PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4007 di giovedì 11 maggio 2017

Nuove metodologie di attacco agli ATM

Degli esperti hanno analizzato a fondo una nuova tecnica di attacco e hanno scoperto che funziona perfettamente. Ecco cosa hanno divulgato le pubblicazioni specializzate. Di Adalberto Biasiotti.

In Italia abbiamo già una lunga esperienza di attacchi agli ATM, che vengono perpetrati sia strappando dal proprio ancoraggio la macchina, sia infilando del gas esplosivo all'interno della macchina, sia ancora adottando dispositivi di vario tipo, che catturano i codici di sicurezza della tessera e la parola chiave dell'utente.

Questa nuova tecnica si basa invece su una combinazione di attacco fisico ed attacco informatico.

Dopo che sono state riscontrate delle anomalie meccaniche in alcune macchine, dalle quali erano state sottratte praticamente tutte le banconote custodite nei cassetti, gli esperti hanno trovato che i malviventi avevano praticato un foro del diametro di circa tre centimetri sul pannello frontale del dispositivo.

Questo foro può essere praticato con relativa facilità utilizzando le punte a tazza, che sembra possano perforare con relativa semplicità la struttura metallica frontale, che non è stata certamente progettata dal fabbricante per resistere a questo tipo di attacchi.

Una volta aperto un foro di circa tre centimetri di diametro, immediatamente a valle si trovano dei circuiti elettronici, cui è possibile accedere con relativa semplicità.

In particolare, praticando questo foro si può accedere a un porta seriale cui si può collegare un circuito esterno, pilotato dai malviventi. La porta seriale sopramenzionata permette di mettere in collegamento fra loro tutti i componenti informatici dell'ATM, partendo dal computer che controlla l'interfaccia di utente fino al dispositivo che aziona gli erogatori di banconote.

Una attenta analisi del protocollo informatico che si svolge attraverso questa porta seriale ha messo in evidenza che il protocollo è protetto da un algoritmo criptografico ben poco resistente, tant'è vero che gli studiosi hanno avuto la possibilità di violare questo algoritmo. Inoltre non sembra vi siano applicativi che garantiscano un'autentica del collegamento fra i vari moduli all'interno della macchina.

A questo punto i ricercatori hanno sviluppato un compatto circuito elettronico portatile, basato sul microcomputer Arduino, un'alimentazione a 9 volt e qualche altro componente, in grado di inviare comandi sulla porta seriale sopramenzionata.

Il dispositivo è stato quindi in grado di inviare un comando di erogazione di banconote alla macchina, che ha cominciato a sputare banconote a tutta velocità. Il dispositivo informatico interno è stato in grado di individuare la anomalia della situazione e reagire, ma il tempo richiesto per queste operazioni è stato decisamente inferiore al tempo necessario per estrarre tutte le banconote.

I ricercatori hanno allora messo in guardia il fabbricante dello ATM su questa debolezza, ma sembra che trovare soluzioni sia molto difficile. Ad esempio, il software dell'apparato non può essere aggiornato a distanza e quindi un eventuale intervento su questo fronte richiederebbe un intervento informatico su decine di migliaia di macchine.

Sono state anche interessate le associazioni di categoria, che al momento hanno scelto la strada del silenzio.

Non appena si è diffusa questa notizia, molti esperti ha fatto presente che negli ultimi tempi, soprattutto in Russia e nell'estremo oriente, alcuni hacker sono riusciti a infettare le reti bancarie, che controllano questi ATM, in modo da obbligare le macchine ad erogare le banconote contenute all'interno.

L'attacco che abbiamo appena illustrato è però particolarmente temibile, in quanto è relativamente facile da perpetrare e le tracce possono essere nascoste con facilità. In qualche macchina, attaccata con questo sistema, i malviventi hanno applicato un adesivo in corrispondenza del foro, impedendo quindi che una sommaria ispezione potesse mettere in evidenza l'attacco avvenuto.

D'altro canto, macchine di questo tipo, lasciate abbandonate nottetempo in aree neanche troppo ben illuminate possono essere bersagli attraenti per i malviventi. La installazione di sistemi di videosorveglianza può costituire un modesto deterrente, ma per solito questi impianti permettono solo di ricostruire l'accaduto e non di impedirlo.

Infine, un possibile intervento può essere realizzato rendendo più difficile la foratura del pannello frontale, ma esso non è certamente facile da attuare, per la necessità di intervenire su decine e decine di migliaia di apparati in servizio.

Chi scrive ricorda perfettamente un attacco che ha coinvolto parecchie centinaia di casse continue, realizzate per le Poste italiane, che potevano essere appunto neutralizzate con artifizi straordinariamente semplici e di natura prevalentemente meccanica.

Adalberto Biasiotti

www.puntosicuro.it