PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4325 di Lunedì 08 ottobre 2018

L'FBI lancia un allarme rosso per attacchi agli ATM

L'FBI ha lanciato un allarme a tutte le banche mondiali, avvertendo che dei criminali informatici stanno pianificando un furto di milioni di dollari in un attacco coordinato, di dimensione mondiale, alle macchine ATM.

Questo allarme è stato lanciato solo pochi giorni dopo che si è saputo che uno dei maggiori fabbricanti di ATM, la NCR, ha messo disposizione degli aggiornamenti software, afferenti alla sicurezza, dopo che alcuni ricercatori hanno dimostrato la presenza di punti deboli della comunicazione criptografata tra i computer e gli erogatori di banconote degli ATM; tali debolezze potrebbero consentire agli attaccanti di effettuare prelievi non autorizzati.

L'attacco dovrebbe arrivare a breve termine.

L'FBI, senza dare troppi dettagli sull'origine di questa notizia, ha indicato che l'attacco con ogni probabilità potrebbe coinvolgere una violazione dei protocolli di emissione delle carte di credito e debito, in modo da permettere una facile clonazione di queste carte ed effettuare prelievi abusivi.

Con ogni probabilità, l'attacco dovrebbe verificarsi, concentrandolo in un breve periodo di tempo, quasi certamente un weekend.

Il messaggio di allarme afferma anche che, sulla base di precedenti esperienze similari, le banche, che potrebbero essere attaccate con maggiore probabilità, sono quelle di dimensioni medie, per la più probabile presenza di vulnerabilità e controlli informatici meno incisivi.

Secondo uno specialista del settore, un attacco similare, che è stato rivelato nel luglio 2018, ha portato alla perdita di 2,4 milioni di dollari per una banca americana, grazie a due attacchi informatici, che hanno coinvolto centinaia di macchine ATM nel maggio 2016 e nel gennaio 2017 negli Stati Uniti.

Un altro attacco è stato registrato presso un ATM della Banca Nazionale degli Stati Uniti, che è iniziato sabato 28 maggio 2016 ed è proseguito per il successivo lunedì, che era un giorno federale di festa.

Un secondo attacco è stato registrato, presso un'altra banca, durante un weekend.

In entrambi i casi, ha riportato questo esperto, gli attaccanti sono riusciti a catturare dei dati circuendo un dipendente bancario; questo fatto ha consentito loro di compromettere il sistema informatico bancario, che gestiva i crediti e debiti dei clienti.

In queste tipologie di attacco, i criminali informatici tipicamente usano accedere ai sistemi bancari, per disattivare gli allarmi di sicurezza e sospendere i limiti di prelievo di ATM.

Anche nel settembre 2017 l'Europol ha lanciato un allarme per questa stessa tipologia di attacco.

L'FBI sollecita le banche a riesaminare le misure di sicurezza informatica in essere, effettuando l'aggiornamento dei software e attuando protezioni più incisive, al più presto possibile.

In particolare, l'FBI raccomanda che le banche attuino i seguenti interventi:

- utilizzo di sistemi di autentica a due fattori, utilizzando strumenti fisici o digitali,
- segregazione degli applicativi, che gestiscono le procedure per ottenere un estratto conto o per aumentare il livello di prelievo oltre una soglia predeterminata,
- attivazione di applicazioni in grado di bloccare l'esecuzione di malware,
- tenere sotto stretto controllo i profili di accesso di dipendenti, che hanno livelli di autorità elevata, nell'ambito della gestione delle procedure di accesso e prelievo agli ATM,
- tenere sotto controllo un traffico di rete indirizzato a regioni, dalle quali non ci si aspetta di dover ricevere messaggi, indirizzati alla specifica istituzione finanziaria.

Per quanto mi riguarda, raccomando ai lettori di tenere sotto frequente controllo il proprio estratto conto e, se possibile, attivare i segnalatori automatici, che allertano il titolare del conto, in caso di prelievo.

Source: GAO. | www.gao.gov

Adalberto Biasiotti

www.puntosicuro.it