ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4600 di Mercoledì 11 dicembre 2019

Il furto dei dati di carte di credito alle macchine automatiche

Individuati dei dispositivi, chiamati skimmer, che permettono di catturare i dati delle carte di credito dei correntisti ed effettuare prelevamenti a loro insaputa. Per fortuna, si sta facendo qualche passo avanti in un settore specifico.

Gli skimmer, come quello visibile in fotografia, sono oggi una realtà del mondo della criminalità organizzata o meno. Possono essere installati con relativa facilità, ma le difficoltà sono maggiori o minori, seconda del tipo di macchina sulla quale lo skimmer viene installato.

Un dispositivo che può essere facilmente violato è il distributore di carburante. Questo distributore è dotato di terminali che possono essere aperti con chiavi universali ed è quindi più facilmente attaccabile, rispetto ad un bancomat bancario, che per solito è dotato di significative protezioni aggiuntive.

È bene precisare che in Italia spesso le macchine che controllano l'erogazione di carburante sono di buon livello, ma la situazione è ancora a macchia di leopardo.

Questo è il motivo per cui gli scienziati dell'Università di California hanno sviluppato un'applicazione per smartphone, che può rapidamente identificare la presenza di uno skimmer installato su un distributore di carburante, riducendo il tempo di ispezione da 30 minuti a pochi secondi. Come accennato, gli skimmer oggi sono installabile su un gran numero di dispositivi, ma l'esperienza mostra come i distributori di carburante, specie di tipo antiquato, possono essere facilmente violati da malviventi dotati di una certa preparazione.

Utilizzando un collegamento wireless, i malviventi, che si parcheggiano nella vicinanza della stazione di servizio ed erogazione carburante, possono catturare, tramite un collegamento Wi-Fiv, sia i codici delle carte, sia i PIN, e possono quindi facilmente creare un duplicato di queste carte.

La app sviluppata dai ricercatori, chiamata Bluetana, non solo analizza i segnali bluetooth che sono presenti nell'area occupata dalla stazione di distribuzione carburante, ma può anche distinguere i segnali provenienti da apparecchiature legittime, rispetto ad altri di natura fraudolenta. Al proposito, è bene tener presente che in una normale stazione di servizio possono essere presenti numerosi segnali Wi-Fi provenienti ad esempio da sistemi antintrusione, da dispositivi di tracciamento dei veicoli e via dicendo. I ricercatori non hanno voluto diffondere i dettagli sul funzionamento di questo applicativo, perché temono che questi dettagli possono essere sfruttati dai malviventi per migliorare ulteriormente le loro capacità.

Da quel poco che si è saputo, l'algoritmo prende in considerazioni elementi oggettivi, come l'intensità del segnale ed altri elementi caratteristici della radiazione Wi-Fi, che possono essere indicatori di una situazione anomala.

Durante una prima campagna di applicazione sperimentale, sono stati individuati ben 42 skimmer installati in tre diversi Stati americani. Due di questi sembra che abbiano funzionato ininterrottamente per più di sei mesi, prima di essere individuati.

Ad oggi, questo applicativo è disponibile solo per gli ispettori, che le compagnie petrolifere mandano a controllare il livello di sicurezza delle stazioni; l'applicativo quindi non è disponibile per il pubblico in generale. Terremo sotto controllo la situazione per vedere se si potranno in futuro avere delle evoluzioni positive.

Adalberto Biasiotti