Il vero tesoro delle truffe online che rubano le carte di credito? I dati delle vittime, usati per creare identità sintetiche *di Velia Alvich*

Lo studio condotto dalla società di threat intelligence Recorded Future per Mastercard: l'82% delle carte sottratte danno accesso alle informazioni personali di chi viene colpito dagli scam (Fonte: https://www.corriere.it/ 30 aprile 2026)

Sono sempre meno le carte di credito che vengono rubate dai cybercriminali. Quello fotografato in un report di **Recorded Future** e presentato da **Mastercard** è un trend di decrescita che potrebbe far pensare a una notizia positiva, ma che al suo interno nasconde delle insidie. Nel 2025 sono state rubate (e rivendute sul **dark web o su Telegram**) "solo" 142 milioni di carte, il **19% in meno** rispetto all'anno precedente, quando sono stati registrati circa 176 milioni di furti. Degli incidenti registrati nell'anno scorso, 1,4 milioni di carte di pagamento appartengono agli italiani. Ma dietro la rassicurante percentuale (globale) che diminuisce si nasconde un nuovo obiettivo dei criminali informatici: quello di ottenere quanti più dati personali delle vittime in un colpo solo. A crescere, infatti, è stata un'altra cifra: il numero di informazioni sottratte insieme alle carte. L'82% delle volte, infatti, le carte portano con sé dati fondamentali che possono diventare un "abilitatori" per nuove truffe. «Il vero dato è che a quelle carte corrispondono nomi, cognomi, indirizzi email e numeri di telefono: per fare truffe complesse bisogna avere delle **identità altrettanto complesse** e strutturate da mettere in gioco per superare i sistemi di controllo tradizionali», così Lorenzo Giudici, responsabile di Business Development Security Solutions di Mastercard, spiega le ragioni dietro l'evoluzione del trend nelle truffe.

In questo contesto, salta ancora di più all'occhio un genere di truffa che si è diffusa già da anni e che ora sta tornando in auge (con nuovi obiettivi): si tratta dell'**e-skimming**, un sistema per rubare i dati di una carta quando si fanno i pagamenti online — che in passato era comune anche quando si facevano operazioni di prelievo agli Atm o si pagava usando un Pos "infetto" — usando un pezzo di codice informatico, cioè uno script che compromette la catena dei servizi online. In casi come questo, quando si è in fase di checkout (che spesso è affidato a terze parti) il malware **estrapola le informazioni fondamentali** della vittima senza che questa se ne renda conto, magari lasciando che il pagamento vada a buon fine. Perché la vera miniera d'oro si trova nei dati.

In uno scenario in cui il crimine informatico è sempre più industrializzato e i dati personali degli utenti sempre più preziosi, il settore dei pagamenti digitali rappresenta contemporaneamente uno dei bersagli più esposti e uno dei laboratori più avanzati di innovazione nella sicurezza. È proprio qui che attaccanti e difensori nel settore dei pagamenti digitali lottano per sfruttare gli avanzamenti tecnologici a proprio vantaggio. Come, per esempio, **l'intelligenza artificiale**, che viene usata dai cybercriminali per due scopi.

Innanzitutto per verificare in massa — spesso con servizi offerti su Telegram — se le carte rubate sono ancora attive, prima ancora di usarle per truffe più grandi. In secondo luogo, per combinare dati reali (rubati con le tecniche già menzionate) e dati fittizi per creare delle identità sintetiche perfettamente credibili da usare per interazioni fraudolente (e quindi per far cadere altre vittime in altri tipi di scam). Non a caso, nel 2025 le **frodi legate alle identità sintetiche sono cresciute del +300%**. Un trend, insomma, che richiede ancora più attenzioni da parte di chi difende il consumatore. «In questo scenario, assistiamo a uno slittamento nell'approccio alla strategia di difesa: la sicurezza non può restare reattiva, servono framework predittivi solidi al passo con l'avanzamento del crimine informatico», ha dichiarato Luca Corti, Country Manager Italia di Mastercard. «Siamo in prima linea nello sviluppo di **sistemi di threat intelligence avanzata basata sull'AI**, con l'obiettivo di intervenire prima che le frodi si verifichino e rafforzare la fiducia nel digitale».