DIPARTIMENTO DEL TESORO
MINISTERO DELL'ECONOMIA E DELLE FINANZE

Frauds: some facts

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

UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n° 2 - Novembre 2012

In questo numero:

In qualità di Direttore dell'Ufficio VI, l'uscita di questo numero della newsletter mi fornisce la possibilità di rivolgere un saluto ai destinatari di questa importante pubblicazione, che ha lo scopo di aggiornare e mantenere alto l'interesse sulle tematiche legate alle frodi sui mezzi di pagamento e sulle attività svolte dall'Ufficio Centrale Antifrode dei Mezzi di Pagamento/UCAMP, istituito presso il Dipartimento del Tesoro, Direzione V "Prevenzione dell'utilizzo del Sistema Finanziario per fini illegali". Sono certo che nei prossimi mesi, anche grazie al qualificato contributo dei nostri interlocutori istituzionali del mondo bancario, accademico e della società civile, riusciremo a mantenere alta l'attenzione degli operatori e dei cittadini sulla fenomenologia e le insidie delle frodi in genere. ***Antonio Adinolfi***

Le transazioni non riconosciute

Un anno di raccolta dati, prodotti dal SIPAF - segmento informazioni, ha permesso di individuare due tipologie di fenomeni che analizziamo di seguito:

- punti di accettazione collegati a sistemi di giochi online;
- punti di accettazione relativi ad ATM - trasferimento fondi tra carte di credito a carte ricaricabili.

In merito al primo punto, attraverso l'analisi dei risultati restituiti dalla funzionalità di individuazione dei sospetti punti di accettazione, il sistema ha restituito una lista di punti vendita classificati con categoria merceologica standard ISO/VISA 7998 *(Betting/track/casino/lotto*).

L'analisi del fenomeno ha messo in evidenza che da quanto il sistema è in esercizio (01.12.2008/31.12.2011) sono state individuate 31.534 transazioni disconosciute per un importo medio di circa € 252,00 per il solo fenomeno giochi on-line.

Lo schema riportato in *figura 1* illustra come sia possibile, monetizzare beni e servizi, partendo dall'acquisizione illecita di numeri di carte e spendendo sui siti di gioco online.

Figura 1 - schema di spendita di una carta di pagamento, attraverso sistemi di gioco on-line

Il frodatore recupera le credenziali di accesso al portale della banca o le informazioni sulla carta di credito, attraverso tecniche di *social engineering*, *phishing* o attraverso l'utilizzo di *trojan* (es. *ZEUS*). Le informazioni delle carte collezionate, vengono utilizzate per la spendita su siti di casinò e/o giochi on-line.
Lo schema di frode prevede che i partecipanti al "gioco", "investano" ovvero, perdano il loro denaro. Tali somme saranno vinte da un complice del frodatore che avrà poi il compito di incassare e monetizzare le vincite, trasferendole su "N" carte ricaricabili non intestate oppure acquisite illecitamente con falsa identità.
Le carte ricaricabili che hanno raccolto i fondi illecitamente spesi on-line, potranno poi essere utilizzate per acquisti on-line o spese presso i POS per l'acquisto di beni o servizi.
Lo schema illustrato precedentemente, può essere utilizzato anche come meccanismo di riciclaggio denaro.

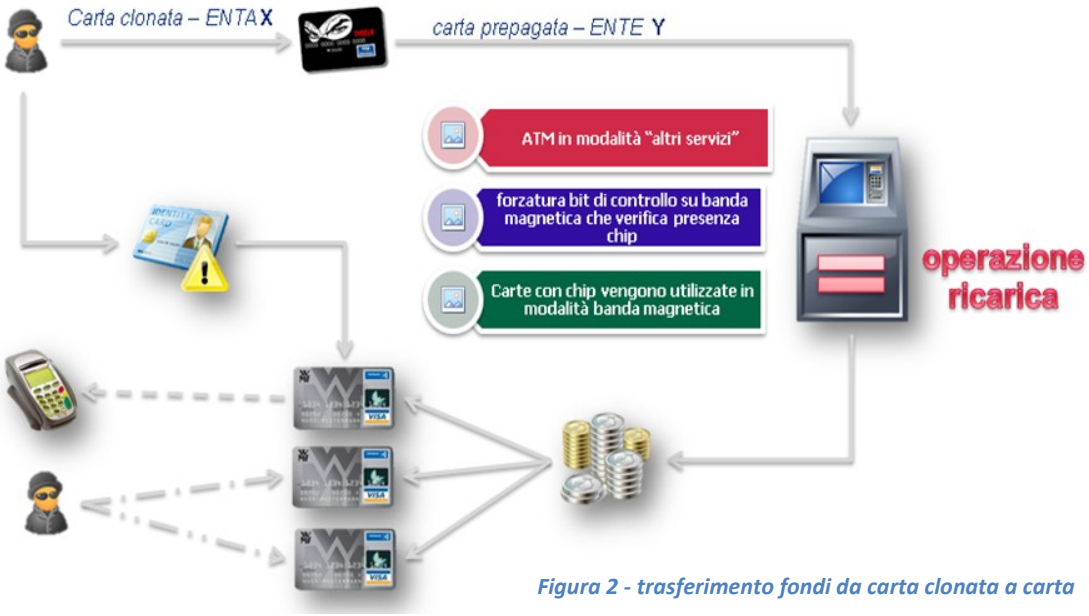

Figura 2 - trasferimento fondi da carta clonata a carta

La seconda tipologia di frode (*figura 2*), mostra come un frodatore, trasferisce fondi da carte di pagamento clonate a carte ricaricabili. Le carte di pagamento, di proprietà della Banca X vengono utilizzate presso particolari sportelli ATM, effettuando un'operazione di ricarica (trasferimento fondi) su una carta ricaricabile acquisita con falsa identità di proprietà della Banca Y. Questo tipo di operazione è consentita solo in modalità banda magnetica. Il frodatore in possesso di carte clonate procederà durante la fase di riscrittura della banda magnetica su una *blank card* a forzare il *bit* di controllo preposto alla verifica della presenza di carta con *chip*. In questo modo viene aggirato dal frodatore il controllo in locale effettuato dall'ATM. L'ATM vulnerabile potrà essere utilizzato in modalità "*altri servizi*" effettuando l'operazione di ricarica.

Con il monitoraggio e l'analisi dei dati presenti nei segmenti DATI e INFORMAZIONI del Sipaf, svolto da Ucamp, è possibile verificare l'andamento dell'utilizzo dello strumento "carta" e il fenomeno legato all'utilizzo illecito delle carte di pagamento in una particolare categoria merceologica.

Il punto di forza del sistema SIPAF è rappresentato indubbiamente dalla condivisione delle informazioni fornite da tutti gli Enti accreditati a sistema. Il concetto di condivisione, rappresenta la linfa vitale del sistema, garantendo l'individuazione pro-attiva dei punti di compromissione e dei punti di accettazione.

La fiducia nei pagamenti elettronici tra sicurezza reale e percepita

Prof. Massimo Petrone - Università degli Studi del Molise

L'Italia per diversi anni ha visto procedere con molta lentezza la penetrazione dei pagamenti elettronici tra la popolazione. Qualcosa però sta cambiando: se da una parte i comportamenti non sembrano rivoluzionarsi, dall'altra registriamo una forte consapevolezza dell'aumento di peso del pagamento elettronico nella vita di tutti i giorni. Da una recente indagine Ipsos emerge, infatti, che solo il 38% dei 14-64enni intervistati paga solo ed esclusivamente in contanti quando fa acquisti nei negozi.
Inoltre il futuro sembra comunque a favore dei pagamenti immateriali: solo una minoranza (36%) pensa che nel futuro ci sarà sempre il contante, mentre il 55% ritiene che tra 10 anni tutti i pagamenti avverranno con metodi elettronici.
Il continuo aumento del numero di utenti che impiegano i sistemi di pagamento elettronico trova la sua motivazione nella crescente fiducia che gli stessi attribuiscono ai metodi impiegati nonché nell'efficienza delle funzionalità implementate per renderne agevole l'utilizzo. Dette motivazioni vanno inquadrate all'interno di un contesto nel quale la sicurezza può essere sia reale che percepita e tali diverse condizioni non sono né perfettamente coincidenti né totalmente indipendenti. Il legame tra i diversi aspetti sopra considerati è sinteticamente schematizzato nella Figura 1.

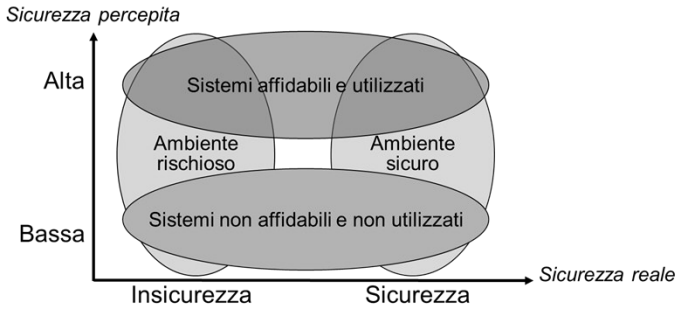

Figura 1: Incidenza della "Sicurezza reale" e della "Sicurezza percepita" sull'affidabilità e sull'utilizzabilità dei sistemi di pagamento elettronico (e-Pagamenti).

Al fine di poter raggiungere un ottimale rapporto tra la sicurezza percepita e quella reale occorre considerare i seguenti aspetti:

- l'innalzamento della sicurezza reale comporta significative conseguenze dal punto di vista funzionale ed operativo (maggiore complessità degli strumenti e dei sistemi e, a volte, incremento degli attori coinvolti) e, conseguentemente, una maggiore resistenza all'uso dei sistemi di pagamento elettronici (e-Pagamenti);
- l'aumento della sicurezza percepita determina una maggiore fiducia nei sistemi e, conseguentemente, una maggiore diffusione dei sistemi di pagamento elettronici (e-Pagamenti).

Lo schema riportato nella seguente Figura 2 sintetizza il tipo di legame esistente tra la "Sicurezza reale" e la diffusione dei pagamenti elettronici (e-Pagamenti) caratterizzato dal fatto che ad

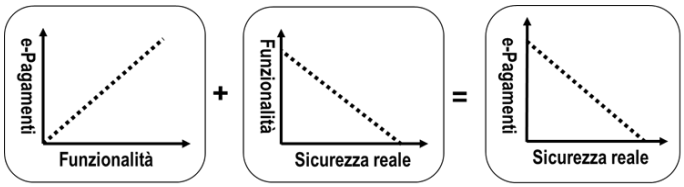

Figura 2: Rapporto tra "Sicurezza reale" e "e-Pagamenti" come somma del rapporto tra "Funzionalità" e "e-Pagamenti" nonché tra "Sicurezza reale" e "Funzionalità"

un aumento della "Sicurezza reale" corrisponde un decremento dell'utilizzo dei sistemi utilizzati. Tale circostanza è dovuta alle seguenti condizioni:

- ad un incremento dell'efficienza della funzionalità dei sistemi utilizzati per i pagamenti elettronici (e-Pagamenti) corrisponde un aumento del relativo utilizzo;
- ad un aumento della "Sicurezza reale" corrisponde un decremento dell'efficienza della funzionalità dei sistemi utilizzati per i pagamenti elettronici (e-Pagamenti).

Lo schema riportato nella seguente Figura 3 sintetizza il tipo di legame esistente tra la "Sicurezza percepita" e la diffusione dei pagamenti elettronici (e-Pagamenti) caratterizzato dal fatto che ad un aumento della "Sicurezza percepita" corrisponde un incremento

Figura 3: Rapporto tra "Sicurezza percepita" e "e-Pagamenti" come somma del rapporto tra "Fiducia" e "e-Pagamenti" nonché tra "Sicurezza percepita" e "Fiducia"

dell'utilizzo dei sistemi utilizzati. Tale circostanza è dovuta alle seguenti condizioni:

- ad un incremento della "Fiducia" corrisponde un incremento dell'utilizzo dei sistemi utilizzati per i pagamenti elettronici (e-Pagamenti);
- ad un aumento della "Sicurezza percepita" corrisponde anche un incremento della "Fiducia".

Lo schema riportato nella seguente Figura 4 mostra il legame tra la Sicurezza (reale percepita) e l'utilizzo dei sistemi di pagamenti elettronici (e-Pagamenti). In particolare, nello schema viene evidenziato lo spazio entro il quale si raggiunge un equilibrio tra la fiducia e l'efficienza della funzionalità dei sistemi utilizzati per i pagamenti elettronici (e-Pagamenti).

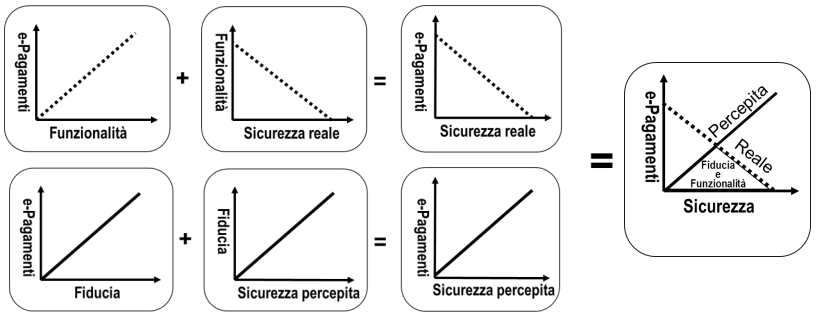

Figura 4: Rapporto tra "Sicurezza" (reale e percepita) e "e-Pagamenti" come somma del rapporto tra "Sicurezza reale" e "e-Pagamenti" nonché tra "Sicurezza percepita" e "e-Pagamenti"

Da quanto sopra riportato si evince che per favorire la diffusione dei sistemi di pagamento elettronico è indispensabile ridurre la distanza tra la sicurezza reale e quella percepita intervenendo, da un lato, sui requisiti che incidono sulla fiducia dell'utente e, dall'altro, sulle modalità di accesso al servizio.

Con riferimento all'uso di sistemi di pagamento on-line, Jøsang e al. hanno introdotto il seguente insieme di requisiti di fiducia che rappresentano un'utile indicazione per la progettazione e la gestione dell'identità dei suddetti sistemi di pagamento:

F1. *Il service provider protegge la privacy del client* – CL ha *fiducia* in SP. SP deve adottare adeguate politiche di sicurezza.

F2. *Il service provider ha implementato soddisfacenti procedure di registrazione utente e meccanismi di autenticazione (dalla prospettiva del client)* – CL ha *fiducia* in SP. SP deve implementare adeguate procedure e meccanismi di autenticazione.

F3. *Il client maneggia le proprie credenziali di autenticazione con adeguata cura* – SP ha *fiducia* in CL. CL deve seguire le pratiche raccomandate da SP.

F4. *L'accesso al servizio tramite asserzione tra service provider da parte degli utenti avrà luogo unicamente quando legittimamente richiesto dal client* – i SP hanno *fiducia* l'uno nell'altro. C'è accordo tra i SP.

F5. *La corrispondenza delle identità tra service provider è corretta* – i SP hanno *fiducia* l'uno nell'altro. I SP hanno comuni procedure di corrispondenza.

F6. *Il service provider rispetta le politiche ammesse per la correlazione dei dati personali dello stesso client da altri service provider* – i SP hanno *fiducia* l'uno nell'altro. C'è accordo tra i SP.

F7. *Il provider di credenziali ha implementato adeguate procedure per la registrazione degli utenti e per l'emissione delle credenziali* – SP ha *fiducia* in IdP.

F8. *Il Personal Authentication Device è a prova di manomissione.*

F9. *Il service provider ha l'identità attesa.*

Formazione & Eventi

Programma *Pericles* - Dubrovnik (Croazia) 10/12 ottobre 2012

Il Dipartimento del Tesoro, Direzione V, UCAMP - con il sostegno finanziario e la partecipazione della Commissione Europea/OLAF - ha organizzato in data 10/12 ottobre 2012 il seminario internazionale intitolato "*A community strategy to protect the Euro in the Mediterranean area*". Il seminario si è tenuto a Dubrovnik (Croazia) e ha visto la partecipazione di rappresentanti delle principali Istituzioni centrali, oltre che dell'Italia, della Croazia, della Turchia, del Montenegro, della Bosnia Erzegovina, dell'Albania, del Marocco e dei Paesi Bassi. La finalità principale del seminario è stata quella di rafforzare ulteriormente la cooperazione transnazionale, portando a confronto sia le esperienze delle Autorità amministrative, di polizia e giudiziaria sia le esperienze delle realtà del mondo bancario/finanziario complessivamente impegnati nella prevenzione e contrasto al fenomeno della contraffazione monetaria.

61° Euro Counterfeiting Experts Group (ECEG/Olaf) Bruxelles (Belgio) 14 novembre2012

Il 14 novembre l'UCAMP ha partecipato al 61° meeting dell'Euro Counterfeiting Experts Group presieduto dal'Unità di protezione dell'Euro dell'OLAF. Nel corso del meeting sono stati tra l'altro presentati i risultati ottenuti dell'azione di formazione sviluppata dal Dipartimento del Tesoro, Direzione V, UCAMP a Dubrovnik in Croazia, nell'ambito del programma di formazione comunitario denominato "*Pericles*".

Training tecnico sulla lotta alla contraffazione dell'Euro
Mosca (Federazione Russa) 20/22 novembre 2012 - Programma *Pericles*

Su invito dell'Ufficio Centrale Italiano Falso Monetario - istituito presso il Dipartimento della Pubblica Sicurezza, Servizio Cooperazione Internazionale Forze di Polizia - l'UCAMP ha partecipato all'azione formativa promossa da quell'Ufficio interforze e tenutasi a Mosca nei giorni 20-22 novembre 2012, intervenendo sul tema del ruolo dell'Ufficio Centrale. Anche quest'azione è stata sviluppata dall'UCIFM nell'ambito del citato, noto programma di formazione comunitario "*Pericles*".

Carte 2012 - Roma 15/16 novembre 2012

Il 15 e 16 novembre l'UCAMP ha partecipato all'evento di riferimento per il mondo carte di pagamento organizzato a Roma dall'ABI - ***"Carte 2012"***. L'Ufficio ha illustrato alla qualificata platea il Sistema di prevenzione Sipaf - istituito presso il Ministero dell'Economia e delle Finanze, Dipartimento del Tesoro, Direzione V e gestito da UCAMP - che s'identifica nello strumento operativo, previsto dalla normativa italiana, attraverso il quale viene quotidianamente effettuata in maniera efficace la prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento.

Attività GIPAF

Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento

Il giorno 26 settembre si è tenuta la seduta plenaria del GIPAF durante la quale sono stati presentati i lavori svolti nei diversi sottogruppi (Rapporti statistici, Sviluppo tecnologico, Analisi Legislativa e Collegamenti Pubblico/Privato).
L'incontro ha consentito di affrontare le principali tematiche nei settori d'interesse, facendo registrare la numerosa ed attiva partecipazione degli esperti invitati.

Saluto al Dott. Francesco Carpenito

Si coglie l'occasione di questo numero della newsletter per salutare il Dott. Francesco Carpenito, il quale, come annunciato nella riunione del GIPAF sopra citata ha lasciato in data 14 ottobre 2012 l'incarico di Direttore dell'Ufficio VI/UCAMP, rivolgendo un caloroso saluto ai suoi collaboratori ed esprimendo il ringraziamento per la collaborazione fattiva ricevuta nei tre anni d'incarico. Si coglie l'occasione di questo numero della newsletter - una delle concrete iniziative avviate nel corso della gestione del Dott. Carpenito - per contraccambiare le espressioni di ringraziamento augurandogli per il futuro le migliori fortune professionali ed umane.

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

Via XX Settembre, 97
00187 – Roma
Tel. 0647610538
Web: http://www.dt.tesoro.it
e-mail: ucamp.carte@tesoro.it

ISSN .....