Scritto da Administrator
Martedì 26 Luglio 2016 16:57


Foto: www.agi.it

Quarantanove anni fa, se avevi bisogno di contanti dovevi recarti in banca e richiederli alle casse. Dal 27 giugno del 1967 tutto è cambiato: in quel giorno i londinesi per la prima volta hanno potuto prelevare soldi dal proprio conto corrente attraverso un nuovo sportello automatico, che in seguito è stato conosciuto come bancomat, o ATM in breve. Da allora questa tecnologia ha conquistato il mondo arrivando a quasi tre milioni di macchine in tutto il globo, con una crescita di circa
280
nuove installazioni ogni giorno.

Oltre a garantire un'indubbia convenienza agli utenti, gli ATM hanno anche attirato l'attenzione dei criminali .

{loadposition user7}

Lo spazio per migliaia di banconote presente in ogni macchina permette un potenziale guadagno così elevato da indurre alcuni criminali ad appropriarsi del contenuto anche con la forza bruta, sradicando letteralmente le macchine dai muri o rimuovendole interamente dal loro alloggiamento.

Altri malviventi scelgono metodi più sofisticati, come la costruzione di parti contraffatte della macchina, davvero difficili da notare, i cosiddetti ***skimmer***. Tra questi, come indicato anche dall'FBI, troviamo: falsi pannelli, schermi, tastierini per il PIN, lettori delle carte e videocamere nascoste nonché tutte le combinazioni possibili di questi apparecchi.

Se i criminali riescono nei loro intenti possono usare i dati ottenuti per impersonare le loro vittime, svuotarne i conti o venderne le informazioni ad altri malintenzionati online. Quest'ultima opzione, però, non è più così remunerativa visto che il pagamento per i dati di una carta di credito sono crollati passando da centinaia di dollari per carta (aziendale) del 2010 ai pochissimi dollari di oggi.

Infine esistono i criminali informatici che si interessano esclusivamente delle vulnerabilità dei software installati sugli ATM. Sfortunatamente, comprometterli non è così difficile come dovrebbe essere. Larga parte degli ATM funziona ancora con software obsoleti o non adeguatamente aggiornati come Windows XP
o Windows XP Embedded, entrambi ben oltre il termine del loro ciclo di vita.

Questi malviventi tentano diversi espedienti per far sì che le macchine distribuiscano contanti. Uno dei più diffusi è connettersi attraverso le porte USB, nascoste nell'involucro posteriore dei bancomat, ed installare dei malware programmati affinché gli ATM rilascino denaro. Alcuni bancomat inoltre avviano automaticamente qualsiasi programma venga inserito nelle porte USB e sono quindi più semplici da infettare.

Lo scorso anno, attraverso gli skimmer è stato messo in atto un ***nuovo tipo di attacco denominato "scatola nera***".
Dopo aver scollegato il distributore di denaro dell'ATM dal corpo centrale della macchina, i criminali lo hanno connesso con il loro computer immettendo comandi fraudolenti per far in modo che la macchina rilasciasse denaro. Un'ulteriore tecnica in uso consiste nel tentativo di intercettare le comunicazioni della macchina su Internet o attraverso il cavo telefonico effettuando dei veri e propri attacchi di tipo man-in-the-middle, registrando così le informazioni dei clienti quando queste sono online.

Cosa significa tutto questo per un classico utente dei bancomat?

E' importante che i clienti conoscano le tecniche di manomissione degli hardware per saperle riconoscere. Per aiutarvi gli esperti di ESET hanno realizzato un elenco raccogliendo i suggerimenti forniti dalle banche e dalle forze dell'ordine:

1. Prima di tutto, controllate l'ambiente circostante per essere sicuri che la gente in coda dietro di voi sia a debita distanza.

2. Controllate il bancomat prima di utilizzarlo. Se notate qualcosa di sospetto, come parti mancanti o allentate, residui di nastro adesivo o altri danni visibili, evitate di usarlo e contattate l'assistenza della macchina. Ponete estrema attenzione nelle note località turistiche che sono spesso il bersaglio preferito dei criminali.

3. Coprite il tastierino quando inserite il vostro PIN. In questo modo vi proteggerete da eventuali videocamere nascoste o da altri dispositivi per la registrazione installati sul bancomat dai truffatori.

4. Se possibile scegliete ATM all'interno della banca che sono più difficili da raggiungere per i criminali che vogliono installare degli skimmer.

5. Se la macchina non eroga contanti o non restituisce la carta dopo la transazione o dopo aver premuto il tasto “Annulla”, contattate immediatamente la banca o l'istituto di credito associato alla vostra carta.

Fonte: ESET

{jcomments on}

{loadposition user6}