24 agosto 2022 7:50

## MONDO: Bastano 6 secondi per sottrarre una carta di credito

I ricercatori *"stimano che una carta di pagamento media possa essere violata in soli sei secondi*": parola di NordVPN, il cui studio su 4 milioni di carte di pagamento trovate sul dark web giunge a descrivere l'estrema fragilità di sistemi che cedono troppo facilmente ad attacchi di tipo "brute force".
Il termine "forza bruta" è infatti ideale e significativo per descrivere questo tipo di offensive: non attacchi in punta di fioretto, indovinando codici e password con stratagemmi e inganni, ma vere e proprie prove di forza computazionale tentando milioni di combinazioni in pochi secondi tentando di trovare la soluzione giusta. Spiega Marijus Briedis, Chief Technology Officer di NordVPN:
*L'unico modo in cui un numero così elevato di carte di pagamento potrebbe apparire sul dark web è attraverso un attacco di tipo brute force. Ciò significa che, in pratica, i criminali cercano di indovinare il numero e il CVV della carta. Le prime 6-8 cifre rappresentano il numero ID dell'emittente della carta. Di conseguenza, agli hacker non rimane che indovinare 7-9 numeri, perché la sedicesima cifra è un checksum ed è utilizzata esclusivamente per determinare se sono stati commessi errori in fase di inserimento del numero. Utilizzando un computer, un attacco di questo tipo può richiedere solo sei secondi.*

"Trial-and-error", insomma, fin quando il server dei malintenzionati non ha trovato la combinazione giusta. Tutto quel che occorre è "forza bruta", dunque ingenti investimenti per l'offensiva ed in relativi guadagni attraverso il malaffare:
*Per indovinare le nove cifre necessarie per ottenere un numero di carta completo, un computer deve passare in rassegna 1 miliardo di combinazioni. E ci vorrà soltanto un minuto per un normale computer, che può provare circa 25 miliardi di combinazioni all'ora. Tuttavia, a seconda dell'emittente della carta, un criminale potrebbe aver bisogno di sole sette cifre per indovinare correttamente.*

Ma cosa si può fare contro attacchi di questo tipo? Poco o nulla: il problema in questo caso non è in password sciagurate o in click disattenti, ma in una fragilità di sistema che va semplicemente controllata e gestita.
*Rivedere il proprio estratto conto mensile per individuare eventuali attività sospette e rispondere in modo rapido e serio a qualunque notifica inviata dalla propria banca in cui si comunica che la propria carta potrebbe essere stata utilizzata senza autorizzazione. Un altro consiglio è avere un conto in banca separato per scopi diversi e mantenere solo piccole somme di denaro in quello a cui sono collegate le carte di pagamento. Alcune banche offrono anche carte virtuali provvisorie che è possibile utilizzare qualora non ci si senta al sicuro durante gli acquisti online.*

La miglior misura di protezione è quella predisposta dai maggiori circuiti, i quali valutano e limitano i tentativi per ovviare proprio ad attacchi di forza bruta:
*Mastercard, ad esempio, ha un sistema di autenticazione centralizzato. Pertanto, un criminale può provare solo circa 10 volte con un numero prima che il sistema centralizzato di Mastercard lo rilevi. Con il sistema di sicurezza di Visa, un criminale può provare 30 o 40 volte, forse anche di più. E se sceglie il momento giusto della giornata, quando c'è molto da fare, può provare molte più volte, perché il sistema è di tipo federato decentralizzato.*

*(Giacomo Dotta su Punto-informatico.it del 23708/2022)*