MEF Dipartimento del Tesoro

Newsletter

Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

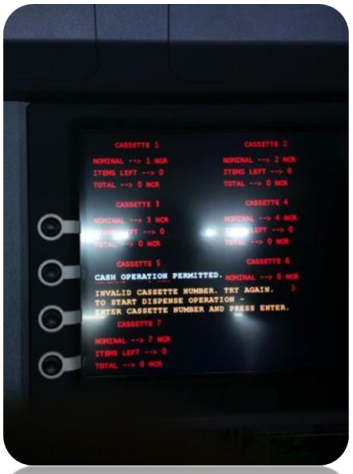
UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n° 11 - Novembre 2015

In questo numero:

ATM malware: come operano i moderni criminali informatici!

Negli ultimi mesi, gli esperti di sicurezza hanno osservato numerosi attacchi informatici contro gli sportelli automatici (ATM), causati da codici malevoli.
Le tendenza si è consolidata nell'ultimo anno: infettare un ATM con un malware consente ai criminali di prelevare somme di denaro con un minimo sforzo, digitando un codice specifico sul tastierino oppure impartendo un comando attraverso un SMS inviato a mezzo telefono cellulare.
Il fenomeno criminale ha origini in Europa orientale, dove sono attive le principali comunità di hackers specializzate in questa tipologia di frodi.
Se in passato gli hacker utilizzavano principalmente card skimmers e microcamere per carpire dati delle carte di credito dei clienti degli istituti finanziari, oggi prediligono compromettere direttamente l'ATM, istruendolo a rilasciare un somma di denaro disponibile in cassa. L'utilizzo del malware quindi fa sì che non sia più necessario clonare la carta dell'utente.
Lo scorso anno, una banda di criminali ha rubato quasi 1,6 milioni di sterline in una serie di attacchi a dispositivi ATM nel solo Regno Unito. Il gruppo ha utilizzato un malware per infettare gli ATM riuscendo in poche tempo a compromettere almeno 50 sportelli automatici.



Proprio come ogni malware, questi codici evolvono nel tempo: i loro autori ne hanno potenziato le capacità implementando funzionalità che consentono loro di rimanere nascosti ai sistemi di difesa utilizzati dall'industria bancaria.
Molti di questi codici hanno la capacità di restare dormienti sino a quando i criminali non procedono alla loro attivazione, tipicamente mediante un codice inserito attraverso la tastiera dell'ATM. Tra le varie funzionalità implementate dagli autori vi è la capacità di disabilitare temporaneamente la connettività alla rete locale, occultandosi ai sistemi di diagnostica. Le versioni più recenti dei malware sono in grado di eliminare altri malware eventualmente presenti sull'ATM garantendo ai criminali l'accesso esclusivo allo sportello automatico.

Ma quali sono i principali malware scoperti ad oggi e come operano?

I malware utilizzati per compromettere i dispositivi ATM hanno fatto la loro comparsa nella scena criminale nel 2013. In pochi mesi sono stati scoperti i codici **Tyupkin, Padpin e Ploutus.**

Ben presto questi malware, hanno fatto il giro del mondo: il codice **Tyupkin,** ad esempio, è stato utilizzato per compromettere macchine in diversi paesi, tra i quali *Russia, USA, Cina, India e Francia*. Gli esperti dell'azienda Kaspersky Lab hanno scoperto che i criminali che hanno utilizzato il malware Tyupkin hanno infettato solo i distributori automatici che non avevano alcun allarme di sicurezza installato.

Un altro malware che ha catturato l'interesse degli esperti di sicurezza negli scorsi mesi è **Ploutus**, un codice malevolo, scoperto da Symantec, che sfruttava una falla nel sistema Windows XP in uso ancora da molti ATM sparsi per il mondo. La particolarità dell'attacco basato su Ploutus era l'utilizzo dei telefoni cellulari per impartire istruzioni all'ATM mediante SMS.
In questo caso gli attaccanti, avuto accesso fisico all'ATM, vi connettevano un cellulare e, sfruttando la funzione di tethering USB, riuscivano a far pervenire all'ATM i comandi utili garantire l'erogazione delle banconote.
Ploutus appartiene a quella famiglia di malware che implementa una variante di uno schema di attacco noto come "BlackBox attack" in cui un dispositivo è connesso all'ATM per far pervenire comandi impartiti dall'esterno. Nel caso specifico gli hacker usarono un cellulare, ma la medesima funzione poteva essere implementata mediante un dispositivo Raspberry PI.
Tornando ai giorni nostri, qual è lo stato dell'arte dei malware utilizzati per compromettere i sistemi presenti negli sportelli automatici delle banche?

Lo scorso settembre, gli esperti dell'azienda di sicurezza FireEye hanno scoperto **SUCEFUL**, il primo malware "multi-vendor" capace di infettare gli ATM progettati dai principali produttori del settore.
SUCEFUL è in grado di interagire con successo con l'interfaccia XFS Manager implementata dai produttori degli ATM per il controllo delle principali periferiche connesse allo sportello automatico, come stampanti, dispenser, lettore di schede e pad. Secondo gli esperti delle aziende Diebold ed NCR, SUCEFUL è in grado di leggere i dati della carta di pagamento e di disabilitare le funzionalità in uso all'ATM, volte al rilevamento dei malware.
Ma SUCEFUL non è l'unico malware individuato di recente dalle aziende di sicurezza; nello stesso periodo i ricercatori dell'azienda Proofpoint hanno individuato un altro codice malevolo di nome **GreenDispenser**. GreenDispenser presenta molte analogie con il malware Tyupkin citato pocanzi, tra le caratteristiche di interesse l'implementazione di un meccanismo di autenticazione a due fattori (2FA) per la protezione dell'accesso al menù utilizzato dal malware per controllare l'ATM.
Interessante notare che il secondo fattore di autenticazione è ottenuto decodificando un codice QR visualizzato sullo schermo dell'ATM, circostanza che suggerisce l'uso anche di una app mobile da parte dei criminali per le operazioni di accesso al malware.
Gli esperti non hanno dubbi: l'utilizzo di malware per compromettere gli sportelli automatici continuerà a crescere ed è lecito attendersi che il livello di sofisticazione sia destinato ad aumentare, soprattutto per quanto concerne le tecniche per eludere i controlli di sicurezza.

Va tuttavia sottolineato che gli attacchi descritti sono stati possibili a causa di una palese inefficacia delle misure di sicurezza fisica adottate dagli istituti di credito vittime dei criminali informatici. Ad essere maggiormente esposti agli attacchi informatici sono risultati essere tutti gli ATM considerati "periferici", ovvero installati presso centri commerciali, aeroporti e distributori di benzina in cui le misure di sicurezza fisica non sono correttamente applicate.
Infatti, contrariamente a quanto si possa pensare, la prima infezione dell'ATM richiede che l'attaccante abbia un accesso fisico all'ATM per poter inoculare il malware mediante un CD oppure una chiavetta USB.
I criminali informatici sono soliti aprire il vano del bancomat in cui sono ospitati i connettori per le periferiche e le apparecchiature di rete e spesso tale vano non è protetto adeguatamente, é di semplice accesso per agevolare le operazioni di manutenzione ordinaria
Chiudiamo la nostra brevissima analisi dei malware con una lista di accorgimenti che gli Istituti di Credito dovrebbero sempre adottare per mettere in sicurezza i propri ATM:

- Mantenere aggiornato il sistema operativo in uso dall'ATM.
- Utilizzare processi di crittografia per la protezione del disco al fine di evitare manomissioni.
- Fornire un'adeguata protezione fisica.
- Installare un sistema di videosorveglianza efficace per proteggere i bancomat ed essere sicuri che gli allarmi di sicurezza funzionino. Assicurarsi che le telecamere siano visibili, circostanza che potrebbe fungere da deterrente.
- Controllare periodicamente lo stato di stato della sicurezza fisica e logica dei bancomat installati. Controllare regolarmente il bancomat per individuare eventuali segni di manomissione.
- Evitare l'uso di chiavi master fornite dai produttori degli ATM per la protezione del vano di servizio.
- Disabilitare da BIOS l'avvio da supporti mobili non autorizzati (ad esempio, CD ROM o chiavette USB), e proteggere il BIOS da eventuali modifiche.
- Essere a conoscenza di possibili attacchi di ingegneria sociale da parte dei criminali che cercano di raccogliere informazioni sui bancomat installati fingendo ispettori delle aziende produttrici.

L'UCAMP ha avuto modo di sentire i rappresentati del GIPAF i quali hanno riferito che per gli ATM italiani non risultano evidenze relativamente ad attacchi malware.

Ing. Pierluigi Paganini

Bitcoin*: tra assenza di regolamentazione e posizioni dottrinali.*

In un avviso del gennaio 2015 BankItalia definisce come valute virtuali (*virtual currencies*) le «rappresentazioni digitali di valore utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente». Il Bitcoin è indicato da Bankitalia come un esempio di moneta virtuale.

Bankitalia puntualizza che le valute virtuali non rappresentano in forma digitale le comuni valute a corso legale e non devono essere confuse con i tradizionali strumenti di pagamento elettronico quali le carte di credito, i bonifici bancari, le carte prepagate e altri strumenti di moneta elettronica. Infatti non sono emesse o garantite (*not backed*) da una banca centrale o da un'autorità pubblica. Generalmente non sono regolamentate anche se l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbano ritenersi attività lecite.
In Italia manca una disciplina sul Bitcoin e un intervento normativo non sembra essere imminente in ragione del fatto che il fenomeno risulta essere al momento poco sviluppato rispetto ad altri paesi. L'Unione Europea non ha ancora adottato alcun provvedimento di regolamentazione del Bitcoin.

Rileviamo che nell'ottobre 2012 è stato pubblicato uno studio BCE che ha affrontato con un approccio strutturato lo schema monetario di moneta virtuale. Interessante è il confronto che viene fatto nello studio tra lo schema Bitcoin e lo schema di monete elettroniche a corso legale, di cui alla Direttiva 2009/110/CE (concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica) e alla Direttiva 2007/64/CE (relativa ai servizi di pagamento nel mercato interno, c.d. *Payement Services Directive* o PSD).

I *bitcoin* sono *file* (cioè una sequenza di BIT) creati da utenti per mezzo di un *software open source* che esegue particolari algoritmi per la soluzione di un problema crittografico (c.d. *proof of work*) la cui risoluzione genera blocchi di BIT convalidati.

Il processo di generazione dei *bitcoin*, noto con il termine di *mining* (c.d. "estrazione") ha una complessità progressiva, in base alla generazione della moneta. Tale complessità è in funzione del tempo e dell'aumentare dei *bitcoin* in circolazione, la cui quantità è limitata *a priori*. Le informazioni necessarie al *software* per la generazione dei *bitcoin* sono scaricate *on-line*.

Dato che la creazione dei *bitcoin* richiede un'elevata potenza di calcolo del computer, per la soluzione dei suddetti problemi computazionali l'utente potrà collegarsi a servizi di *pool mining* (c.d. "consorzi di estrazione"). Tali servizi si realizzano in un calcolo distribuito e collaborativo, utilizzando una rete di computer *peer-to-peer* ("da pari a pari"). Se ne evince che ogni computer della rete è un nodo che tratta alla pari con gli altri nodi.

Una percentuale sul totale di *bitcoin* "estratti" dall'utente grazie al lavoro dell'intero *pool* sarà devoluta al *pool* stesso. Si sottolinea come esistano diverse tariffe al riguardo. Pertanto, questo tipo di valuta virtuale non ha un unico emittente ma viene creata direttamente in rete tramite un particolare algoritmo.

Generalmente Bitcoin è indicato con il simbolo "฿" o con l'abbreviazione BTC o XBT. Ogni utente potrà creare un conto personalizzato (o "portafoglio elettronico") per la conservazione e per la movimentazione di *bitcoin* (c.d. *e-wallet*). Tale conto potrà essere locale, salvato e gestito sul proprio *computer* (anche su uno *smartphone*), oppure potrà essere accessibile *on-line* tramite autenticazione dell'utente sul sito del *wallet provider* (in questo caso si tratta di *virtual wallet*).
I *bitcoin*, oltre che creati dall'utente, possono anche essere acquistati su una piattaforma di scambio, pagandoli con moneta legale. Un possessore di *bitcoin* potrà rivenderli in qualsiasi momento in cambio di moneta legale.
Il sistema della valuta virtuale Bitcoin consente la detenzione e la cessione anonime di valori in *bitcoin* all'interno della rete da parte di utenti che hanno indirizzi *bitcoin*.

Il Bitcoin è definito anche una "cripto moneta digitale" (*crypto-currency*) per l'utilizzo della crittografia nel suddetto processo di generazione e in quello di trasferimento tra conti diversi. Si impiega un sistema di crittografia asimmetrica (detta "a doppia chiave" o "a chiave pubblica") per assicurare la circolazione sicura dei *bitcoin* e per evitare che un utente possa utilizzare due volte la stessa moneta nei pagamenti di beni o servizi. L'algoritmo di crittografia utilizzato in questo processo di trasferimento è chiamato "Algoritmo di Firma Digitale su Curve Ellittiche" (noto come ECDSA o *Elliptica Curve Digital Signature Algoritm*). In questo modo saranno garantite la sicurezza dell'identità del beneficiario, la convalida del pagamento ricevuto e la "non ripudiabilità" della transazione effettuata. Ogni successiva transazione creerà una "catena di firme digitali", permettendo a chi riceve il pagamento di verificare la concatenazione delle diverse transazioni. Esse saranno annotate su un registro pubblico (*database*) condiviso da tutti i nodi della rete partecipanti al sistema (c.d. *Blockchain o "*Blocco catena"). È evidente come in tale sintema il controllo della creazione e del trasferimento della moneta da parte di autorità centrali o di altri intermediari sia sostituito dall'uso della crittografia. L'avviso al pubblico del 2014 di BankItalia (v. apertura articolo) richiama l'attenzione degli utilizzatori sui rischi insiti nell'utilizzazione e nell'investimento in valute virtuali. Questo è in linea anche con l'avvertenza già emanata nel dicembre del 2013 dalla'Autorità Bancaria Europea (ABE).

BankItalia avverte che «l'acquisto, il possesso o lo scambio di valute virtuali possono comportare rischi significativi, soprattutto per coloro che ne fanno uso senza disporre di un'adeguata conoscenza del fenomeno e consapevolezza dei rischi connessi». Inoltre «in assenza di obblighi informativi e di presidi di trasparenza, può risultare difficile reperire indicazioni di affidabilità per comprendere il funzionamento, i costi, il valore e i rischi di ciascun tipo di valuta virtuale». L'elenco dei rischi indicati da BankItalia comprende fra l'altro: *a)* l'assenza di tutele legali e contrattuali analoghe a quelle che accompagnano le operazioni in valuta legale;

b) l'assenza di forme di controllo e vigilanza da parte della Banca d'Italia o da parte di altre Autorità italiane demandate in materia; *c)* l'assenza di forme di tutela o garanzia delle somme depositate sulle piattaforme di scambio; *d)* la perdita permanente della moneta a causa di malfunzionamenti, attacchi informatici o smarrimento della *password* di accesso alla piattaforma di scambio; *e)* l'accettazione di valute virtuali da parte dei fornitori di beni e servizi su base volontaria; *f)* l'elevata volatilità del valore delle monete virtuali a causa dei meccanismi di formazione dei prezzi con conseguente rischio di perdite; *g)* il rischio di utilizzo delle monete virtuali per transazioni connesse a attività criminali e illecite; *h)* l'incertezza del trattamento fiscale delle valute virtuali in assenza di una regolamentazione con conseguenti implicazioni imprevedibili.

Sui rischi connessi all'utilizzo delle monete virtuali per attività criminali e illecite, si segnala che il FATF (*Financial Action Task Force*) ha pubblicato il 23 giugno 2014 un documento di discussione sulle monete virtuali. Ciò in adempimento dei propri compiti di effettiva attuazione delle misure legislative, regolamentari e operative nella lotta contro il riciclaggio di denaro, il finanziamento del terrorismo e ogni altra minaccia per l'integrità del sistema finanziario internazionale.

Per quanto riguarda la suddetta incertezza del trattamento fiscale delle valute virtuali, una recente sentenza della Corte di Giustizia Europea (caso C-264/14) ha richiamato l'attenzione degli addetti ai lavori sugli aspetti fiscali relativi ai *bitcoin*. Alla domanda di pronuncia pregiudiziale della Svezia circa l'assoggettamento all'imposta sul valore aggiunto (IVA) delle operazioni di cambio del Bitcoin in una valuta tradizionale o viceversa, la Corte ha risposto che non ricadono nella sfera di applicazione della suddetta imposta, seguendo l'orientamento dell'Avvocato Generale presso la Corte stessa.

Nell'Unione Europea non vi è una posizione uniforme fra gli Stati membri. Spagna, Regno Unito, Belgio, Finlandia propendono per l'esenzione IVA; Estonia e Polonia sono per l'imponibilità. In Italia è stato presentato all'Agenzia delle Entrate un interpello che propone l'esenzione IVA. La qualificazione della criptovaluta a livello giuridico italiano, in assenza di una regolamentazione porta la dottrina alla formulazione di mere ipotesi su come le transazioni di *bitcoin* potrebbero essere tassate. Tenuto conto delle diverse possibilità di utilizzo dei *bitcoin* si oscilla dalla disciplina IVA a quella IRPEF e IRPEG. Restiamo in attesa di chiarimenti.

Stefano Russo
Docente di Informatica giuridica
Luiss Guido Carli

Seminario Pericles 2015

A Community strategy to protect the Euro in the Mediterranean area

Si é svolto dal 25 al 27 Novembre a Marrakesh, in Marocco, uno degli eventi formativi di maggiore rilevanza per questo Ufficio: il programma Pericles "A Community Strategy to Protect the Euro in the Mediterranean Area".
Il programma Pericles favorisce la cooperazione tra le autorità nazionali, europee ed internazionali nella lotta alla falsificazione dell'euro. Le misure adottate comprendono lo scambio d'informazioni (seminari, workshop, incontri e conferenze), tirocini, scambi di personale nonché l'assistenza tecnica, scientifica e operativa. Quest'anno i paesi che sono intervenuti al programma internazionale sono stati: *Albania, Algeria, Croatia, Cyprus, Egypt, France, Italy, Jordan, Malta, Montenegro, Morocco, The Netherlands, Senegal, Spain, Tunisia, Turkey.*

Sono stati trattati i seguenti argomenti:

- *The European measures for the protection of Euro against counterfeiting.*
- *The Role of National Central Offices.*
- *The gathering and analysis of technical and statistical data relating to counterfeit notes and coins in Europe and other Countries.*
- *European and domestic legislations, criminal procedures and practices regarding currencies counterfeiting.*
- *The Role of the Central banks and the financial intermediaries in fighting the counterfeiting of euro and other currencies.*

Particolare importanza in questa edizione é stata data alla sezione Training, la quale, grazie alla preziosa collaborazione della BCE, della Banca d'Italia e della Zecca dello Stato, ha consentito, all'interno dei Workshops A e B, di allestire dei laboratori di individuazione delle banconote e monete contraffatte.
Con questo evento abbiamo puntato a coinvolgere sia il settore pubblico sia quello privato. Non è un caso che i rappresentanti istituzionali dei ministeri dell'Interno e dell'Economia, la Magistratura, le Forze di Polizia e le Banche centrali sono stati seduti, fianco a fianco, ai rappresentanti di banche commerciali, di associazioni di categoria del mondo bancario e ad altri soggetti del settore privato. Ognuno ha un ruolo significativo nella lotta alla contraffazione e, anche se i singoli contributi possono differire, sono tutti indispensabili.

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI (UCAMP)

Via XX Settembre, 97
00187 – Roma
Tel. 0647613535
Web: http://www.dt.tesoro.it
e-mail: ucamp.carte@tesoro.it