che aveva lasciato strascichi per almeno 32 mettendo a repentaglio l'utilizzo delle mail (ma non solo).

INCERTEZZA

E ieri, oltre all'allarme lanciato da alcune fonti sulla rete di comunicazione della sicurezza nazionale e rivelato dalla Cnn, ci sono state segnalazioni di problemi a un altro colosso privato: Apple. Ha scritto il New York Post: «Gli utenti Apple sono stati colpiti da diffuse interruzioni di servizio, con migliaia di segnalazioni di malfunzionamenti riguardanti l'App Store, iCloud e l'assistenza Apple che hanno inondato il sito di monitoraggio Downdetector. Poco dopo mezzogiorno (ora della costa orientale degli Stati Uniti), le segnalazioni sono aumentate vertiginosamente, con utenti che lamentavano il blocco dei propri account Apple, l'impossibilità di attivare nuovi dispositivi ed errori durante il tentativo di accedere ai servizi cloud». Non solo: alcuni media specializzati rivelano che quasi 200 siti sono stati minacciati da attacchi informatici. Nell'elenco compaiono non solo soggetti americani, ma anche europei. Ad esempio Cnn, Bbc, Ikea, Air France e Zoom. L'obiettivo era rubare dati finanziari, criptovalute, ma anche compromettere dispositivi Apple.

Secondo l'esperto Scott Helme, ricercatore di sicurezza informatica, «del codice JavaScript dannoso è stato inviato ai visitatori di 178 organizzazioni tramite la piattaforma di sperimentazione web Optimizely. L'elenco comprende alcuni dei siti più visitati al mondo». Optimizely (importante piattaforma cloud) ha diffuso un comunicato in cui spiega «di aver identificato e contenuto un incidente di sicurezza che ha interessato alcuni clienti di Optimizely Web Experimentation». Ultimo tassello: l'Fbi ieri ha emesso un'allerta sicurezza. Ha scritto: «I criminali informatici e gli hacker

allineati a Stati stranieri stanno sfruttando Artex, un framework di test di penetrazione alimentato da superintelligenza, per automatizzare attacchi contro aziende e organizzazioni in tutto il mondo. Artex può accelerare le intrusioni dal targeting iniziale all'accesso privilegiato in meno di tre ore. È stato utilizzato nel compromesso della catena di approvvigionamento ConnectWise di ottobre, che ha esposto ambienti client Microsoft 365 e ha coinvolto tentativi di autenticazione contro più di 2.250 tenant downstream». Tradotto: gli hacker stanno usando l'intelligenza artificiale per nuovi e più efficaci attacchi.
Cosa sta succedendo negli Stati Uniti? Tra disservizi collegati a infrastrutture vetuste come quella del controllo del traffico aereo, reti informatiche fragili e attacchi hacker intensificati, gli ultimi mesi sono stati caratterizzati da una serie di emergenze. E resta sempre il dubbio di fondo: davvero ciò che viene catalogato come incidente non nasconde invece un'offensiva informatica magari di gruppi legati a potenze straniere? D'altra parte, è lo stesso problema con cui conviviamo in Europa tra attacchi a siti web pubblici e privati, falsi allarmi bomba per aerei e scuole, sabotaggi informatici ai frigoriferi dei supermercati come avvenuto in Francia, ma anche in Sicilia. Ma torniamo alla ricostruzione di ciò che è trapelato sui disservizi della rete di comunicazione dell'Nsa. Se fossero l'effetto di un attacco informatico, sarebbe uno scenario particolarmente grave alla luce del ruolo svolto dall'agenzia che deve proprio garantire la cybersicurezza.

CONTROLLORI

La Cnn racconta: «Stando a quanto riferito da sei persone a conoscenza dei fatti, la rete altamente riservata utilizzata dalla National Security Agency per le sue comunicazioni interne è fuori servizio.
La rete, denominata NsaNet, consente ai dipendenti di comunicare internamente informazioni classificate. Al momento non vi sono prove di un attacco informatico. Mentre l'agenzia s'impegna a comprendere la portata del problema, ha predisposto arrivi scaglionati per il personale». Lauren Bis, portavoce della Casa Bianca, ha commentato: «Non abbiamo riscontrato alcuna prova che si sia trattato di un attacco informatico. Non c'è alcuna crisi di cui gli americani debbano preoccuparsi».
Successivamente il Wall Street Journal ha scritto che l'interruzione delle comunicazioni dell'Nsa è stata causata da «un aggiornamento del software»: non è rassicurante.
Mauro Evangelisti