Skimming: invece dei bancomat presi di mira dai criminali anche negozi e benzinai

Data: 2 settembre 2013 | Autore: Redazione

FIRENZE, 09 FEBBRAIO 2013- Il termine “skimming” deriva dal verbo inglese to skim, che vuol dire “sfiorare, strisciare”. Da questa parola discende la parola skimmer che è il congegno elettronico utilizzato per memorizzare i contenuti delle bande magnetiche delle carte di pagamento.

Negli sportelli automatici ATM (Automated Teller Machine), meglio noti come sportelli bancomat sono i dispositivi usati per leggere le relative carte elettroniche di pagamento e, quindi, abilitare l’utente alle operazioni richieste dopo aver effettuato l’ulteriore verifica del PIN (Personal Identification Number) che, pur presente in modalità cifrata all’interno della banda magnetica della carta, viene digitato direttamente dall’utente dopo aver inserito la Card nello Skimmer.

L’uso improprio di questi dispositivi, la loro manomissione, fino ad arrivare addirittura alla sostituzione dello skimmer originale con uno appositamente installato per leggere e registrare i contenuti delle carte magnetiche che vengono fatte “strisciare” al suo interno, ha determinato lo sviluppo di una nuova tecnica criminale chiamata, come detto, skimming, termine poi utilizzato anche per descrivere in generale le truffe compiute ai danni di possessori di carte di credito, bancomat, carte prepagate etc. attraverso un utilizzo illecito di dispositivi di lettura delle stesse (skimmer e P.O.S.).

Si tratta di un fenomeno organizzato, sia in termini tecnici che logistici. Ad essere coinvolti sono bande di criminali che si muovono in tutta Europa, non solo rumeni e bulgari, anche se questi pare siano i più avanzati e strutturati.

Prima ad essere colpiti erano bancomat, terminali per il pagamento con carta di credito posti in ogni luogo possibile, dai supermercati ai distributori di biglietti nelle stazioni.
Ma ora nuovi i criminali hanno scoperto un nuovo trucco per copiare i dati delle carte. La tendenza inversa riguarda gli apparecchi per i pagamenti nelle stazioni di servizio, i terminali nelle stazioni e quelli nel commercio al dettaglio.

L'anno scorso, anche i sistemi di apertura di porte delle banche sono stati manomessi dagli hacker ma alcune delle banche hanno già reagito e tolto i sistemi di apertura automatica con carta. Ma appena si trova una soluzione, i criminali scoprono un nuovo trucco per copiare i dati delle carte. Nel 2012, infatti, sono aumentati molto i casi di skimming presso le stazioni di servizio.Anche i terminali nel mercato al dettaglio sono stati maggiormente manipolati. Ma il dato più preoccupante è che nei negozi, i criminali non manipolano però i terminali quando fanno gli acquisti. I criminali rimangono nei negozi di notte eludendo i controlli. Così si prendono tutto il tempo per modificare i terminali delle casse. Dopo pochi giorni, i ladri tornano nel negozio e smontano le loro apparecchiature portandosi via migliaia di dati di clienti del rispettivo negozio.

Per Giovanni D'Agata, fondatore dello "Sportello dei Diritti" l'ultima difesa per i malcapitati truffati nel caso in cui venga scoperto il responsabile - essendo lo skimming un'attività idonea ad integrare gli estremi della figura di reato prevista dall'art. 12 del D.L. 143/91, convertito nella Legge 197/91 - è quella di perseguirlo in sede penale costituendosi parte civile nel relativo giudizio sperando di poter essere risarciti in quella sede.[MORE]

(notizia segnalata da giovanni d'agata)