Phishing e cybericiclaggio: lo "stato dell'arte" nel panorama italiano

Gerardo Costabile e Francesco Cajani

L'informatizzazione della gestione dei conti correnti consente benefici tangibili per l'utenza ma richiede una maggiore attenzione alla tutela dei consumatori nell'ambiente virtuale. Fenomeni quali le frodi on line basate sul "furto d'identità" sono sempre più diffusi in Italia e, se è vero che l'anello debole della catena PC-uomo rimane purtroppo il secondo, non bisogna fare ricadere sull'utente tutti i rischi insiti nell'*home banking.

Banche, finanziarie, siti di aste on line, provider o, addirittura, l'ufficio delle imposte americano promettono maggiore sicurezza, ricchi gadget o un lauto risparmio di tasse per un'ipotetica casa a Miami, in cambio della "semplice" compilazione di un dettagliatissimo questionario, con tanto di dati bancari o carta di credito, per un "più veloce" accredito del promesso. L'estate 2006 è stata, per il secondo anno consecutivo, particolarmente calda, per una vertiginosa ascesa, su scala internazionale, dei casi di furto di informazioni delicate, come quelle bancarie e finanziarie, sfruttando Internet e la posta elettronica, oltre che una buona dose di ingegneria sociale. Infatti, se da un lato la maggiore informatizzazione degli strumenti di gestione del proprio conto corrente consente di evitare, con pochi click e seduti comodamente a casa propria, le inutili code del lunedì mattina, si evidenzia nel contempo un incremento di frodi on line basate sul furto di informazioni (come, per esempio, le password di accesso per le citate transazioni bancarie). Il tutto con un buon mix di tecniche psicologiche ed e-mail o siti civetta ben architettati, sfruttando contestualmente l'autorevolezza del falso mittente e una trasversale ignoranza dell'utenza media.

Quest'attività prende il nome di *phishing*, una nuova parola che si fa strada nel *mare magnum* di Internet. Parafrasando il verbo inglese *to fish* (pescare), è questa la nuova frontiera del furto d'identità e delle frodi on line, fuori e dentro la rete, metaterritorio dove si sono trasferiti parte degli ormai obsoleti tecnici fittizi marchiati Telecom o Enel o degli improvvisati marescialli della Guardia di Finanza, con tanto di tesserino falso, deputati alla riscossione del canone Rai ecc... Ma lo scopo è sempre quello: mettere le mani sui nostri soldi e, peggio ancora, sulla nostra identità personale.

A tale scopo vengono utilizzate affinate tecniche, per reperire, direttamente dall'interessato, informazioni personali sensibili o delicate, come numeri di conto

Gerardo Costabile
Member of "The International Association of Computer Investigative Specialists"
Francesco Cajani
Sostituto Procuratore presso il Tribunale Ordinario di Milano

corrente o password dei servizi di *home banking*, sfruttando metodi di ingegneria sociale e, quindi, senza sferrare un vero e proprio classico attacco informatico, tale da mettere in ginocchio il relativo server bancario. Il fenomeno in parola non è più solo di enorme attualità all'estero (ricordiamo che negli Usa il Senato ha già da due anni adottato uno specifico "*Anti-Phishing Act*", qualificando tali comportamenti come veri e propri crimini federali e, quindi, prevedendo fino a cinque anni di carcere per i cosiddetti *phisher*), ma ha avuto un vero e proprio boom anche in Italia, a partire dai primi mesi del 2005[1], con le prime e-mail in lingua inglese inviate indistintamente, utilizzando la nota tecnica di *spamming*[2], ai titolari di caselle di posta elettronica gestite da provider italiani.

Per meglio comprendere il fenomeno illecito, occorre ricordare come per il funzionamento della maggior parte dei servizi on line si è soliti far ricorso a una "accoppiata" composta da:

a) un "nome utente" o "*user-id*", dichiarazione esplicita della propria identità al sistema;
b) una password, ovvero quella porzione di informazione che solamente il soggetto e il sistema conoscono e che conferma, a ogni effetto, la dichiarazione di identità precedente, autorizzando alle funzioni e ai servizi che quella identità porta con sé.

In molti casi, nel tempo, la citata accoppiata è stata integrata da una o più credenziali ulteriori, al fine di creare un ingresso multilivello con più password, differenziando la prima (che consente una mera visualizzazione) dalle altre, cosiddette "dispositive", da utilizzarsi invece per i movimenti di denaro (a volte per scaglioni). In pochissime occasioni, e principalmente per gli utenti "business", vi sono altri sistemi di autenticazione, quali le "*one time password*", tramite dispositivi portatili similari a un portachiavi (in gergo definiti "*dongle*"). Questi, mediante un piccolo display a cristalli liquidi, definiscono, di volta in volta, password utilizzabili per una sola transazione. Tale metodo, come acclarato dalla comunità scientifica internazionale, può, allo stato dell'arte, dirsi il più affidabile nel settore dell'home banking, con un giusto compromesso per quanto concerne i costi (circa 5 euro cadauno), anche se negli ultimi mesi si sono registrate le prime avvisaglie di frodi "*in real time*" consumate in America, proprio velocizzando il bonifico in frode nell'arco del ristretto tempo del dispositivo in parola, comunicando a video all'utente informazioni non veritiere rispetto a quelle fraudolente in *background*.

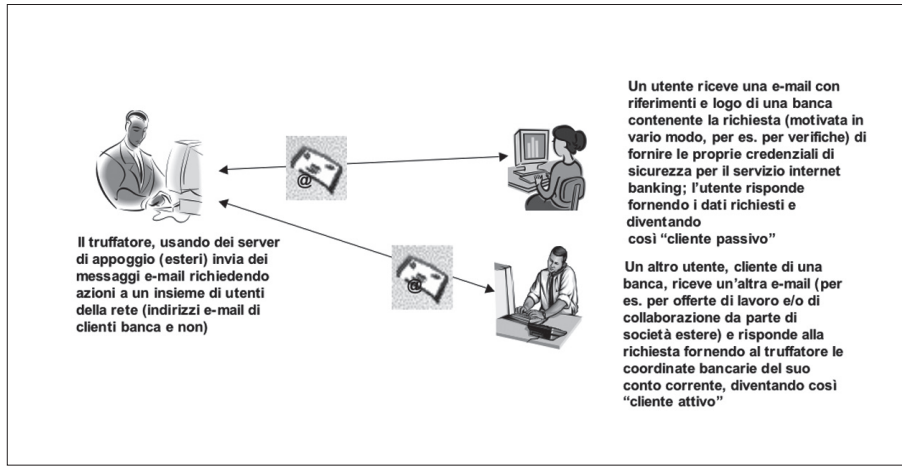
Come già accennato, il tentativo di forzare il sistema centrale contenente i dati relativi a migliaia di utenti è un compito arduo e quasi impossibile per la stragrande maggioranza dei pirati informatici. Risulta quindi molto più semplice attaccare i singoli clienti del servizio di *internet banking*, il vero anello

[1] La prima e-mail di phishing inerente a un istituto di credito italiano risale al 16.03.2005.
[2] Con tale modalità i relativi messaggi sono diretti a un numero elevato - allo stato indeterminabile - di soggetti, considerando le probabilità che una parte di essi sia effettivamente correntista dell'istituto di credito oggetto dell'attacco.

debole della sicurezza delle transazioni. Questo per un duplice motivo: innanzitutto, le tecnologie utilizzate rendono più semplice nascondere le proprie tracce ed evitare di essere rintracciati; in secondo luogo, l'utente medio non sempre possiede le capacità necessarie e per proteggersi da attacchi e per riconoscerli qualora si presentassero. In questo modo il pirata informatico, invece di attaccare un istituto di credito o un ente statale, e quindi affrontare parecchi livelli di sicurezza e di sistemi di rilevazione di effrazione digitale, si ritrova la strada sgombra nell'attacco del singolo individuo, normalmente privo anche delle più basilari tecnologie di protezione.

Come prima fase della truffa (Fig. 1) c'è la già ricordata azione tecnica e psicologica di *social engineering*, tesa alla raccolta di credenziali di autenticazione ai sistemi di home banking, direttamente nei confronti degli utenti finali. Si tratta, è bene precisarlo fin da subito, di attività posta in essere - per quanto risultante dalle indagini svolte su tutto il territorio nazionale[3] - da soggetti tutti operanti dall'estero.

Fig. 1 – L'acquisizione delle credenziali dei clienti



Le e-mail di phishing, all'inizio in inglese e successivamente in un italiano poco corretto, prendono come modello una reale comunicazione di servizio dell'istituto bancario, imitando alla perfezione non solo l'impostazione grafica del messaggio di posta elettronica, ma anche, con poco sforzo, il tenore linguistico e lessicale di una comunicazione standard, che l'utente finale è abituato a vedersi recapitare.

Tuttavia, cliccando sul *link* proposto nel corpo del testo, la pagina che viene caricata non è quella della banca, ma quella di un sito *Web*, creato ad arte per consentire al malintenzionato mittente di sottrarre e memorizzare le informazioni fornite da utenti ignari: informazioni riservate e confidenziali come la user id e la password sono così acquisite direttamente dall'attaccante.

[3] Reati ipotizzati: artt. 110, 81, 640 ter, 615 quater, 615 quinquies Codice Penale.

L'ipotesi investigativa che riconduce a un'unica mano l'azione criminale posta in essere dall'estero nello scorso anno è ribadita dalla circostanza che, negli ultimi mesi del 2005, si sono registrati attacchi di phishing che vedevano coinvolti insieme più istituti di credito.

Nella Fig. 2 sono riportate alcune e-mail tipo (prive del riferimento agli istituti di volta in volta attaccati) che sono state utilizzate per lo scopo.

Fig. 2 – Esempi di e-mail di phishing

From: Banca XXXXXX (*mittente_fasullo@bancaxxxxxxx.it*)
To: *utente_destinatario@nomedominio*
Subject: Banca xxxxxxx: email - *utente_destinatario@nomedominio*

Dear Banca xxxxxxx Customer,
We find that some of our members no longer have access to their email addresses. As result Banca xxxxxxx server sent this letter to verify e-mail addresses of our clients. You must complete this process by clicking on the link below and entering in the small window your Banca xxxxx bank online access details:

http://www.una-banca-a-caso.it

From: Banca XXXXXX (*mittente_fasullo@bancaxxxxxxx.it*)
To: *utente_destinatario@nomedominio*
Subject: Banca xxxxxxx: email - *utente_destinatario@nomedominio*

Caro cliente,
Banca xxxxxx vi rimborsa per la vostra fedelta con 100 Euro. Prima di usare questo importo, dovete seguire il collegamento e usare il vostro Codice cliente e Codice segreto. Un operatore si mettera in contacto con voi per confermare l'importo.

http://www.una-banca-a-caso.it

From: Banca XXXXXX (*mittente_fasullo@bancaxxxxxxx.it*)
To: *utente_destinatario@nomedominio*
Subject: Banca xxxxxxx: email - *utente_destinatario@nomedominio*

"Siamo spiacenti di anonciare che negli ultimi giorni hackers hanno trasmesso fraudolenti email chiedono le parole d'accesso dei nostri clienti. D'ora in poi una nuova misura di sicurezza sara' attivata. Tutti i clienti sono sospesi. Per riattivare il vostro cliente dovete seguire il collegamento e fornirci nuove informazioni di sicurezza per verifica soltanto".

http://www.una-banca-a-caso.it

La casistica comprende tuttavia altre ipotesi, qui sintetizzate:

- e-mail che invita ad accedere al sito della banca per ottenere il nuovo pin di sicurezza;
- e-mail contenente un avviso di addebito in conto di un importo non indifferente, per l'acquisto - per esempio - di un PC: maggiori dettagli il destinatario

li può trovare nel sito indicato nella e-mail, per accedere al quale vengono poi richieste la user-id e la password, in modo da poterle catturare;
– e-mail che invita ad accedere al sito della banca proprio perché fantomatici phisher avrebbero attentato alla sicurezza del conto corrente del cliente: il destinatario, accedendo al sito, riceve sul computer un programma "*trojan*"[4] che si mette in "ascolto" e provvede a raccogliere i dati digitati dal cliente sul suo PC e, successivamente, a inviarli all'hacker o a una banda criminale.

Proprio quest'ultima fenomenologia ci fa comprendere come il fenomeno illecito si stia aggravando, perché, negli ultimi mesi, le e-mail di phishing lasciano sempre più spesso il posto ai *malware*[5], utilizzati per carpire informazioni riservate sui conti bancari o per dirottare gli utenti a veri e propri siti clone al momento della digitazione del sito della propria banca (cosiddetta tecnica di *hijacking*[6]).

Sono infatti in costante aumento gli utenti che, pur non avendo risposto ad alcuna e-mail, sono stati vittime di bonifici on line in frode proprio a causa dell'utilizzo (per operazioni di home banking) di computer infetti.

Questo spiega altresì come esistano correntisti di istituti di credito non oggetto di attacchi di phishing[7] che abbiano comunque lamentato un danno a seguito di bonifici on line in frode.

Successivamente all'acquisizione delle credenziali e alla possibilità per il phisher di disporre bonifici on line in frode, nasce il problema di come incassare le relative somme (dal momento che il sistema dell'home banking italiano non consente bonifici verso l'estero, se non tramite ulteriori controlli da parte degli istituti bancari). Su scala internazionale, ormai, il sistema è abbastanza rodato: quasi contemporaneamente all'invio delle e-mail di phishing, si registra una richiesta, preferibilmente sempre veicolata via posta elettronica, di collaborazione indirizzata a cittadini italiani o comunque residenti in Italia.

Sotto quest'ultimo profilo, si è rilevata anche nel panorama italiano una proliferazione di fantomatiche[8] società estere che inviano messaggi di posta elettronica, sempre con la medesima tecnica di spamming, del tenore di quello riportato di seguito (Fig. 3).

[4] Il termine si dice sia stato coniato dall'hacker Dan Edwards e si rifà alla mitologia greca: al cavallo diTtroia. Infatti agli inizi si trattava di programmi che si spacciavano per giochi o upgrades *ma che in realtà nascondevano altre nefandezze. In generale, un trojan è un virus che viene mascherato all'interno di un'applicazione apparentemente inoffensiva.*
[5] "Malware" è un neologismo nato dalla fusione di "malicious" e "software." Questi programmi, in particolar modo, non sono utilizzati per danneggiare il personal computer, ma per accedere al sistema della vittima o, peggio ancora, registrare le informazioni riservate, quali password e dati delle carte di credito.
[6] Dirottamento del browser, finalizzato generalmente a condurre il navigatore su un sito diverso rispetto a quello digitato sulla barra di navigazione.
[7] I casi italiani di e-mail di phishing (con i relativi istituti interessati) sono tutti recensiti dal sito www.anti-phishing.it .
[8] I primi accertamenti di Polizia Giudiziaria hanno infatti riscontrato la natura fittizia delle stesse, desunta da numerosi indizi concordanti (quali, tra l'altro, l'utilizzo di proxy *per l'invio di e-mail e l'intestazione dei siti Internet indicati a nomi del tutto estranei ai fatti).*

Fig. 3 – Esempi di e-mail di reclutamento di financial manager

PLATINWAY CORP

- Ha sempre sognato di diventare manager di una società ed avere una buona paga? Noi possiamo aiutar La a realizzare il Suo sogno offrendo Gli un profitto sicuro, stabile che riceve ogni mese lavorando su Internet.

Lei ci chiede: ma perché proprio noi? Ma è tutto molto semplice! Sicuramente è già stufo dei costanti problemi con la mancanza dei soldi sia per il pagamento dei conti a catena, che per una casa nuova, o magari vuole che i Suoi figli abbaino la possibilità di studiare in all'università prestigiosa?

O forse è già da tempo che sogna di una nuova automobile?

Si ricordi le parole di Pitagora: "Non fermatevi là dove siete arrivati", dopo tutto quello che Le serve per poter lavorare con noi è:

- essere residente in Italia
- avere un conto bancario in una banca
- avere un computer collegato alla rete globale
- possedere un po' di tempo libero
- e, naturalmente, il desiderio di fare questo lavoro.

Il Suo lavoro sarà facile e piacevole, e soprattutto REDDITIZIO! La nostra società prenderà cura della Sua prosperità. Si registri gratis per scoprire nuove possibilità di lavoro su Internet.

Cambi la Sua vita in meglio insieme a Platinway Corp.

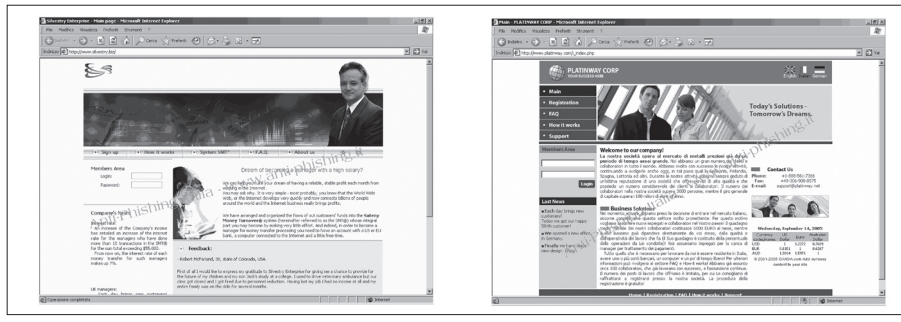
URL: http://www.platinway.com/
E-Mail: support@platinway.net

© Copyright 2005 **PLATINWAY CORP.** All rights reserved.

Tuttavia l'invio di e-mail (per di più con sofisticate tecniche in grado di eludere anche filtri *antispam*) non costituisce l'unico modo utilizzato per instaurare un primo contatto con i soggetti che saranno poi utilizzati come *financial manager*, in quanto le stesse fantomatiche società si avvalgono anche di contatti via ICQ (o altri canali di chat) nonché di inserzioni su siti Internet specializzati (es. Monster) in offerte di lavoro.

Molte di queste fantomatiche società hanno anche allestito un sito Internet (con sezioni in italiano, come quello della Fig. 4) per rendere ancora più credibile, sotto il profilo della liceità di quanto offerto, la loro azione.

Fig. 4 – Pagine Web



Tramite tali siti è altresì possibile stampare la documentazione relativa a fantomatici contratti di collaborazione nonché ricevere ulteriori informazioni, sintetizzate (nel caso della Platinway Corp) in alcune FAQ (Risposte alla più frequenti domande) riportate nella Fig. 5. Si noti come, dopo aver allettato l'utente

con un lavoro semplice e redditizio, i truffatori cerchino di spaventarlo così da convincerlo anche sulla serietà e validità della relativa società.

Fig. 5 – Estrapolazione di alcune FAQ della società di reclutamento Platinway

- **Quale sarà l'interesse che riceverò?**
Questo dipende dalla velocità e qualità del lavoro che Lei fa. Di base è del 7% con la copertura da parte nostra di tutte le spese per la spedizione del denaro. Più proficuo è il Suo lavoro, più alto sarà l'interesse che riceve!

- **Con che tipo di somme dovrò lavorare?**
Lei opererà con le somme dai 500 EURO fino ai 10.000 EURO (vale per i collaboratori professionali)

- **Perché nel contratto è necessario indicare TAN?**
Questo è fatto con lo scopo di proteggere le nostre attività dalle operazioni truffaldine ed anche per impedire ai tentativi di appropriarsi dei nostri capitali

- **Che cosa succede nel caso se io non vi mando il denaro necessario e me lo lascio?**
Tutta l'informazione su di Lei sarà immediatamente comunicata al FBI, o all'Interpol o ad altre organizzazioni con le quali abbiamo la stretta collaborazione.

Si rimanda (anche per la visualizzazione delle relative pagine, molte delle quali non più disponibili su Internet a seguito di interventi delle Autorità giudiziarie competenti) all'archivio truffe *on line* del sito di Anti-Phishing Italia (*http://www.antiphishing.it/archivio/false.societa.php*) dal quale provengono le due immagini qui riprodotte e da cui abbiamo anche tratto l'elenco delle società coinvolte (aggiornato al febbraio 2006) riportato nella Fig. 6.

Fig. 6 – Elenco delle società di reclutamento di finalcial manager

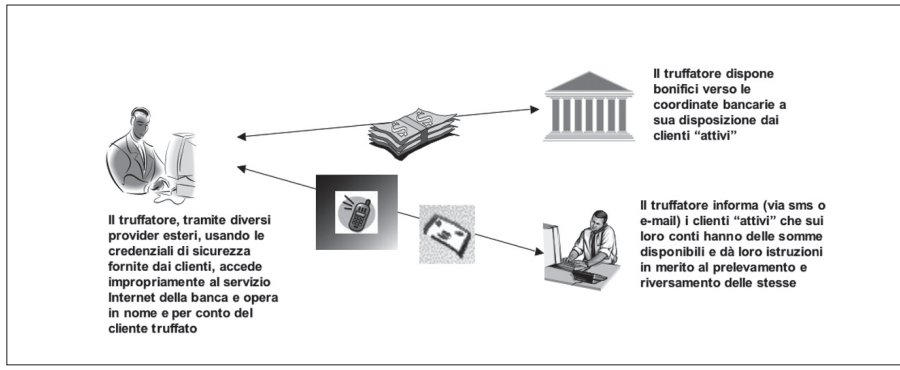
Nome società	Data di rilevazione	Lingua utilizzata
ADWARE INC	20-Oct-05	Ingl.
Applied Cash International	27-Oct-05	Ingl.
AQuantive INC	28-Oct-05	Ingl.
AROMATIC FOODS LIMITED	29-Oct-05	Ingl.
BaliseMotor Inc.	3-Feb-06	Ingl.
Baltic Finance Group Inc	23-Sep-05	Ingl.
Clarke Thomas Inc.	10-Feb-06	Ingl.
CoralAir Inc	24-Aug-05	Ingl.
Creative Finance Centre	1-Nov-05	Ingl.
davidalistair@davidalistair.ws	30-Oct-05	Ingl.
Des-igretest.com	23-Feb-06	Ingl.
Dickson Kenington's Arts	1-Nov-05	Ingl.
Digicreator	18-Aug-05	Ingl.
Digitals Planet Co.	4-Oct-05	Ingl.
Docindutry Finance Group	31-Oct-05	Ingl.
ECO LIFE COMPANY	18-Oct-05	Ingl.
EUROPE SELLS LTD	27-May-05	Ingl.
F.F.E Group	26-Oct-05	Ingl.-Ita.
Finance Mover INC.	20-Aug-05	Ingl.
Finance Services Company (f-services.net)	10-Oct-05	Ita.
Financial Service Inc.	15-Oct-05	Ingl.
FinServices	15-Dec-05	Ingl.
Firebird Private Equity Ltd	18-Oct-05	Ingl.
firstagencymail@aol.com	8-Nov-05	Ingl.
GERNIUS LLC	20-Oct-05	Ingl.
H & L LIMITED	26-Oct-05	Ingl.
infoleechanholdings @takemail.com	2-Nov-05	Ingl.
IRG "Italy Representative Group"	25-Oct-05	Ingl.
irwinghighland.com	17-Oct-05	Ingl.
italy@euroimperials.biz	18-Nov-05	Ingl.
italy@euroimperials.com	2-Nov-05	Ingl.

Nome società	Data di rilevazione	Lingua utilizzata
italyctc@aol.com	9-Feb-05	Ingl.
itvacancyfree@aol.com	20-Sep-05	Ingl.
Kemper Isurance Companies	27-Oct-05	Ingl.
Legal PCS Group - PCSGroup@aol.com	13-Nov-05	Ita.
LOOKJOB@AOL.COM	18-Oct-05	Ingl.
manager@des-integratst.com	1-Feb-06	Ingl.
Market Bonds	30-Jun-05	Ingl.
Microlinks Inc.	15-Oct-05	Ingl.
Miratek Investments	22-Nov-05	Ingl.
Multipay Gateway Corporation	13-Oct-05	Ita.-Fran.
Platinway	14-Sep-05	Ita.- Ingl.
Prompt Insurance	19-Oct-05	Ingl.
psa-4u.com	27-Jan-06	Ingl.
PURE ARTS GROUP	7-Jul-05	Ingl.
Rusromance	30-Jun-05	Ita.
Safe Sales Inc.	21-Nov-05	Ita.
Sateny	6-Sep-05	Ita.
Silvestry Enterprise	14-Sep-05	Ingl.- Ita.(?)
Solid Job Company	26-Oct-05	Ingl.
SOSA FABRICS LIMITED	3-Nov-05	Ingl.
Star Pay S.A	10-Feb-06	Ingl.
SYIGENTA VIETNAM LIMITED	3-Nov-05	Ingl.
Swiport Inc.	29-Sep-05	Ita.- Ingl.(?)
THERUSMARKET Investment	17-Oct-05	Ingl.
Trinity Financial Services	2-Nov-05	Ingl.
TrustBizJob	6-Oct-05	Ingl.
Web Click Company	18-Jan-06	Ingl.
WORLDEXCHANGE	Data n.d.	Ingl.
XMEDIABUILD	Data n.d.	Ingl.
You can work 30 mins per day and earn $1000's	1-Jan-06	Ingl.

Una volta accettata l'offerta di lavoro, ai collaboratori viene richiesto di comunicare le coordinate del proprio conto corrente, in quanto l'attività richiesta consisterà proprio nel prelevare le somme di denaro, di volta in volta accreditate su tali conti (e apparentemente provenienti da clienti di tali società, che però altro non sono che i correntisti frodati), al fine di ritrasferirle all'estero.

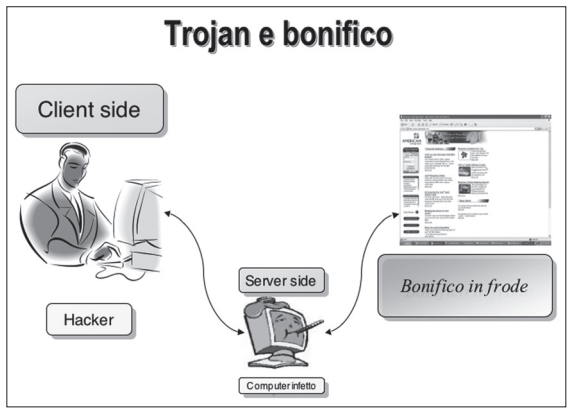
La prospettata attività (lecita) di *financial manager* costituisce in realtà l'anello per far pervenire agli autori della truffa i relativi proventi.

Fig. 7 – L'accesso fraudolento via Internet Banking ai conti dei clienti



Ottenuta così anche la disponibilità attiva di soggetti italiani o comunque residenti in Italia, la seconda fase della truffa (Fig. 7) è quindi volta a sottrarre i soldi dal conto corrente del quale si sono fraudolentemente acquisite le credenziali di accesso, attraverso bonifici disposti a favore del conto corrente comunicato al phisher dal financial manager.

Fig. 8 – Rappresentazione grafica dell'uso di zombie da parte del fondatore

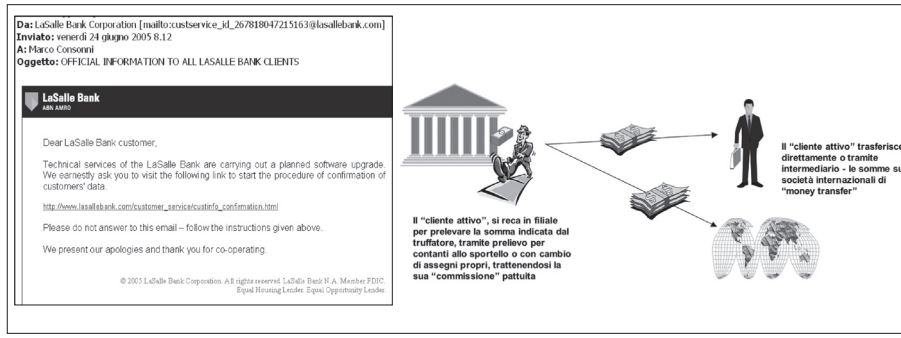


Tali bonifici on line vengono materialmente effettuati tramite operazioni partite principalmente da personal computer allocati in gran parte all'estero ma anche in Italia, quasi certamente appartenenti a una rete di macchine compromesse (in gergo *zombie*[9]), in danno degli ignari titolari dei rispettivi conti ordinanti (Fig. 8).

[9] Uno zombie è un computer che è stato infettato con del codice maligno, in attesa di essere attivato. Quando viene attivato, insieme agli altri zombie, può essere utilizzato per lanciare un attacco verso un sito web, un altro computer che gli è stato indicato, oppure, nel caso di illeciti on line, per effettuare disposizioni di bonifici in frode non direttamente dalla propria postazione.

A riprova di questo, un sequestro di un personal computer di un soggetto italiano apparentemente ordinante (tramite il proprio indirizzo IP[10]) di un bonifico in frode ha consentito di confermare - grazie alla *computer forensics* effettuata sulla macchina - la presenza di circa 130 trojan, con il risultato che (proprio per l'effetto di tali virus) tale PC veniva amministrato da remoto (senza che l'utente se ne potesse rendere conto) al fine di operare i bonifici in frode e inviare *spam* per catturare le credenziali di una banca estera (in USA) utilizzando un messaggio come quello riportato di seguito (Fig. 9).

Fig. 9 – Esempio di phishing ai danni dei clienti di una banca americana



La terza fase della truffa consiste nel sollecitare il financial manager al trasferimento delle relative somme, fornendo di volta in volta le indicazioni necessarie ma comunque sempre tramite servizi di *money transfer* (*Western Union* o *Money Gram*), previa trattenuta di un compenso oscillante tra il 5% e il 10% delle somme inviate.

La condotta di questi ultimi rientra senza ombra di dubbio nella nozione di trasferimento di risorse provenienti da un'attività illecita da parte di soggetto estraneo alla commissione del reato presupposto, così come prevista e sanzionata dall'articolo 648 bis del Codice Penale (riciclaggio di denaro).

Ad acclarare tale posizione è la stessa Banca d'Italia, la quale, recentemente, ha definito formalmente il phishing una "anomalia rilevante ai sensi delle Istruzioni operative della Banca d'Italia per l'individuazione delle operazioni sospette (cosiddetto "decalogo antiriciclaggio[11]") ai fini antiriciclaggio".

Sul punto si registra l'importante Comunicazione dell'Ufficio Italiano Cambi del 28 marzo 2006[12] (il cui testo integrale è reperibile sul sito *www.uic.it* nella sezione antiriciclaggio) nella quale, tra l'altro, si legge:

[10] Indirizzo numerico di un computer sulla rete Internet.
[11] Provvedimento del 12.1.2001 recante "Istruzioni operative per l'individuazione di operazioni sospette".
[12] Tale comunicazione è stata indirizzata ai seguenti soggetti: Associazione Bancaria Italiana, Federazione Italiana delle Banche di Credito Cooperativo Casse Rurali ed Artigiane, Associazione fra le Banche Estere in Italia, Poste Italiane S.p.a, Esercenti attività di Money Transfer.

"In considerazione della rilevanza del fenomeno, che ha coinvolto numerosi utenti e ha determinato la sottrazione di importi complessivamente ingenti, si ritiene ragionevole richiedere la collaborazione attiva degli intermediari con riferimento al fenomeno del phishing.

A fini di un adeguato monitoraggio dell'operatività della clientela e per la segnalazione di operazioni sospette, si elencano di seguito gli indicatori di anomalia relativi all'operatività degli utenti attivi con riferimento alle tipologie di intermediari coinvolti nella frode informatica.

È opportuno che le banche e le Poste Italiane prestino particolare attenzione:

- *all'alimentazione dei rapporti tramite bonifici on line che presentano le seguenti caratteristiche:*
  - *provengono da ordinanti diversi dai titolari dei rapporti,*
  - *sono accreditati nel medesimo giorno in un intervallo di tempo ristretto,*
  - *presentano singolarmente un importo inferiore alla soglia di registrazione,*
  - *non appaiono coerenti con l'attività svolta dal cliente;*
- *a operazioni di prelevamento di contanti in stretta successione temporale rispetto all'accredito dei bonifici;*
- *all'utilizzazione di rapporti, anche di recente apertura, unicamente per l'esecuzione di operazioni della specie;*
- *all'accredito di bonifici riconducibili ai clienti che hanno dichiarato la cessione delle proprie credenziali o un tentativo di furto della propria identità elettronica.*

Si potrà ottenere immediata discriminazione, ai fini del monitoraggio, identificando i bonifici effettuati tramite il proprio canale home banking o provenienti da banche che operano esclusivamente on line.

È opportuno che gli esercenti attività di money transfer prestino attenzione:

- *a clienti che inviano denaro a numerose controparti localizzate in Paesi dell'Europa dell'Est e, in particolare, a quei clienti che nello stesso giorno effettuano più trasferimenti di importo frazionato in favore della stessa persona o di più persone;*
- *a clienti stranieri che, in assenza di plausibili motivazioni, inviano denaro a controparti dislocate in Stati diversi da quelli di origine;*
- *ai beneficiari localizzati in Paesi dell'Europa dell'Est che risultano ricevere molteplici trasferimenti, in un arco temporale limitato, provenienti da differenti città italiane (questa anomalia è rilevabile dagli intermediari che gestiscono le reti di money transfer).*

Si specifica che l'attività di monitoraggio e prevenzione da parte degli intermediari è indirizzata a tutte le modalità di furto di identità elettronica di cui il phishing costituisce solo una delle possibili forme.

Tanto si rappresenta perché i soggetti tenuti all'obbligo della segnalazione di operazioni sospette siano informati, con le modalità più idonee, anche in considerazione della necessaria riservatezza".

La ricordata comunicazione dell'Ufficio Italiano Cambi sembra intervenire a censurare la gravità del fenomeno (relativo alla contestata condotta di riciclaggio), tenuto conto che ogni bonifico illecitamente disposto si attesta intorno ai 5.000,00 euro e che, allo sportello bancario, vengono chieste anche somme (provenienti da più bonifici on line disposti a distanza di pochi secondi uno dall'altro) complessivamente superiori alle soglie previste dalla normativa antiriciclaggio.

Sotto questo punto di vista, i casi più significativi finora registrati (che rendono appieno l'idea del fenomeno) sono stati:

- 3 bonifici on line da 12.000,00 euro cadauno, illecitamente disposti alle ore 9.17.25, 9.18.03, 9.18.35: il cliente beneficiario, alle ore 10.09 della medesima giornata, prelevava 32.400,00 euro per contanti allo sportello;
- 4 bonifici on line da 5.000,00 euro cadauno, illecitamente disposti alle ore 9.38.04, 9.39.57, 9.40.20 e 9.40.42: il cliente, alle ore 15.39 della medesima giornata, prelevava 18.000,00 euro allo sportello con assegno.

Entrambi i casi citati riguardavano per di più bonifici on line relativi allo stesso istituto di credito (quanto a conto ordinante e conto beneficiario), con maggiore possibilità di controllo allo sportello della provenienza illecita delle somme.

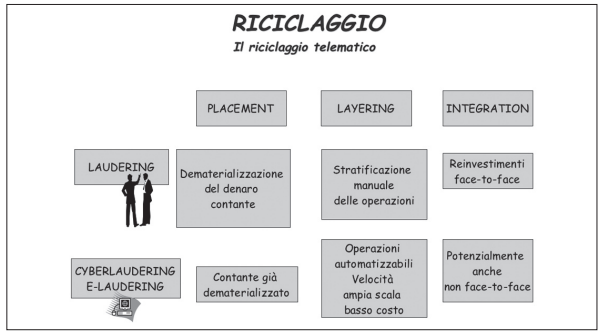
Il fenomeno non deve quindi essere sottovalutato, né dai correntisti né tantomeno dagli istituti di credito interessati: basti pensare che nel gennaio di quest'anno sono stati arrestati a Milano due soggetti di apparente nazionalità lettone, venuti appositamente in Italia - transitando per la Spagna (dove avevano compiuto un'identica attività illecita) - con documenti d'identità falsi, al fine di aprire numerosi conti correnti bancari da utilizzare come "appoggio" per l'attività illecita. Tali soggetti erano, tra l'altro, in possesso di documentazione costitutiva di una delle fantomatiche società estere utilizzate per fornire un'apparente liceità nella ricerca dei financial manager.

Più in generale, a fornire le stime sui progressi del *cybercrime* (che già a partire dall'anno scorso ha battuto i proventi ottenuti dalla vendita di sostanze illecite come eroina e cocaina) è stata Valerie McNiven, durante un convegno sulla sicurezza informatica nel settore bancario tenuto a Riyadh, Arabia Saudita, nei mesi scorsi: "Il *cybercrime* si evolve ad una velocità talmente elevata che la legge non riesce a tenere il suo passo", ha dichiarato la consulente del governo americano per il cybercrime, secondo la quale lo sviluppo tecnologico in crescita nei paesi in via di sviluppo porterà a un aumento delle truffe che, a oggi, vantano un "fatturato" superiore ai 150 miliardi di dollari[13]. Infatti, la problematica di interesse con le nuove tecnologie è relativa alla facile dematerializzazione delle somme frodate, alla velocità di automatizzare le operazioni

[13] *Fonte: The Register* - http://www.theregister.co.uk/2005/11/29/cybercrime/.

con costi relativamente bassi, distraendo gli investigatori sulle azioni in essere da soggetti italiani, integrando i capitali illeciti all'estero (Fig. 10).

Fig. 10 – Le varie fasi del riciclaggio e del cybericiclaggio



Cosa fare, dunque? Su sollecitazione delle Autorità giudiziarie, è stato predisposto dall'ABI un decalogo *antiphishing* per i correntisti, che si riporta integralmente

"1. Diffidate di qualunque mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali. La vostra banca non richiederà tali informazioni via email.
2. È possibile riconoscere le truffe via e-mail con qualche piccola attenzione; generalmente queste e-mail:
- *non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);*
- *fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;*
- *promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione;*
- *non riportano una data di scadenza per l'invio delle informazioni.*

3. Nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca tramite il call center o recandovi in filiale.
4. Non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate. Diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @.

5. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto. In proposito si sottolinea la necessità di stabilire l'autenticità della connessione sicura facendo doppio click sul lucchetto in basso a destra e verificando la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale.
6. Diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop up (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca tramite il call center o recandovi in filiale.
7. Controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito.
8. Le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (cosiddette patch) che incrementano la sicurezza di questi programmi. Sui siti di queste aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.
9. Sia le e-mail che i siti di phishing tentano spesso di installare sul computer della vittima codice malevolo atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Si può impedire tale operazione tenendo sempre aggiornato il software anti-virus presente sul proprio computer.
10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo.
In caso di dubbio, rivolgetevi alla vostra banca!"

Se è vero che la potenzialità distruttiva di tale tipo di frode si basa sull'induzione in errore del correntista, è logica conseguenza che una maggiore attenzione dello stesso sarebbe di per sé idonea a contrastare in radice il problema, anche se - come sottolineato dalla richiamata comunicazione dell'Ufficio Italiano Cambi - i controlli degli istituti di credito meriterebbero una maggior incisività, poiché non pare opportuno far ricadere completamente sull'utente i rischi insiti nel sistema dell'home banking, dal momento in cui gli stessi sono ben conosciuti dagli istituti di credito (che sicuramente hanno maggiori mezzi e conoscenze tecniche per prevenirli).

Più in generale, il cliente dovrebbe essere considerato nell'alveo della cosiddetta *chain of security*, e non esclusivamente fuori rispetto al perimetro di tutela aziendale. La sicurezza del cliente è di certo una risorsa per tutto il sistema e

addirittura può rivelarsi quella vera risorsa di marketing in un settore delicato dove si cerca senza indugio la *business security*. Purtroppo, secondo qualcuno, il phishing e il furto di identità digitale sono una problematica squisitamente tecnica, da "approccio informatico" alla sicurezza. Ma siamo sicuri che sia un'impostazione corretta? È opinione di chi scrive, infatti, che è necessario un approccio più strutturato nelle varie strutture aziendali coinvolte, con un metodo simile a quello impostato per il *crisis management*.

Da un lato, quindi, il metodo migliore è quello di incrementare e ottimizzare il rapporto con il cliente, sia tramite il sito Web sia con strumenti tradizionali, senza sottovalutare il fenomeno. Contestualmente, invece, dovranno essere curate tutte le fasi del processo, compresa una maggiore consapevolezza degli "avamposti della frode", ovvero gli sportelli al pubblico dove si monetizzano (almeno per il momento) le somme di denaro.

La fase preventiva potrà vedere in primo piano una maggiore sensibilizzazione dell'utente sull'ambito della sicurezza informatica e in particolare l'indicazione su possibili strumenti di sicurezza da adottare in casa. Contestualmente dovranno essere studiate, nei tempi opportuni, quelle sofisticazioni degli accessi ai servizi di home banking (ma non solo) tramite l'utilizzo, per esempio, di autenticazione forte, con strumenti che generino una password diversa a ogni utilizzo.

Allo stesso modo pare sempre più opportuno certificare o stigmatizzare i canali di comunicazione tra cliente e istituti di credito, o comunque stabilire delle procedure chiare e trasparenti sulle modalità di comunicazione in parola. Si sono registrati casi, infatti, di e-mail istituzionali che avvertivano del pericolo phishing usando lo stesso metodo (e lo stesso linguaggio) dei frodatori, rischiando alla fine di indurre in errore l'utente medio nell'identificazione dei messaggi di posta elettronica ricevuti.

Solo in questo modo, infatti, i vari "mattoni" potranno consentire di innalzare quel muro di protezione per i clienti e per il sistema, tentando di conseguenza di ridurre gli impatti dei tentativi di frode on line.