Nelle mani dei mega hacker

Una schermata di Ticketmaster, la società americana che vende biglietti online, appartenente a Live Nation Entertainment. Da qui sono stati sottratti i dati di milioni di clienti.

di Stefano Piazza e Luciano Tirinnanzi

Milioni di clienti di una società che vende online sono stati depredati dei loro dati con tecniche cinesi di cyber spionaggio. Non rimane che difendersi.

Lo scorso maggio Ticketmaster, una delle maggiori società di vendita e distribuzione di biglietti al mondo, è stata vittima di un gigantesco attacco informatico. La violazione ha esposto le informazioni sensibili di milioni di clienti, compresi i dettagli dei pagamenti e i loro dati personali. L'hackeraggio è stato collegato al famigerato gruppo di criminali informatici ShinyHunters, che vanta una lunga storia di violazioni di dati e attacchi ransomware (cioè con richieste di riscatto) di alto profilo. Un singolo attacco informatico, dunque, è stato in grado di mettere a rischio la sicurezza informatica di oltre 500 milioni di utenti ma, soprattutto, li ha esposti a future frodi.

Gli hacker di Ticketmaster hanno ottenuto l'accesso alla rete aziendale sfruttando le poche ma esistenti vulnerabilità nel portale del servizio clienti. Una volta all'interno, hanno esfiltrato enormi quantità di dati e cronologie di acquisto. Dopodiché le informazioni rubate hanno iniziato a essere messe in vendita sui forum del dark web a poche ore dall'attacco.

Anche se questo episodio è già gravissimo di per sé, la vera notizia è che simili incidenti non rappresentano semplici violazioni dei dati personali, ma sono al contrario attacchi diretti alla sicurezza nazionale che coinvolgono governi ostili all'Occidente. Vale per l'America come per l'Europa, le cui infrastrutture digitali si dimostrano sempre più fragili di fronte a gruppi di cyber criminali (quando non direttamente cyber soldati) che sfruttano le nostre debolezze per sottrarre informazioni riservate e puntano a destabilizzare le nostre società attraverso violazioni di infrastrutture critiche, testando periodicamente i nostri livelli di difesa. Oggi è il segreto bancario, domani cosa sarà?

ShinyHunters vanta una rete di hacking internazionale, composta anche da europei come Sébastien Raoult, un programmatore francese sospettato di appartenere al gruppo e per questo arrestato in Marocco e poi estradato negli Stati Uniti (rischia dai 20 ai 116 anni di carcere). Ma l'intelligence americana ritiene che dietro si celino in realtà gruppi legati a doppio filo a figure come il Segretario della Commissione centrale per gli Affari politici e legali della Repubblica popolare cinese, Chen Wenqing, che è stato a lungo al vertice del ministero della Sicurezza di Pechino. Due mesi prima dell'attacco a Ticketmaster, infatti, sette hacker - membri del gruppo APT31, di cui è dimostrato il collegamento al governo cinese - sono stati sorpresi in flagranza di reato durante intrusioni informatiche contro individui critici nei confronti di aziende e politici cinesi.

Gli attacchi seguivano le stesse modalità di hacking di ShinyHunters, anche se avevano lo scopo di minacciare gli oppositori al regime intaccandone la credibilità sia in ambito commerciale che politico. Gli hacker avrebbero utilizzato tecniche avanzate di cyber spionaggio per accedere illegalmente ai sistemi informatici delle vittime,

Sotto, pagina dark web degli ShinyHunters. L'intelligence americana ritiene che dietro si celi una figura come Chen Wenqing (*a destra*), a lungo al vertice del ministero della Sicurezza di Pechino.

GETTY IMAGES, SHUTTERSTOCK (2)

modificando dati personali e informazioni riservate ma lasciando le loro «impronte digitali», ragione per cui sono stati colti sul fatto. Questo genere di operazioni, però, non si fermano. E il motivo è che sono parte di una più ampia strategia di sorveglianza e controllo da parte del governo cinese, volta a proteggere i propri interessi geopolitici e commerciali su scala globale, anche solo testando l'affidabilità di sistemi di protezione privati.

Come difendersi allora? In Occidente si segue la via delle tecnologie d'identità digitale quali i Decentralized identifiers (Did) che, grazie all'uso di blockchain decentralizzate, permettono agli individui di gestire autonomamente l'accesso alle proprie informazioni personali senza doverle condividere direttamente con terze parti in ogni transazione online. Questo approccio ridurrebbe il rischio di attacchi informatici, poiché i dati non vengono memorizzati su server esterni. Integrando queste tecnologie anche nel settore pubblico si ritiene possibile rendere più complesso per i criminali penetrare i nostri device e rubare i dati. Questo è particolarmente importante per settori come la finanza, la sanità e i servizi pubblici essenziali, che sono tra i principali obiettivi degli attacchi informatici. L'Unione europea ha già lanciato quattro progetti pilota su larga scala per garantire nuove forme di identità digitale, tra cui il portafoglio digitale dell'identità Ue. Una vera sfida.

Secondo la Commissione, «questi progetti coinvolgono circa 360 entità, tra cui aziende private e autorità pubbliche di 26 Stati membri, oltre a Norvegia, Islanda e Ucraina».

Allo stesso tempo, Regno Unito, Canada e Australia hanno avviato programmi per incentivare l'adozione di strumenti di identità digitale rispettosi della privacy e al tempo stesso difficili da frodare. Gli Stati Uniti, invece, stanno rimanendo indietro: il più recente piano di implementazione della strategia nazionale per la cybersecurity dell'amministrazione Biden-Harris arranca, con il Consumer Financial Protection Bureau che ha presentato una proposta regolatoria a giugno, ancora non decollata.

Attualmente, però, almeno cinque milioni di americani stanno testando la patente di guida digitale, disponibile in 11 Stati e in fase di sperimentazione in altri 12. Queste patenti digitali potrebbero presto essere utilizzate anche per superare i controlli di sicurezza negli aeroporti, ma rappresentano solo un primo passo verso un sistema avanzato e a prova di hacker. Il National Cybersecurity Center of Excellence (NCCoE) ha lanciato l'anno scorso l'allarme: «Accelerare l'adozione delle identità digitali su dispositivi mobili». Il progetto sembra essere pronto a decollare grazie alla collaborazione di quindici organizzazioni pubbliche e private.

Questi sforzi promettono di migliorare la privacy e il controllo dei dati personali, offrendo al contempo trasparenza e conformità alle normative. Tuttavia, la risposta tradizionale alle violazioni dei dati è spesso inefficace, limitandosi a misure temporanee che non affrontano le vulnerabilità digitali immanenti legate alla condivisione e verifica delle informazioni personali online. Una soluzione in campo sembra essere l'hacking etico, ovvero una pratica che sta cambiando il paradigma e l'approccio in campo tecnologico: l'hacking etico nasce infatti allo scopo di individuare le vulnerabilità che caratterizzano il sistema informatico di un ente o di un'azienda. Dunque, non rappresenta la minaccia ma un sistema di difesa che scova le falle informatiche di un sistema a fin di bene e suggerisce come ripararle, innalzando il livello di difesa. Basterà? ■