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° 10 - Luglio 2015

In questo numero:

Attività di carding nell'underground:
I Black Market

Come anticipato nel precedente articolo, pubblicato nella newsletter nr. 9 di marzo 2015, tra i fenomeni di maggiore interesse legati alle frodi relative alle carte di pagamento osservati nello scorso anno, vi è il rapido aumento dei reati operati in rete.

In rete esistono numerosi forum e siti internet che offrono ogni genere di prodotto, soluzione e servizio finalizzato alla realizzazione di frodi informatiche relative alle carte di pagamento. Nei differenti forum in rete, specializzati in questo genere di attività, è possibile reperire lotti di dati relativi a carte di credito rubate, codici malevoli per infettare i sistemi di pagamento da cui estrarre i dati relativi alle carte, noleggiare botnet composte da migliaia di PC infetti da utilizzare per le campagne di spam, servizi di riciclaggio del denaro e persino guide per criminali neofiti che si desiderano avviarsi a questa nuova redditizia attività.

Tra le attività più popolari nell'ecosistema criminale vi è senza dubbio quella del "carding" ovvero della commercializzazione o scambio dei dati relativi alle carte di pagamento. La disponibilità di questa tipologia di informazioni nell'ecosistema criminale agevola attività illecite relative alle frodi con carte di credito. Gruppi di criminali acquisiscono i dati relativi a carte di credito rubate da usare per la clonazione di carte di pagamento, per effettuare acquisti in rete oppure per rivendere a loro volta tali dati integrandoli con servizi ed informazioni accessorie. I luogo di scambio preferito dalla criminalità sono sicuramente i Black Market.

Molti forum in internet offrono prodotti relativi ad attività illegali connesse alle carte di pagamento, la maggior parte di questi servizi web è nascosto all'interno di reti di "anonimizzazione" come la popolare rete Tor.
Tra le comunità più attive nella commercializzazione di dati relativi a carte di pagamento in rete potremo citare embargo.cc, rescator.cm e netsky.bz, sebbene la maggioranza delle vendite avvenga attraverso mercati specializzati nel Dark Web.

La scelta di black market ospitati in reti come Tor è dettata dalla necessità di garantire l'anonimato di venditori e acquirenti e di offrire al tempo stesso ambienti in cui operare secondo regole stabilite dalla comunità, che premiano venditori più affidabili e mettono a disposizione servizi di escrowing a garanzia delle transizioni.

Proprio i servizi di escrowing (acconto di garanzia) sono uno degli elementi che maggiormente influenzano lo sviluppo di comunità dedite alle frodi relative alle carte di pagamento. La disponibilità di servizi di escrowing consente agli acquirenti di acquistare prodotti con la certezza che siano rispettate le condizioni specificate (e.g. percentuale di validità delle carte di credito appartenenti a un lotto di carte) e al tempo stesso consentono ai venditori di avere certezza che il pagamento sia effettuato secondo le modalità pattuite.

Rintracciare gli operatori di un black market è un'impresa tutt'altro che semplice e richiede un notevole sforzo da parte delle autorità. Perciò questi ambienti sono considerati dai criminali informatici sufficientemente sicuri.
Altro elemento a favore di questi mercati paralleli è la possibilità di effettuare pagamenti utilizzando moneta virtuale, come il Bitcoin, che fornisce un ragionevole livello di anonimato delle transazioni.

Va detto che il prezzo dei dati relativi alle carte di pagamento si è progressivamente ridotto nel corso degli ultimi anni e tale flessione è principalmente imputabile alla aumentata disponibilità di dati relativi a carte di credito rubate. Tale disponibilità è sicuramente condizionata dagli innumerevoli incidenti occorsi negli ultimi anni e che hanno portato al furto di dati relativi a diverse centinaia di milioni di carte di pagamento in tutto il mondo.

Tra i settori maggiormente colpiti dalle organizzazioni criminali vi è il retail: la rapida diffusione di malware specifici per il furto dei dati gestiti da sistemi PoS è sicuramente una delle principali cause per l'aumento dei volumi di dati provenienti da attività illecite ed immessi nell'ecosistema criminale.
Navigando nei principali siti che offrono dati relativi alle carte di credito è facile imbattersi in termini come "CVV" e "Dump." Il termine CVV, che non deve essere confuso con il codice composto da tre cifre e presente sul retro della carta di credito, è utilizzato dagli operatori dell'underground criminale specializzati nella commercializzazione delle carte di pagamento, per indicare i record relativi alla carta e che possono includere il nome dell'intestatario, l'indirizzo dell'intestatario, la data di scadenza e il CVV2 che è il codice presente dietro la carta. I CVV possono essere utilizzati solo per frodi online, anche dette "Card No Present fraud" (CNP). Il prezzo medio di un CCV relativo ad una carta di credito statunitense è di poco superiore alla decina di dollari.

Il termine Dump è invece utilizzato per indicare i dati grezzi immagazzinati nella banda magnetica di una carta di credito, informazioni di solito catturate mediante attività di "skimming" oppure attraverso l'uso di malware che infettano i sistemi di pagamento PoS. I dati componenti un DUMP possono essere utilizzati dai criminali informatici per clonare carte di credito e utilizzare le carte prodotte per prelievi presso gli ATM delle banche o per pagamenti in cui è necessaria la presenza fisica della carta. I prezzi dei DUMP sono generalmente superiori a quelli dei CVV in quanto i criminali possono utilizzarli per acquistare beni di valore superiore. Il Dump di una carta di credito può arrivare anche a superare i 100$, se la carta è relativa ad un cliente Top e quindi ha disponibilità finanziari superiori.

Riassumendo, il prezzo dei dati relativi a carte di credito/debito statunitensi (CVV US) arriva fino a 10 dollari, mentre per una carta relativa ad un cittadino europeo si può arrivare a spendere una cifra che varia dai 5 ai 25 dollari.

Il prezzo è superiore se i dati includono il contenuto delle tracce presenti nella banda magnetica della carta (DUMP), per cui si potrebbe arrivare a pagare ciascun pezzo diverse decine di euro.

HACKER CREDENTIALS AND SERVICES	DETAILS	PRICE
*Visa and Master Card (US)		$4
American Express (US)		$7
Discover Card with (US)		$8
Visa and Master Card (UK, Australia and Canada)		$7 -$8
American Express (UK, Australia and Canada)		$12- $13
Discover Card (Australia and Canada)		$12
Credit Card with Track 1 and 2 Data (US)	Track 1 and 2 Data is information which is contained in digital format on the magnetic stripe embedded in the backside of the credit card. Some payment cards store data in chips embedded on the front side. The magnetic stripe or chip holds information such as the Primary Account Number, Expiration Date, Card holder name, plus other sensitive data for authentication and authorization.	$12
Credit Card with Track 1 and 2 Data (UK, Australia and Canada)		$19-$20
Credit Card with Track 1 and 2 Data (EU, Asia)		$28

Figura 1 - Prezzi e dati relativi alle carte di credito (Rapporto Trend Micro su Underground Russo)

Nei black market è possibile reperire non solo i dati relativi alle carte di credito, ma sempre con maggior frequenza è facile imbattersi in venditori che offrono anche altri servizi per agevolare le operazioni dei propri clienti o per compiere frodi più evolute.

Negli ultimi mesi si è osservato un significativo aumento nella vendita di informazioni accessorie relative a ciascuna carta di credito. Nella quasi totalità dei forum specializzati nella vendita di carte di credito è possibile acquistare “Fullz” ovvero l’insieme completo di informazioni relative ad un particolare individuo che comprende i suoi dati personali, dati relativi alle carte di pagamento, il numero di previdenza sociale e una collezione di informazioni accessorie tra cui eventuali bolletta delle principali utenze dell’intestatario della carta.

Il pacchetto completo consente ai criminali di acquisire l’identità della vittima per condurre diverse tipologie di frodi finanziarie. Queste informazioni possono essere utilizzate per aprire conti correnti di appoggio utilizzati per traferire temporaneamente le somme di denaro ricavate grazie alle attività illecite.

Una particolare categoria di prodotti offerti nell’underground criminale sono i “Dead Fullz” ovvero informazioni finanziarie appartenenti a persone decedute. Queste informazioni, sebbene includano dati relativi a carte di credito non più valide, possono essere utilizzate per numerose attività criminali, ad esempio per aprire un account su piattaforme di pagamento come PayPal da usare per attività di cash out oppure per realizzare frodi relative ad eventuali rimborsi destinate alle persone defunte.

Ulteriori informazioni relative alle attività inerenti le frodi con le carte saranno approfondite all'interno del nuovo "Rapporto statistico sulle frodi con le carte di pagamento," pubblicato dall'UCAMP .

Quest'anno il rapporto integrerà le preziose informazioni inerenti le attività sulle frodi con le carte di pagamento con approfondimenti sulle tecniche, tattiche e metodiche adottate dai principali attori nell'ecosistema criminale, inclusa una dettagliata analisi dei principali black markets e delle relative dinamiche.

Ing. Pierluigi Paganini

Carte prepagate e pagamenti on-line

Un'alternativa all'uso delle carte di pagamento tradizionali

In un nostro precedente articolo ci siamo soffermati sull'importanza delle *policy* e misure di sicurezza informatica a cui un utente deve attenersi prima di effettuare acquisti *on-line* con le carte di pagamento (sia esse di debito che di credito) al fine di ridurre il rischio di frodi (Newsletter n.7 – luglio 2014). Nell'occasione abbiamo evidenziato che gli attuali *software* di sicurezza, adottati dai siti *web* che praticano il commercio elettronico di beni e/o servizi, sono più aggiornati e affidabili, riducendo notevolmente sia i rischi di intercettazione del numero della carta di pagamento nel momento in cui l'acquirente la fornisce, sia quelli di violazione del database aziendale del venditore in cui sono contenuti i dati dei clienti.

Purtroppo, nonostante vengano utilizzate tecnologie sofisticate al passo coi tempi, gli utenti/acquirenti si espongono comunque ai rischi derivanti dal vasto mondo del *web* in quanto sono troppo spesso ingenui in fatto di *policy* e misure di sicurezza informatica. La legge italiana tutela il consumatore che utilizza carte di debito o di credito su pagamenti non autorizzati o eccedenti il prezzo pattuito ovvero, effettuati fraudolentemente da parte da terzi (vedi codice del consumo, d.lgs. n. 206/2005 e successive modificazioni).

Tuttavia il consumatore, con diligente prudenza, deve prestare la massima attenzione nell'uso delle carte di pagamento, e nel caso di pagamento *on-line* deve proteggere il proprio dispositivo informatico per ridurre i rischi di frodi. Per chi comunque non volesse utilizzare le tradizionali carte di pagamento *on-line* per evitare truffe, si suggerisce come valida alternativa la carta prepagata ricaricabile (utilizzabile anche per pagamenti *off-line con POS*). Infatti, tale tipo di carta (non vincolata a un conto corrente) ha una disponibilità limitata a un importo prepagato (c.d. *plafond*). Pertanto l'importo massimo spendibile non sarà mai superiore al *plafond* totale o residuo della carta stessa. Da ciò deriva che i rischi sono limitati all'importo (o al residuo) della carta.

D'altra parte ai sensi della normativa vigente (d.lgs. n.11/2010), in caso di comportamenti fraudolenti, non è prevista la franchigia di centocinquanta euro come nelle carte di credito. È evidente che in tal caso si realizza una minore tutela per il titolare della carta stessa. La carta può essere ricaricata più volte fino alla sua scadenza e non vi sono limiti normativi sul *plafond*.

Ogni pagamento effettuato verrà scalato dall'importo disponibile. I costi di emissione della carta e quelli della sua gestione (ricariche e prelievi dagli sportelli automatici ATM) sono minimi, e non è previsto alcun canone annuo. I circuiti generalmente utilizzati sono quelli comuni alle altre carte di pagamento. Inoltre le prepagate consentono di prelevare contanti presso gli sportelli automatici ATM della banca del cliente o altri ATM abilitati in Italia e all'estero.

Ci sono anche altri servizi aggiuntivi, come la ricarica del telefono cellulare o il rifornimento di carburante senza commissione. Data la variabilità del *plafond*, però, le prepagate, ad esempio, spesso non vengono accettate come garanzia per il noleggio di un'auto o per le prenotazioni alberghiere.

Un altro strumento di pagamento molto interessante per chi vuole fare acquisti *on-line* in totale tranquillità è rappresentato dalla "carta virtuale usa e getta". Alcune banche offrono ai propri clienti le carte virtuali c.d. "usa e getta" che possono essere valide per un unico acquisto il cui importo massimo corrisponde esattamente al prezzo del bene che s'intende acquistare (comprese le eventuali spese e/o commissioni).

Le carte virtuali possono essere anche limiate temporalmente fino ad un massimo di dodici mesi e il loro importo massimo è pari alla somma dei vari acquisti da effettuare (c.d. carta virtuale "di durata"). Il processo di creazione della carta virtuale, avviato solo dopo che l'utente è stato abilitato con un'autenticazione "forte" (codice utente e *password* + OTP), genera il numero della carta, la relativa data di scadenza e il conseguente codice di sicurezza (CVV2).

Le più recenti carte prepagate (c.d. "carte evolute") sono quelle dotate di un codice IBAN che, oltre alle funzioni su citate, consentono il bonifico bancario anche in entrata e l'accredito di stipendi o pensioni (per questo chiamate anche "carte conto").

Invece le carte prepagate c.d. *contactless*, dotate di *chip* con tecnologia di identificazione a radio frequenza (*Radio-Frequency Identification*, RFID) consentono il pagamento avvicinando la carta al POS abilitato con il prezzo impostato in precedenza dall'operatore. In ogni caso si ritiene che il variegato mondo delle carte prepagate si arricchirà in un prossimo futuro di ulteriori e sempre più raffinate novità.

Stefano Russo
Docente di Informatica giuridica
Luiss Guido Carli

EURO - Approfondimento del primo semestre 2015.

La valuta ritirata nel primo semestre 2015 non differisce significativamente da quella osservata nello primo semestre 2014. Infatti, sia per le banconote che per le monete si ha un lieve incremento di unità (circa 4%) e di controvalore in euro (3%-7%). Nel semestre 2015 i sequestri sono stati nulli per le monete e trascurabili per le banconote (circa il 2% di controvalore complessivo). Nel primo semestre 2014 i sequestri erano più consistenti, ma non ragguardevoli (il controvalore si assestò al 14% per le monete e al 7% per le banconote). Ne segue che il circolante (parte complementare ai sequestri), presenta, nel 2015, incrementi più consistenti di quelli relativi all'intera valuta. Infatti, le banconote sono cresciute di circa l'8% (4% in controvalore) e le monete del 24% (23% in controvalore). Vediamo ora come si articolano al loro interno le variazioni osservate sul circolante.

Nelle figure sottostanti si illustra (linea gialla) l'andamento mensile delle differenze assolute, a 12 mesi, articolato, anche, per taglio banconota (figura 1) e per area geografica (figura 2).
Nei primi 4 mesi del 2015 le variazioni assolute hanno oscillato nel range dei 1.000-2.000 pezzi per poi sostanzialmente annullarsi nei mesi rimanenti. In tutti i mesi, pur se con differenti intensità, si ha un aumento delle banconote da 5, 50 e 200 euro ed una diminuzione di quelle da 10 euro.

La banconota da 20 euro presenta incrementi non trascurabili nei primi 4 mesi e si contrae nei successivi. Alla fine del periodo le banconote da 5, 20 e 50 euro sono in crescita, rispettivamente, 1.400, 3.400 e 2.600 pezzi; mentre quella da 10 euro sono in contrazione di 1900 pezzi. L'analisi per area geografica non evidenzia trend sistematici se non per il Sud che presenta un guadagno positivo in tutti i mesi (alla fine del periodo il guadagno è di 3400 pezzi). Importante la contrazione del Nord-Est negli ultimi due mesi.

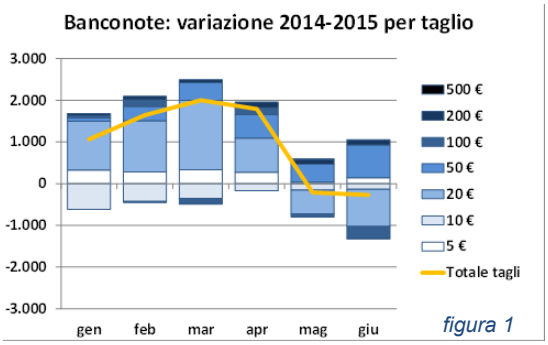

figura 1

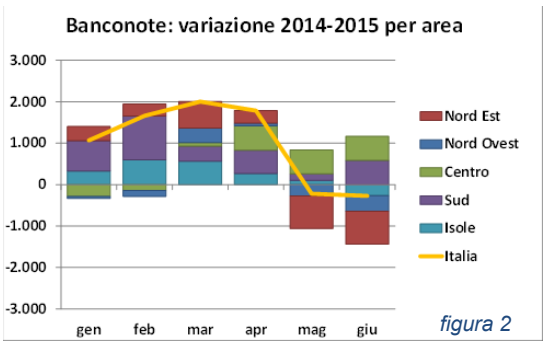

figura 2

Le differenze assolute, a 12 mesi (linea gialla), osservate sulle monete mostrano un trend positivo in tutti i mesi ad esclusione dell'ultimo, in cui, similarmente alle banconote, si ha una contrazione (figure in basso).

L'articolazione per taglio (figura 3) e area geografica (figura 4) mostrano, a differenza di quanto visto nelle banconote, un movimento sostanzialmente corale di tutti i tagli e area geografica nella direzione generale (linea gialla).

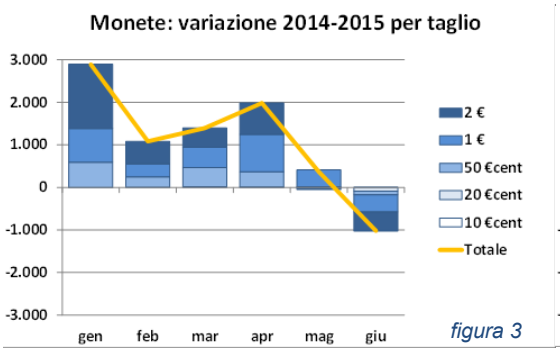

figura 3

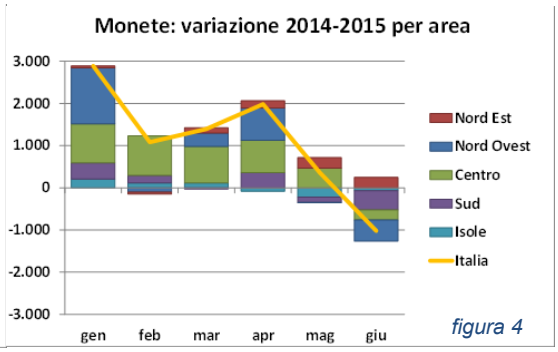

figura 4

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

Via XX Settembre, 97
00187 – Roma
Tel. 0647613535
Web: http://www.dt.tesoro.it