CONVEGNO 2 MARZO
9:30 / 13:30

L'EUROPA
TRA CRIMINI INFORMATICI E SICUREZZA DEI DATI PERSONALI

"Università della Tuscia"
Auditorium
Via Santa Maria in Gradi (Viterbo)

INTERVENTO

ASPETTI DEL CYBERCRIMINE LEGATI AL PHISHING

(Ing. ALOIA ROBERTO)

INDICE

1. COS'E' IL PHISHING

1.1 Introduzione

Il termine ***phishing*** secondo alcuni deriva dalla storpiatura del verbo inglese ***to fish*** che significa pescare, in effetti lo scopo di questa tecnica è quella di pescare utenti in rete per farli cadere in trappole tese da truffatori.

L'attacco generalmente avviene tramite e-mail e si basa sull'invio, da parte di un utente malintenzionato di messaggi che sembrano provenire da siti web autentici o noti, i quali richiedono all'utente ingenuo l'inserimento di informazioni personali.

Ovviamente lo scopo, che sta alla base di questa attività, è il lucro e per essere più precisi il furto di denaro perpetrato ai danni di utenti ignari.

Di recente, i casi di phishing hanno avuto una vittima ben precisa: l'home banking[1], ovvero le carte di credito, i conti correnti on-line, i codici relativi a depositi effettuati in noti istituti di credito.

Ma come è possibile riuscire a rubare denaro attraverso il phishing?

La tecnica utilizzata per colpire gli utenti italiani attraverso il phishing è stata, sinora, quella di inviare un'e-mail (a volte si utilizzano anche le finestre a comparsa) apparentemente proveniente dal proprio istituto di credito (Banca Intesa, Unicredit, Banca di Credito Cooperativo, Poste Italiane i casi più frequentemente riscontrati) con cui si informa l'utente che, a causa di problemi tecnici, è necessario collegarsi al nuovo sito, entrare nella sezione riservata al proprio conto e compilare un apposito form[2].

Nella suddetta e-mail, il link indirizza verso un sito (praticamente identico a quello originale) utilizzato come esca per far abboccare gli utenti ignari. In seguito i dati e le informazioni carpite verranno utilizzate nei modi più svariati.

Perché il phishing è subdolo?

E' subdolo perchè sfrutta l'ingenuità e l'ignoranza degli utenti. Il messaggio di posta elettronica del phisher è generalmente scritto in un pessimo italiano (probabilmente i nostri malfattori ancora non utilizzano questa tecnica), con gli accenti sbagliati, con verbi coniugati male.

Per questi motivi, un utente accorto non avrebbe nessun problema a riconoscere la frode e denunciarla almeno sui siti di interesse o blog attivi in tutto il mondo Internet.

Sotto il profilo tecnico è opportuno adottare ulteriori accorgimenti e seguire questi brevi suggerimenti per non cadere in trappola. Nel momento in cui l'e-mail phishing viene ricevuta occorre notare ambiguità letterali (come detto in precedenza) ed analizzare attentamente il link[3] che viene proposto. Quest'ultimo di solito varia dall'originale per qualche carattere (p.es. nel caso di Unicredit Bank, c'era una sola "s" di differenza) o nei casi molto grossolani, è un indirizzo molto strano.

[1] Servizio bancario con il quale l'utente (tramite collegamento telematico) può effettuare da casa operazioni quali ordini di pagamento, richieste assegni, ricevere informazioni relative al suo conto, ecc…
[2] È un modulo contenuto in una pagina Internet e viene utilizzato per richiedere informazioni al visitatore.
[3] Collegamento tra due pagine web (all'interno dello stesso sito, ma anche tra pagine contenute in due siti differenti).

1.2 Come comportarsi nei casi di attacco

Negli ultimi mesi Internet Explorer non ha aiutato molto gli utenti a scovare un eventuale tentativo di phishing, questo perché un errore di gestione degli indirizzi Web permetteva di visualizzare nella barra degli indirizzi[4], ed anche in quella di stato, l'indirizzo web autentico del sito contraffatto anche se in realtà si veniva re-indirizzati su di un sito clone[5].

Il modo di difenderci da queste truffe consiste in:

- Non fornire nessun tipo di dati personali tramite e-mail.
  Aziende importanti come PayPal, Ebay, Poste Italiane, Microsoft non vi chiederanno mai di fornirgli tramite e-mail i vostri dati personali (account, password o numeri di carta di credito);

- Visitare i siti Web digitandone il rispettivo URL[6] nella barra degli indirizzi.
  Non aprite mai direttamente il link che vi forniscono le e-mail phishing poiché indirizzano su server non ufficiali;

- Verificare che il sito Web utilizzi la crittografia.
  In Internet Explorer potete farlo controllando che sulla barra di stato sia presente l'icona del lucchetto giallo (in basso a destra). Facendo doppio clic sull'icona del lucchetto è possibile visualizzare il certificato di protezione del sito. Il nome che segue "**Rilasciato a**" dovrebbe corrispondere al sito in cui pensate di trovarvi. Se il nome è diverso, il sito potrebbe essere contraffatto;

- Esaminare regolarmente i rendiconti bancari e della carta di credito.
  Se controllate il rendiconto della vostra banca e della carta di credito almeno una volta al mese, potrete riuscire a bloccare una frode prima che provochi danni rilevanti.

- Aggiornare il software.
  Le ultime versioni di Internet Explorer non consentono più di contraffare l'URL nella barra degli indirizzi (esistono anche browser alternativi, quali Firefox, che ultimamente si sono affacciati sul mercato come sostituti del prodotto di casa Microsoft ed hanno mirato sulla sicurezza).
  Per quanto riguarda i computer con sistemi operativi Windows, è consigliato aggiornare regolarmente il vostro sistema tramite Windows Update.

[4] Porzione del browser (parte alta = barra degli indirizzi , parte bassa = barra di stato), laddove vengono visualizzati gli indirizzi dei link da raggiungere.
[5] Copia perfetta di un sito ufficiale (p.es Poste Italiane) ospitato su un altro server allo scopo di ingannare l'utente.
[6] Uniform Resource Locator: è l'indirizzo di un sito Internet (p.es. www.google.it).

- Essere cauti e sospettosi.
  Se ritenete di aver ricevuto un e-mail sospetta è consigliato, innanzitutto, verificare la sua eventuale presenza all'interno di un sito che tratta del phishing (p.es. **http://www.anti-phishing.it**); il passo successivo è quello di denunciare immediatamente la frode all'azienda contraffatta, stando attenti a non utilizzare i collegamenti presenti all'interno dell'e-mail ricevuta.
  Inoltre, è buona norma fornire dettagli della frode alla polizia tramite l'Internet Fraud Complaint Center[7]. Il centro opera in tutto il mondo in collaborazione con le forze di polizia e i partners del settore, per chiudere tempestivamente i siti contraffatti e individuare gli autori della frode.
  Se ritenete che le vostre informazioni personali siano state compromesse o rubate, dovreste esporre denuncia al Federal Trade Commission[8].

- Fare una telefonata.
  Forse il metodo più banale e il più vecchio per controllare se il nostro istituto di credito ha veramente richiesto queste informazioni, è telefonare e chiedere delle delucidazioni in merito.

[7] http://www.ifccfbi.gov/
[8] http://www.ftc.gov/

2. TIPI DI ATTACCO

Non tutti gli attacchi phishing sono uguali e per questo motivo sono più difficili da scovare e risolvere nel migliore dei modi.

Per questo motivo, nei paragrafi successivi verranno elencati e spiegati i vari tipi di attacchi, ad oggi perpetuati nei confronti degli utenti.

2.1 Copie

Questa è la tecnica più utilizzata e consiste nell'utilizzare testi, immagini ed in molti casi veri e propri cloni dei siti originali in modo da convincere l'utente dell'effettiva autenticità del messaggio (*ved par. "3.3 Banca Antonveneta"*).

2.2 Utilizzo di indirizzi web autentici

Essendo basato sull'inganno è assolutamente necessario per il phisher mascherare il falso URL verso il quale l'ignaro utente verrà indirizzato con il vero indirizzo del sito clonato.

Per risolvere questo problema i phisher adottano prevalentemente due soluzioni:

- Sfruttare le vulnerabilità dei vari browser;

- Registrare nomi a dominio simili a quelli originali come nel caso della Unicredit Banca (**www.unicreditbanca.com**) la quale ha visto recapitare ai propri clienti un e-mail contenete un falso indirizzo **www.unicreditsbanca.com** simile, ma assolutamente estraneo alla banca in questione.

2.3 Indirizzo web mascherato

Per camuffare l'URL, soprattutto nelle e-mail, il phisher è solito utilizzare una delle seguenti tecniche:

- Conversione nome a dominio in indirizzo IP.
  Questo sistema consente di mascherare il nome del falso sito con il suo equivalente indirizzo IP; così il legittimo indirizzo: **http://www.ebay.com/signin.ebay.com** può trasformarsi in **http://218.154.123.224/signin.ebay.com**;

- Utilizzare il carattere @ (primi casi di phishing).
  Si modifica l'URL in questo modo:
  https://www.paypal.com/it/cgi-bin/webscr@www.microsoft.com, cosicché tutto quello che si trova a sinistra del simbolo @ viene ignorato mentre si è indirizzati verso il sito **www.microsoft.com**.
  Questa tecnica non è più sfruttabile in quando Microsoft ha rilasciato una patch[9] per ovviare al problema;

[9] Denominata anche "fix", è la riparazione di una parte dei programmi informatici che mostrano instabilità o problemi connessi con la sicurezza.

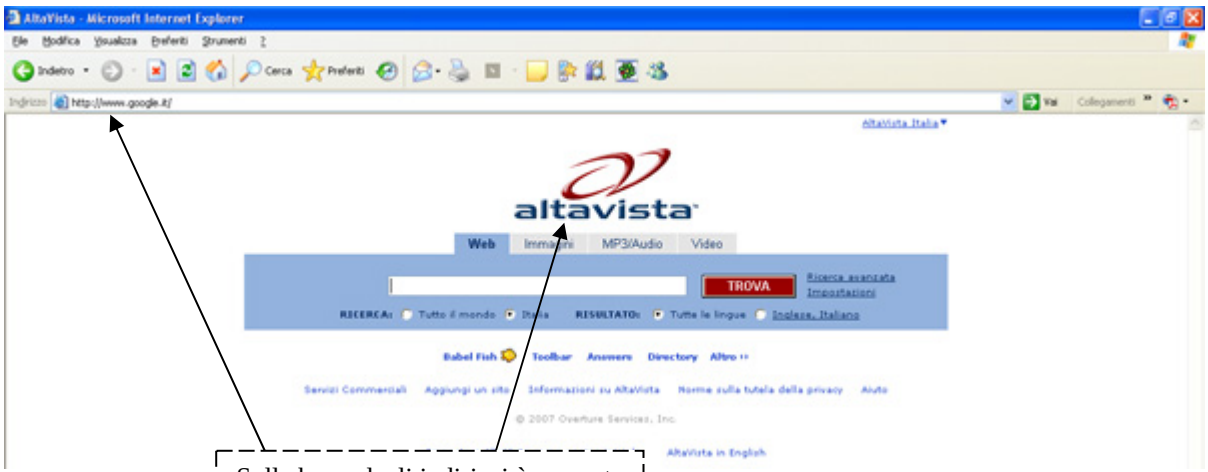
- URL codificato in ASCII[10] esadecimale[11].
  Il phisher codifica l'indirizzo del sito truffa in ASCII esadecimale (p.es. **http://cnn.com** diviene **http://%63%6E%6E%2E%63%6F%6D**);

- URL molto lunghi.
  Si utilizza un indirizzo web di dimensioni superiori a quelle della barra degli indirizzi in modo tale da non far vedere tutto.
  Un esempio è stato l'URL dei clienti Bank of America:
  http://62.193.218.82/daokewqoekwqoekwqoekwqoekwqpewqkeopwkdopsajdaoidjsaoidjsaoidjaoidjsaiodjsaoidjsaoidjsaoidjsaoidsajdoisajdoisajdoisadjsaoijdsaoidjsaoidjsaoidwqewqjepwqiekpwqkeopwk/card_activation.htm;

- Reindirizzamento.
  In questo modo l'utente crede di essere diretto verso il sito reale, mentre in realtà viene trascinato nel sito truffa, così come è avvenuto per i casi di phishing contro Banca Intesa.

2.4 Spoofing della barra degli indirizzi

E' una tecnica molto semplice che si attua sostituendo la reale barra degli indirizzi con una falsa immagine della stessa contenente un falso URL. Nella barra viene riportato il nome del sito sul quale ci aspettiamo di essere, ma in realtà siamo su un altro sito.



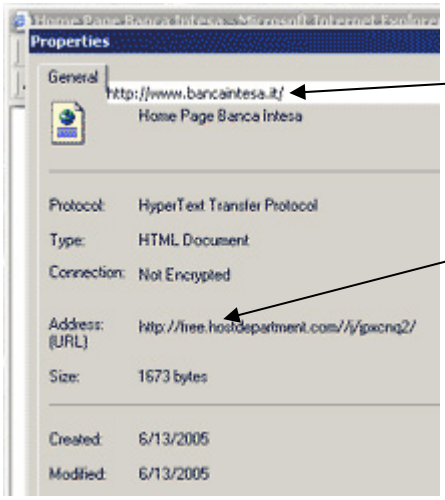
Questa tecnica risulta particolarmente insidiosa se utilizzata per modificare la barra di stato poiché si può visualizzare il lucchetto, tipico delle connessioni protette facendo così credere all'utente di essere in una sessione sicura.

[10] Il codice più diffuso per la rappresentazione dei simboli numerici ed alfabetici come sequenze di bit, rilasciato alla fine degli anni '60 dall'American National Standard Institute.
[11] Sistema numerico basato sulla potenza di 16.Usa i numeri da 0 a 9 e le lettere dalla A alla F.

2.5 Sostituzione dell'indirizzo web

In questo caso i phisher ricorrono alla sostituzione del solo indirisso URL tramite sovrapposizione di un immagine, quindi senza sostituire tutta la barra.

Sulla barra degli indirizzi si nota che è presente un'immagine dal bordo sporco



Aprendo le proprietà della pagina, notiamo nuovamente l'immagine che si sovrappone e successivamente notiamo nel campo **Address (URL)** un indirizzo diverso: **http://free.host**....

2.6 Finestre popup

Questa tecnica è sicuramente la migliore per quanto riguarda la riuscita dell'attacco e basa la sua forza sulla vulnerabilità dei browser.

In breve, l'attacco consiste in un'apertura di una finestra in foreground priva di barra degli indirizzi, degli strumenti e della possibilità di eseguire il "tasto destro" del mouse, dove si richiedono informazioni riservate all'utente. In background è presente il sito originale e quindi la truffa non è banale ed è poco individuabile.

2.7 Cross site scripting (CSS o XSS)

Questa tecnica è molto pericolosa in quanto sfrutta dei siti "reali", quindi ignari allo scopo, mediante l'esecuzione e/o l'inserimento di codice all'interno dei loro domini.

L'utente, ignaro della truffa, non percepisce l'attacco poiché pensa di essere all'interno del solito sito che consulta settimanalmente ma, di solito avviene così, durante l'invio tramite un form di informazioni è vittima del phisher.

2.8 Trojans / Worm / Spyware

Un famosissimo worm, ovvero PWS-Banker.y e le sue varianti hanno aiutato molto la causa del phishing negli ultimi tempi, grazie ad una vulnerabilità riscontrata in Microsoft Windows (in tutte le sue versioni) sulla gestione del file HOSTS[12].

Grazie a tale vulnerabilità, il worm modificava il file HOSTS dove inseriva i siti che effettuavano phishing, in modo tale da associare ad un nome logico tipo **www.bancaintesa.it** un indirizzo fisico differente ovvero quello del sito clonato.

I servizi di home banking attaccati sono stati: Banca Intesa, Banca Lombarda, Csebanking, BYBank di BancaAntonveneta, Credito Cooperativo e Banca Sella.

Inoltre, un ulteriore alleato dei phisher, è il keylogger, il quale è in grado di registrare in maniera subdola e silenziosa tutto quello che viene digitato all'interno del nostro sistema: username e password, indirizzi e-mail, numeri di carta di credito, conto correnti, informazioni riservate,ecc…

[12] File di testo che contiene la lista dei siti o server web ai quali associare un nome logico (p.es. 10.10.10.1 www.miosito.it).

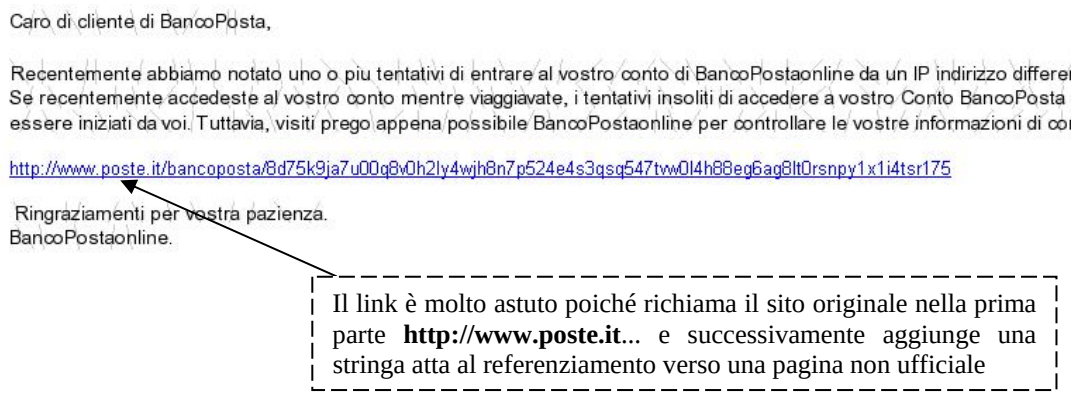
3. ESEMPI DI ATTACCHI

Per rendere più intuitiva la trattazione del phishing, prendiamo in esame alcuni degli attacchi subiti a carico di un numero ristretto di istituti di credito Italiani.

3.1 Poste Italiane

Cominciamo con il caso più noto, relativo a Poste Italiane.

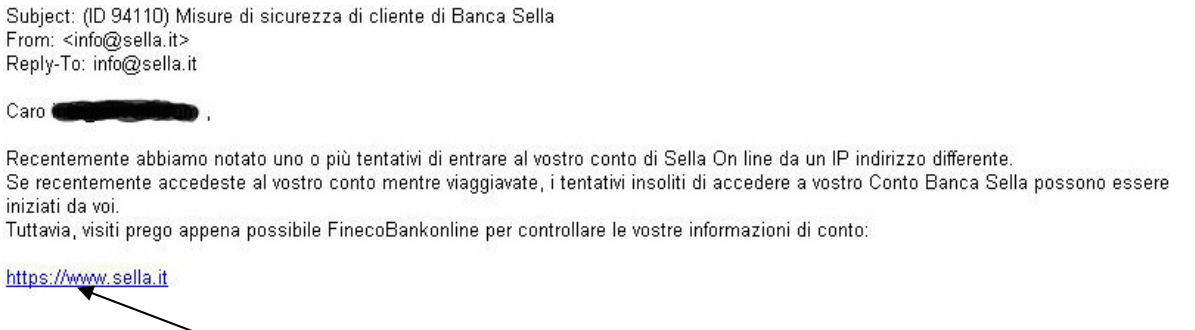
La tecnica di attacco è stata quella di inviare la solita e-mail (con evidenti errori ortografici) contenente un link creato ad hoc.



Il link è molto astuto poiché richiama il sito originale nella prima parte **http://www.poste.it**... e successivamente aggiunge una stringa atta al referenziamento verso una pagina non ufficiale

3.2 Banca Sella

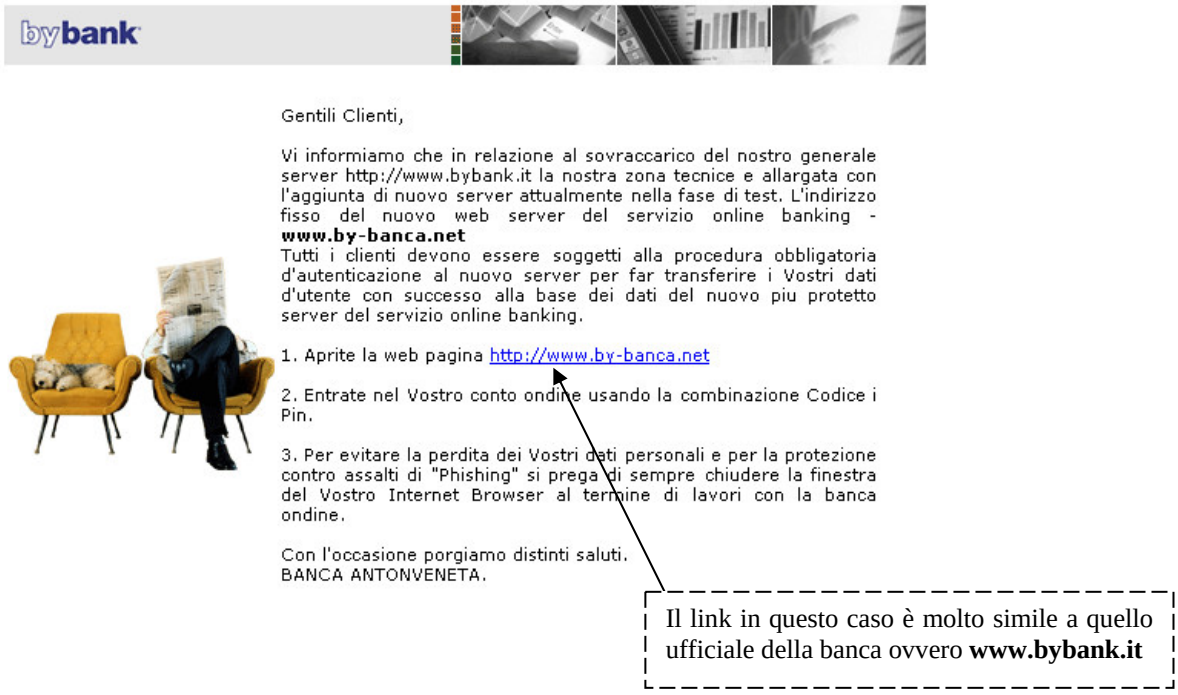
La tecnica di attacco è stata quella di inviare la solita e-mail (con evidenti errori ortografici) contenente un link creato ad hoc.



Il link in questo caso è veramente quello ufficiale della banca ma ad un attento osservatore non sfuggiva il fatto che tale link referenziava non **www.sella.it** ma un altro sito ovvero **http://sosmails.ktown**....

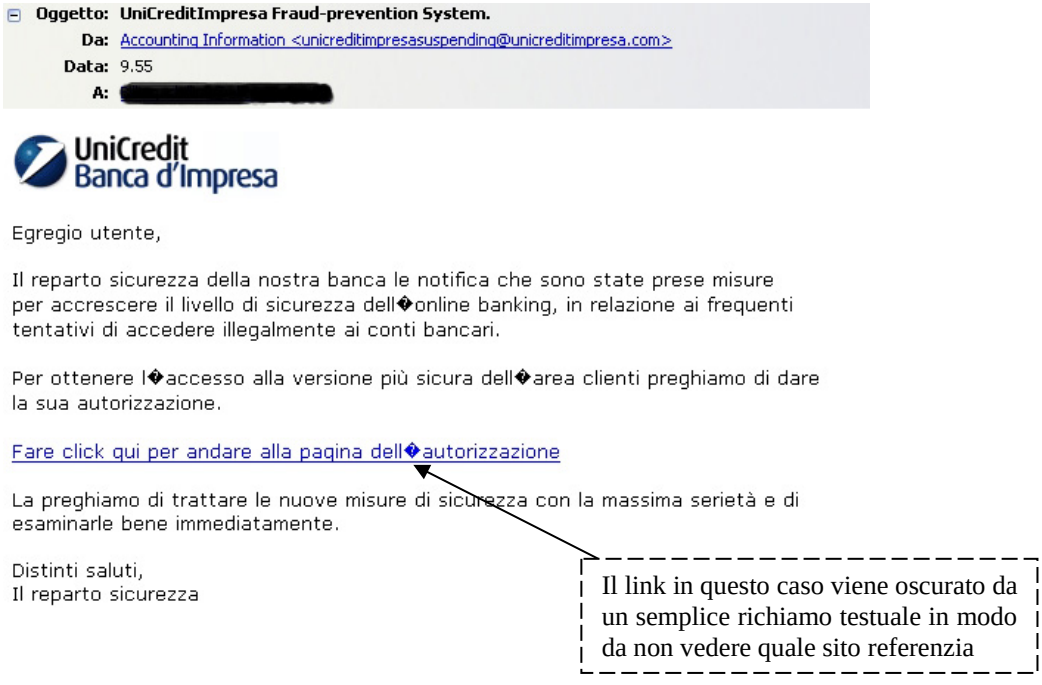
3.3 Banca Antonveneta

La tecnica di attacco è stata quella di inviare la solita e-mail (con evidenti errori ortografici) contenente un link creato ad hoc.



3.4 Banca Unicredit

La tecnica di attacco è stata quella di inviare la solita e-mail (con evidenti errori ortografici) contenente un link creato ad hoc.



4. IL PUNTO DELLA SITUAZIONE

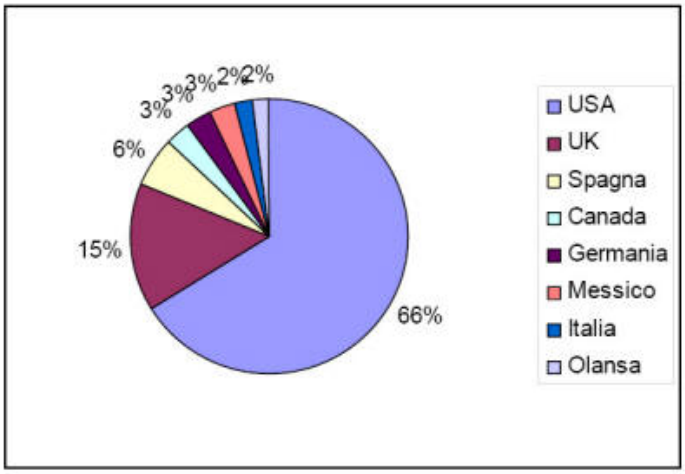
4.1 Il trend

In Italia, le truffe on-line legate alla tecnica del phishing nel gennaio 2007 sono aumentate dell'1% rispetto all'ultima rilevazione effettuata dalla RSA Anti-Fraud Command Center (AFCC) [13], fonte autorevole nel campo delle frodi online tanto da sventare ad oggi ben 30.000 attacchi di phishing.

Questa cifra, anche se molto bassa, fa riflettere sul fatto che nel nostro Paese il phishing sta prendendo piede (anche se molto lentamente per fortuna), tanto che i casi registrati nel 2006 sono ben 126 (fonte: **www.anti-phishing.it**). D'altro canto in Europa la situazione non è migliore.

Per quanto riguarda l'America, invece, il fenomeno è in netto calo con un 66% in meno di attacchi ad oggi rispetto al 78% (gli attacchi sono stati subiti prettamente da banche). Di contro, un maggiore numero di istituzioni finanziarie in Gran Bretagna è finito sotto attacco, mentre la Spagna è cresciuta di poco.

Il phishing, dall'inizio del 2006 è stata la frode più diffusa perpetuata in rete subito dopo i Trojan. L'RSA prevede che per gli anni a venire la situazione si complicherà ulteriormente e le frodi diverranno sempre più sofisticate.



Fonte Data Manager Online

[13] Struttura attiva 24 ore su 24, 7 giorni su 7 atta ad individuare, monitorare e rendere inoffensivi attacchi phishing, pharming e Trojan tentati ai danni di oltre 150 istituzioni di tutto il mondo.

4.2 Una nuova minaccia

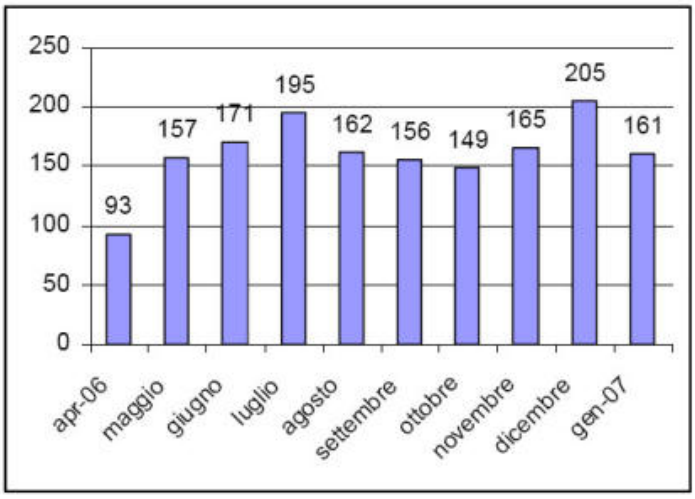
A Gennaio 2007, RSA ha scoperto l'esistenza di un nuovo kit universale acquistabile online e utilizzabile per sferrare attacchi phishing del tipo man-in-the-middle atto a organizzare un attacco, nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere messaggi tra due parti, senza che nessuna delle due sappia se il collegamento sia stato compromesso.

Esso è stato ideato, per facilitare nuovi e sofisticati attacchi creando una situazione in cui i dati personali delle vittime vengono intercettati, senza però che il flusso di comunicazione con il sito legittimo venga interrotto: l'URL fraudolento attivato dai truffatori si mette in pratica nel mezzo, impossessandosi in tempo reale delle informazioni riservate.

4.3 Trend degli attacchi mensili

Il trend italiano degli attacchi è pressoché costante e dal grafico si evidenzia, solamente, un periodo "migliore" relativo ad Aprile 2006 nonché un periodo "pesante" a Dicembre 2006.

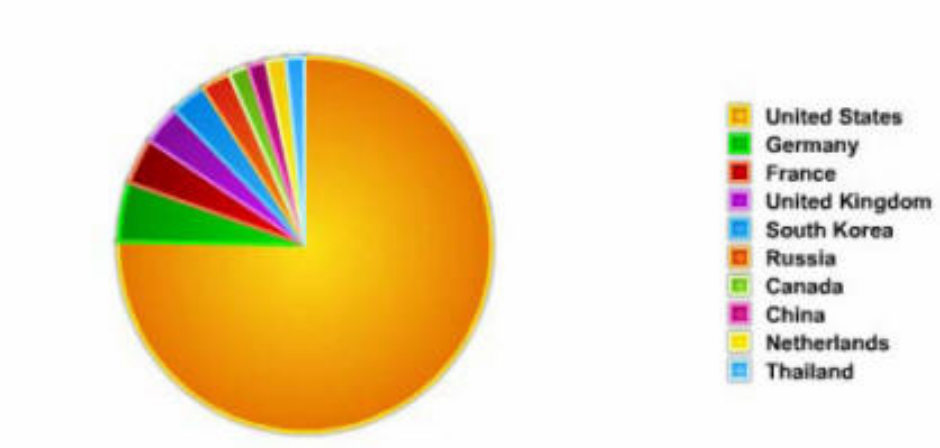
Attualmente la situazione a Gennaio 2007 è in calo rispetto alla fine dell'anno precedente, ma il numero degli attacchi rimane in media con l'anno precedente e ci si aspetta un aumento a breve visto il trend di altri paesi.



Fonte: Data Manager Online

4.4 Principali paesi ospitanti gli attacchi

Dopo il balzo in avanti a dicembre di oltre 10 punti rispetto al massimo storico del 60%, gli Stati Uniti come maggiore paese "ospitante" gli attacchi si è mantenuto intorno al 75% del totale. Belize e Giappone invece sono usciti fuori dalla classifica dei 10 principali paesi.



Fonte Anti-Phishing Italia

5. LA BIOMETRIA - ARMA CONTRO LE TRUFFE

5.1 Introduzione

Negli ultimi periodi, con la crescente insicurezza dei metodi di accesso ai vari servizi quali l'home banking in primis, i consumatori hanno visto di buon occhio l'uso di una nuova tecnologia di criptazione: la biometria[14].

In un intervista, condotta per conto di Unisys dal Ponemon Institute, la maggior parte dei consumatori negli Stati Uniti (63%) e nel Regno Unito (87%) ritiene che le principali minacce, destinate a crescere in futuro, siano legate al furto di identità e la sensazione comune è che gli istituti finanziari e le istituzioni non facciano abbastanza per contrastare questi fenomeni.

A fronte di questi risultati è emerso che una grande parte dei consumatori (92% in Gran Bretagna e il 69% negli Stati Uniti) auspica l'adozione di tecnologie biometriche da parte di banche, gestori di carte di credito ecc…, come valida alternativa all'utilizzo di lettori di smart card, token e password/PIN, per effettuare il controllo dell'identità degli utenti.

5.2 Cos'è la biometria

La biometria, dal greco "bios" (vita) e "metros" (misura), è l'insieme delle tecniche di identificazione automatica e di verifica dell'identità di un soggetto sulla base di peculiari caratteristiche fisiche o comportamentali.

Il riconoscimento biometrico non è di certo una novità tecnologica. Le origini di questa disciplina risalgono a più di un secolo fa, con l'antropometrica, ossia il metodo di identificazione dei detenuti e degli individui sospetti basato sulle caratteristiche della corporatura. Senza andare troppo indietro nel tempo, tecniche biometriche computerizzate sono comunque utilizzate da decenni per la sicurezza in ambito industriale e governativo, ma negli ultimi tre anni l'interesse nei confronti di questa disciplina si è intensificato e i suoi campi di applicazione moltiplicati.

Alcuni Stati membri hanno già da tempo hanno avviato progetti pilota e sperimentazioni di sistemi biometrici negli aeroporti. In Danimarca l'introduzione dei passaporti biometrici è già ben definita nei tempi e nei modi: dalla fine del 2004 fino ai successivi cinque anni verranno rilasciati tre milioni di passaporti biometrici, prodotti dalla società finlandese Setec vincitrice dell'appalto.

La biometria aggirerebbe una delle principali debolezze delle modalità di accesso e autenticazione ai sistemi informatici: la relativa facilità con cui le password possono essere violate. I sistemi biometrici più diffusi in questo campo sono basati sulla rilevazione delle impronte digitali o sulla scansione del volto.

Sul mercato già proliferano le soluzioni hardware e software: attualmente i dispositivi biometrici come scanner di impronte digitali, iride, mano, volto, richiedono ancora investimenti importanti ma riscuotono un interesse sempre maggiore, al punto che la biometria è diventata una parola sempre più ricorrente nel campo della sicurezza informatica. In secondo luogo, il riconoscimento biometrico può essere adottato per la gestione in totale sicurezza dei sistemi

[14] Dispositivi hardware e software che misurano le caratteristiche fisiche di un individuo per determinarne l'identità.

preposti alle transazioni finanziarie. Inserire dati biometrici nei chip di Bancomat e carte di credito, ci tutelerebbe definitivamente da fenomeni deleteri come la clonazione, usi indebiti in caso di furto e ci solleverebbe dall'incombenza di dover conservare in sicurezza i codici Pin.

Attualmente l'unico progetto concreto di un'applicazione destinata ad un ampio bacino di utenti è stato annunciato a Febbraio dalla Bank of Tokyo in collaborazione con Mitsubishi, che prevede di installare sistemi di ***riconoscimento della venatura della mano*** su tutti gli sportelli automatici.

5.3 Tipologie di controlli biometrici

Le tecniche biometriche più diffuse sono:

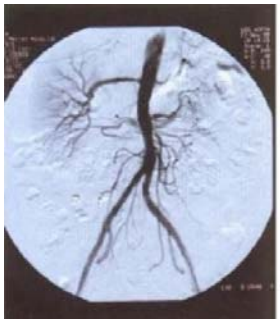
- Rilevazione delle impronte digitali.
  E' la tecnica più antica e più affidabile perché le caratteristiche dell'impronta sono immutabili e i dispositivi di scansione sono molto precisi e poco costosi.
  È ideale per l'autenticazione su dispositivi personali;

- Riconoscimento della geometria della mano.
  Si basa sull'acquisizione di un'immagine tridimensionale, e valuta parametri come forma, ampiezza del palmo e lunghezza delle dita ma il costo dell'hardware è molto alto (circa 1.000 / 2.000 euro a singolo riconoscitore);

- Riconoscimento dell'iride.
  E’ un ottimo identificativo poiché le caratteristiche dell’iride sono uniche e immutabili, in più le condizioni dell'illuminazione non incidono sull'operazione di riconoscimento anche se i non vedenti non possono utilizzarlo.
  Molto usato per la sicurezza degli accessi fisici, anche se i costi sono molto alti;

- Riconoscimento del volto.
  Questa tecnica è limitata da una bassa stabilità, poiché i tratti somatici possono variare nel tempo a causa di incidenti, invecchiamento ed altro.
  Questo tipo di riconoscimento può essere raggirato se non si utilizzano macchine di ultima generazione;

- Scansione della retina.
  E’ una tecnica molto precisa anche se molto costosa;



- Riconoscimento della firma.
  E’ caratterizzato da un'affidabilità bassa.
  E’ usato per l'autenticazione a dispositivi mobili.