ATM e Cybersecurity: Evoluzione degli Attacchi Informatici e Soluzioni di Sicurezza



Nel panorama mutevole del *cybercrime*, il mondo *Finance* – comprensivo di organizzazioni bancarie, assicurative e di intermediazione finanziaria – appare tra i più colpiti già da diversi anni.

L'elevato valore degli *asset* coinvolti, la rilevanza dei dati trattati e l'avanzata digitalizzazione che lo caratterizza hanno reso questo settore sempre più vulnerabile ad attacchi informatici di varia natura, soprattutto di tipo *ransomware*, con perdite globali che nel 2023 hanno sfiorato i 200 milioni di dollari.

ATM Jackpotting, una minaccia dalle molteplici varianti

Se è facile comprendere perché il comparto bancario e finanziario attragga le mire dei cyber criminali, è anche noto come da tempo il settore manifesti una maggiore attenzione alla sicurezza informatica.

In particolare, il focus degli attacchi per il settore bancario si è concentrato sugli sportelli ATM, con modalità che sfruttano le interconnessioni fra le diverse infrastrutture bancarie: i *trend* rilevati, infatti, mostrano come il vettore di attacco si stia spostando dalle tradizionali tecniche *black-box* alle intrusioni di rete condotte attraverso ATM sempre più connessi, ma non sufficientemente presidiati.

Tra le modalità più diffuse vi è l'*ATM Jackpotting* che, aggirando il processo di autorizzazione della transazione grazie a diverse tecniche fraudolente, permette di accedere fisicamente agli sportelli automatici per prelevare denaro in modo illecito.

Dopo il caso registrato nel febbraio 2023 in cui si è osservata la variante denominata **FiXS** – causa di importanti perdite economiche, soprattutto tra gli operatori del Messico – negli ultimi mesi è stata evidenziata una nuova minaccia. Si tratta della combinazione tra due diverse tecniche, ovvero lo ***Shimming*** e il ***Relay Attack***, basate sulla compromissione di due dispositivi (entrambi non presidiati) e sul trasferimento di dati tramite più canali al fine di aggirare le misure di sicurezza.

Rilevata a maggio 2023, questa nuova minaccia si attiva attraverso un piccolo hardware inserito nel lettore delle carte presente sull'ATM, che rende possibile inviare in tempo reale, via *bluetooth*, i dati letti dal dispositivo a un apparecchio mobile che si trova in prossimità dell'ATM. La trasmissione dei dati è finalizzata al trasferimento finale presso un ulteriore dispositivo, rappresentato da un ATM nelle vicinanze, dove gli autori dell'attacco possono poi prelevare il denaro contante.

In questo modo, quando l'utente inserisce la propria carta nell'ATM e avvia l'operazione di pagamento/prelievo, i dati vengono intercettati dallo *shimmer* e trasferiti al dispositivo ATM collegato. Il titolare della carta riceve dapprima un falso messaggio di errore circa l'impossibilità di completare la transazione; successivamente, riceverà un addebito non riconosciuto relativo al ritiro effettuato dai truffatori presso il dispositivo preso di mira.

Questa tipologia di attacco utilizza tecniche innovative e complesse, che varcano le frontiere della sicurezza bancaria mettendo potenzialmente a rischio un livello altissimo di

operazioni ed esponendo le organizzazioni, nonché i loro clienti, a perdite economiche significative.

La visione di Auriga e la protezione multilivello della piattaforma Lookwise Device Manager (LDM)

Nella strategia di sicurezza concepita da Auriga, la migliore risposta all'incremento degli attacchi è l'approccio *Zero Trust*.

Allo scopo di valutare la vulnerabilità dell'infrastruttura tradizionale che gestisce i dispositivi, questo modello interroga ogni accesso e formula una serie di ipotesi: che il sistema di accesso remoto possa essere manipolato, che il sistema di distribuzione del software possa essere utilizzato per diffondere *malware*, che il tecnico della manutenzione (o l'utente finale) possano essere degli hacker, o ancora che il disco rigido possa essere rubato per effettuare attività di *reverse engineering*.

Il valore della strategia ***Zero Trust*** implica un radicale cambiamento nel paradigma della sicurezza, agevolando il passaggio da un modello di legittimità basato su fonti esterne e analisi del comportamento a un approccio realmente proattivo.

Applicando tale visione all'ecosistema degli ATM, uno dei principali punti critici risiede proprio nella drastica riduzione della superficie di attacco. In secondo luogo, è strettamente necessario un controllo stringente delle modifiche apportate all'ATM, bloccando qualsiasi tentativo di modifica del software o dell'hardware che non sia stato esplicitamente autorizzato.

Proprio partendo dall'approccio *Zero Trust* è stata sviluppata **Lookwise Device Manager (LDM)**, la soluzione Auriga per la cybersecurity dei canali bancari *self-service*.

LDM: una soluzione per ogni esigenza

Tra i diversi strumenti da implementare in termini di sicurezza, risultano sempre più importanti le soluzioni software con un grado di protezione più elevato rispetto ai firewall di rete, incaricati di proteggere la rete dal traffico indesiderato: i firewall delle applicazioni, ad esempio, non solo controllano le comunicazioni ma regolano anche quali processi possono essere coinvolti in esse. Inoltre, soluzioni più avanzate come la **microsegmentazione** sono più sicure e consigliabili, poiché utilizzano canali protetti con certificati controllati per ogni connessione, anche se comportano costi di implementazione e manutenzione più elevati.

Un livello di protezione multilivello e maggiormente completo per bancomat, ASST o altri dispositivi critici, è possibile con la piattaforma LDM che copre tutte le fasi del ciclo di vita di eventuali attacchi, garantendo al contempo la piena disponibilità dei servizi per i clienti.

Con l'obiettivo di impedire le connessioni di rete non attendibili e non autorizzate, la soluzione protegge i canali self-service da qualsiasi attacco malware, di tipo *Man-in-the-Middle* e anche remoto, garantendo la piena e costante disponibilità dei servizi per i clienti.

Infatti, indipendentemente dal vettore di attacco, **l'integrità del *file system*** non può essere manomessa; la **crittografia del disco rigido** (Full-disk encryption, FDE) proteggerebbe dagli attacchi di avvio a freddo; la **protezione hardware** dagli attacchi *Black-Box*; e la protezione delle comunicazioni dagli attacchi *Man-In-The-Middle* o dalle intrusioni di rete.

Ma anche qualora l'attacco avesse successo e il *malware* fosse introdotto nell'immagine del software ATM, la protezione **Software Whitelisting** ne impedirebbe comunque l'attivazione.

È inoltre previsto un costante sviluppo della soluzione per migliorarne i processi. In particolare, le funzionalità di crittografia del disco sono state estese agli **ambienti UEFI (Unified Extensible Firmware Interface)** più recenti senza moduli di sicurezza hardware, come i diffusissimi TPM (Trusted Platform Modules).

Questa nuova soluzione FDE consente di rendere la crittografia dipendente dall'Hardware ATM anche senza la necessità del Modulo TPM, oltre che compatibile con tutte le altre protezioni LDM e preattivata in fase di Certificazione Lab Image.

Tale capacità di adattamento e costante miglioramento garantisce ai clienti un'ampia possibilità di scelta, a seconda delle specifiche esigenze di ciascuna organizzazione, contribuendo così alla definizione di strategie di sicurezza innovative ed efficaci.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/atm-e-cybersecurity-evoluzione-degli-attacchi-informatici-e-soluzioni-di-sicurezza/