PHISHING: FRODE IN INTERNET

1. INTRODUZIONE:

Ogni giorno sorgono in Internet nuove minacce che obbligano ad aggiornare tutto quello che riguarda a patch, vulnerabilità del sistema, antivirus, etc..Nonostante attualmente la nuova modalità di delitti in Internet si denomina Phishing. La differenza con le suddette minacce è che questa volta nessuno cerca di accedere al tuo sistema malintenzionatamente, nemmeno cercano di introdurti un virus che possa provocare il malfunzionamento del tuo computer. Con un Phishing, è il proprio utente che invia le informazioni personale e confidenziale di forma volontaria; questo si, animato da tecniche di inganno.

2. CHE COS'È?

Il Phishing non è più che la simulazione di siti internet. Si trattano di messaggi elettronici ingannevoli e pagine web fraudolente che apparentano procedere da istituzioni di fiducia(banche, entità finanziarie..), però che in realtà sono disegnati per ingannare il destinatario e ottenere la divulgazione di informazioni confidenziale. Il termino Phishing significa "pescare" in inglese, giacché in realtà ha una certa similitudine con la pesca. Si lancia l'amo e si aspetta a che qualcuno "abbocchi". La ricompensa non può essere più saporita: dati personali e chiavi d'accesso ai conti bancari.

3. COME FUNZIONA?

Attraverso un messaggio elettronico, simulando procedere di una fonte affidabile (per esempio, della tua banca), si tentano di raccogliere i dati necessari per truffare l'utente. In realtà si tratterebbe di messaggi massivi . I truffatori non sanno quale è la tua banca e per ciò creano una mail con la sembianza corporativa della banca scelta che è inviata massivamente. La realtà è che qualcuno di questi messaggi arriverà ad utenti di questa banca.

Di solito si tratta di messaggi di testo: "Per motivi di sicurezza…", o "Il suo conto si deve confermare..", o "Utenti della Banca avvertono…", indicando all'utente che si stanno realizzando dei cambi e che per sicurezza deve introdurre i suoi dati personali e codici bancari cliccando in un link che loro indicano. Una volta cliccato si riindirizza a una pagina molto simile a quella della banca abituale. La verità è che questo sito appartiene al truffatore, che non deve fare altro che copiare i dati che l'utente compila. Al finalizzare conferma l'operazione rimanendo l'utente tranquillo pensando che i dati inseriti sono stati raccolti per la sua banca.

Altre volte la stessa mail richiede di riempire e pulsare "invio", senza necessità di riindirizzare a un'altra pagina.

La sorpresa in entrambi casi arriverà nel momento in cui il conto bancario sia a 0, e la Banca ti informi che sei stato vittima de una truffa chiamata "phising".

4. COME EVITARLO?

Il fenomeno del Phising ha acquistato una gran importanza su scala mondiale, tanto a livello d'utente come a livello aziendale, inclusi le istituzioni bancarie, che osservano come non possono fare nulla mentre i suoi clienti sono ingannati e inoltre perdono fiducia nella " banca on line".

Attualmente, l'unica forma di evitare questo tipo di truffe consiste nell'essere consapevoli. Purtroppo, nessun antivirus né nessun sistema di sicurezza possono impedire questi attacchi. Di seguito esponiamo qualche consiglio che ci potranno aiutare a riconoscere questo tipo di messaggi:

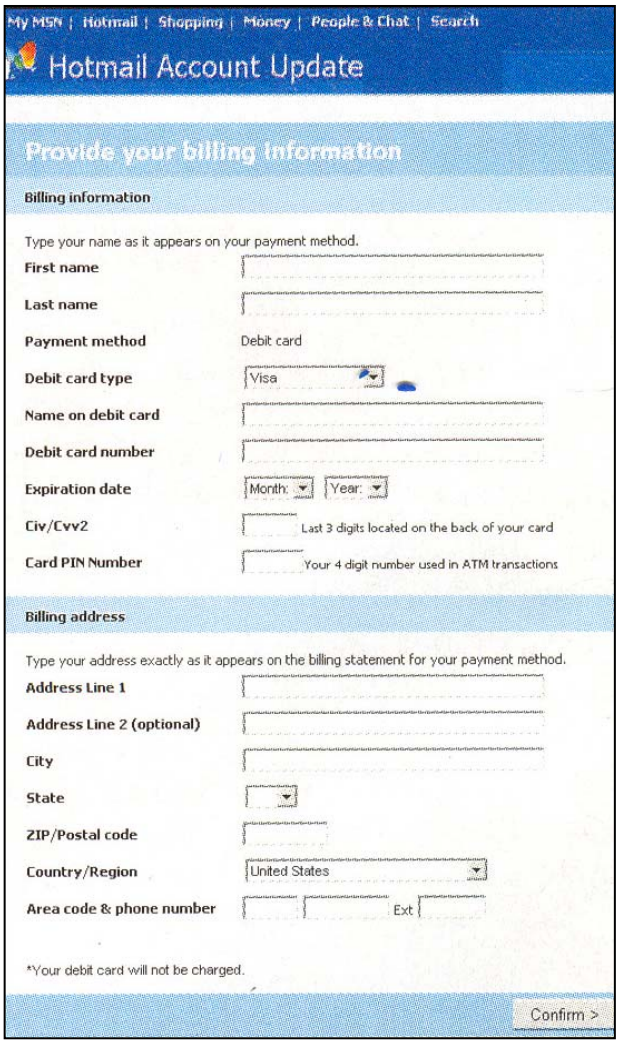
1. In primo luogo, e forse il più importante, è che dobbiamo ricordare che le Banche o Casse di risparmio si comunicano sempre per corriere tradizionale. Non le chiederanno mai di introdurre dati personali o bancari in una mail.
2. In Spagna stanno cominciando a prodursi questo tipo di casi di truffa in banche spagnole, però per il momento sono scarsi e le mail che stanno ricevendo gli utenti stanno scritti in inglese. È logico pensare che una Banca spagnola non invierà comunicati in inglese.
3. Quando riceviamo una mail sconosciuta o di provenienza dubbiosa, è consigliabile chiamare subito alla Banca per confermare la veridicità del messaggio.
4. Osservare se l'indirizzo comincia per htpps, al posto di http: (la "S" indica che la pagina si trova in un server sicuro)

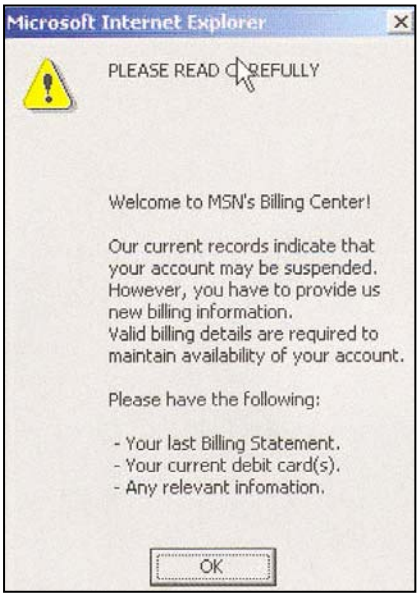
ATTENZIONE: Le tecniche del Phising stanno imparando velocemente da questo tipo di errori e li stanno perfezionando. Consiste in creare una finestra emergente nella posizione dove appare l'URL nella barra degli indirizzi di Internet Explorer, in maniera tale che si sourapponga e occulti l'indirizzo reale del server dell'attaccante dove in realtà si trova l'utente, mostrando al suo posto l'URL della entità bancaria. Il messaggio ha incluso un link che in teoria la dirige alla Web dell'entità. Se l'utente clicca su questo link, può osservare come appare la Web dell'entità e che nella barra degli indirizzi di Internet Explorer appare l'URL corretta, includendo il prefisso https:\\ come se si trovasse in una connessione sicura.

5. Se ha qualsiasi dubbio, può passare il cursore sopra il link allegato alla mail. Molte volte l'indirizzo non è lo stesso che appare nel messaggio.
6. Un'altra maniera di riconoscere questi messaggi è che non sono intestati. Di solito hanno il titolare: "Stimato cliente".
7. Procuri non dirigersi alle sue Web finanziarie di fiducia attraverso di links facilitati o indirizzi di Internet la cui origine sia sconosciuto.

8. Può anche osservare che nella parte bassa del suo browser si vede un lucchetto chiuso(non rotto). Questo simbolo indica un certificato di autenticità e se ci clicchiamo sopra appariranno i dati del certificato. Potremo verificare che non si trova scaduto e che il proprietario corrisponda alla pagina che si sta vedendo.

Vogliamo ricordaLe che il Phishing non è qualcosa di nuovo e che non si estende unicamente alle entità finanziarie. In generale dobbiamo essere cauti e sospettare di fronte a qualsiasi finestra emergente che ci chieda dati bancari. Un'altra frode con messaggi ingannevoli si può trovare in false finestre o e-mails inviati ad utenti di Hotmail. Altro dei settori più pregiudicati è quello delle aste e vendite ondine.





5. RIPERCUSSIONE DEL PHISHING

Nella attualità, i casi più gravi di phishing si sono prodotti negli Stati Uniti, sebbene le mafie si sono rese conto del suo enorme potenziale, per cui la sua espansione si sta producendo a livello mondiale, soprattutto nei Paesi di lingua inglese dove si trova ora più concentrato. In Spagna si sono verificati, per il momento, casi nel Banco Pastor, Banco Popular e Banesto.

La ditta Gartner ha analizzato il problema del Phishing e realizzò un'interessante studio su questo fenomeno negli Stati Uniti. Di seguito esponiamo le conclusioni più rilevanti:

I tentativi di frode contro i consumatori in Internet, meglio conosciuti come phishing, sono diventati così comuni che si stima che 57 milioni di statunitensi hanno ricevuto qualsiasi tipo di messaggio elettronico fraudolento, d'accordo con un nuovo studio presentato da Gartner. Le perdite dirette della frode d'identità contro queste vittime riguardanti questo tipo di attacchi di phishing, costarono alle Banche e Compagnie di credito circa 1,200 milioni di dollari l'anno scorso.

Basati in una inchiesta applicata a 5,000 adulti che usano Internet, gli analisti di Gartner stimano che approssimativamente 30 milioni di adulti utenti della Web credono che hanno sofferto un attacco di phishing, mentre che altri 27 milioni credono che è stato un tentativo di frode.

I tentativi di attacchi phishing non sono nuovi, però sono diventati più comuni nei ultimi 12 mesi. D'accordo con l'inchiesta della ditta consulente , il 76% dei attacchi sospetti accadranno negli ultimi sei mesi (da ottobre del 2003), un altro 16% successe sei mesi fa o prima. Quindi, i risultati combinati suggeriscono che il 92% dei tentativi d frode si sono prodotti nell'ultimo anno.

"Le istituzioni finanziarie, fornitori di servizi di Intenet e altri fornitori di servizi devono considerare seriamente questi tipi di frodi", disse Avivah Litan, vicepresidente e direttore di investigazione della ditta. "Questi fornitori di servizio devono agire e applicare soluzioni che minimizzino o evitino il rischio, sebbene i fornitori dei servizi non siano vittime dirette.

Eventualmente, tutti quegli utenti della posta elettronica si vedranno affettati da per una mancanza di fiducia nelle proppie transazioni se le frodi non saranho ridotte in maniera significativa dai livelli in cui attualmente si trovano.

L'attacco di Phishing accade quando un "ciberpirata" invia un messaggio che contiene un link a un sito di rete fraudolento dove si sollecita all'utente di fornire informazioni sul suo conto personale. Il messaggio e il sito web si trovano tipicamente mascherati simulando il sito di un fornitore di fiducia, istituzione finanziaria o di commercio on line degli utenti.

L'inchiesta di Gartner, conclusa in Aprile, mostrò un alto grado di successo da parte dei truffatori. Basandosi nei sui risultati dell'inchiesta, Gartner stima che circa il 19% dei attaccati o quasi 11 milioni di statunitensi adulti che usano Internet , hanno cliccato in un messaggio di tentativo di frode. Peggio ancora, il 3% dei attaccati, uno stimato di 1.78 milioni di adulti affermano aver dato ai truffatori le sue informazioni finanziaria o personale.

I dati indicano che "le vittime di frodi tipo phishing sono quasi tre volte tanto propense a identificare un frode, come possono esserlo altri consumatori on line", menzionò Litan. "In qualsiasi modo che si veda, i truffatori stanno ottenendo i loro obiettivi fraudolenti. I fornitori di servizi non hanno altra scelta che combattere detti messaggi, se vogliono che la computazione on line ritorni a essere sicura come un canale per le transazioni con i clienti".

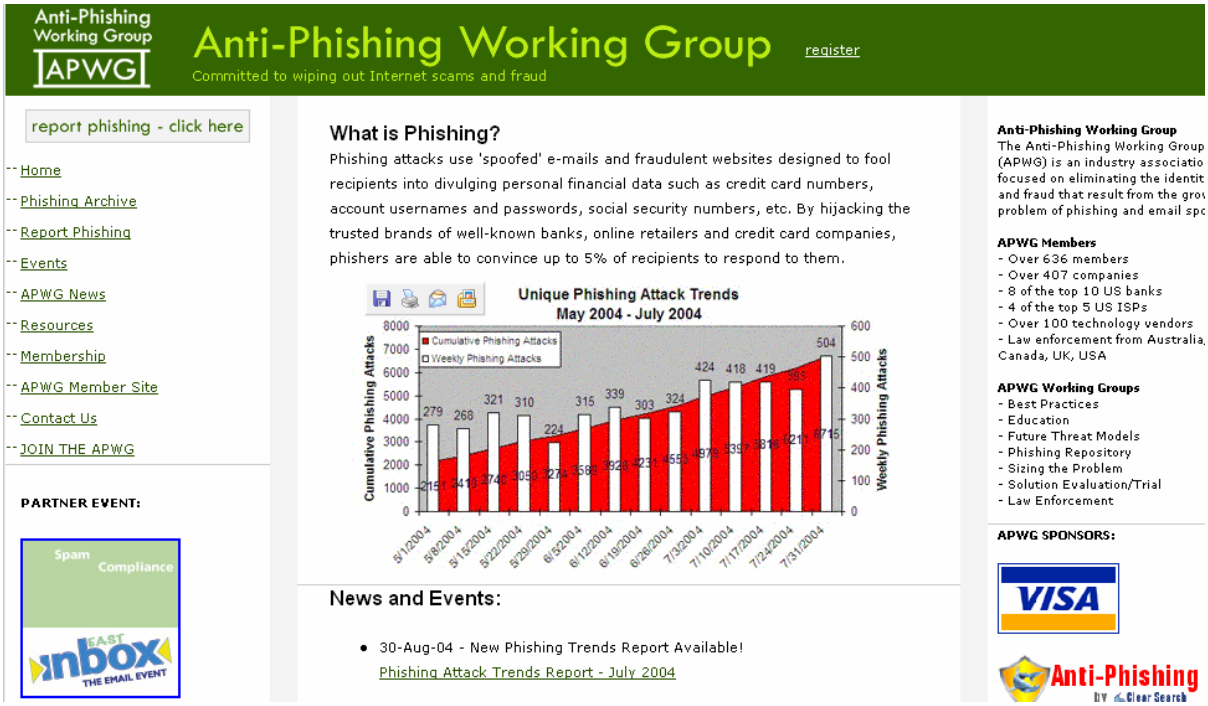
Le soluzioni contro le frodi tipo phishing, da messaggi con firma elettronica digitale fino a servizi anti-phishing amministrati, sono alcune delle tecnologie che discuteranno nelle ricerche future da Gartner.

6. LOTTA CONTRO IL PHISHING

6.1 ANTI-PHISHING WORKING GROUP" (APWG)

La rapida proliferazione di questa nuova truffa si è convertita in una delle principali cause di lotta delle aziende contro i delitti on line. Negli Stati Uniti si è creata la **"Anti Phishing Working Group"(APWG).** Si tratta di una associazione di industrie il cui principale obiettivo è finire con il furto d'identità e i frodi risultanti del crescente problema del phishing in messaggi elettronici fraudolenti. Se vuole ulteriori informazioni su questa associazione, può visitare la sua pagina Web: **http://www.antiphishing.org;** e nel caso che scopra un caso di truffo di tipo phishing, può denunciarlo ed inviargli una mail a **reportphishing@antiphishing.org**

Questa organizzazione realizza un Rapporto mensile analizzando tutti gli attacchi di phishing denunciati a APWG. L'ultimo corrisponde a Luglio 2004 e lo possiamo trovare nella sua pagina web (in inglese). Di seguito riproduciamo i dati più rilevanti del Rapporto.



6.2 DATI

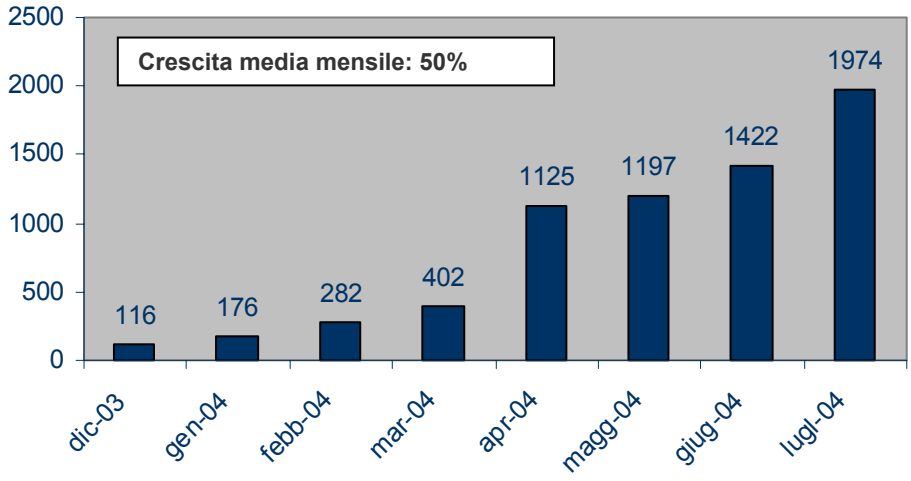
- Numeri di attacchi unici di phishing riportati durante Luglio **1974 attacchi**
- Media mensile di crescita: **50%**
- Organizzazione più attaccata durante Luglio: **Citibank (682)**
- Paese con maggiore numeri di Webs di phishing: **USA (35%)**

***Un "attacco unico di phishing si definisce in questo analisi come un solo invio massivo di messaggi elettronici inviati una volta, destinati a una compagnia o organizzazione e scritti in una stessa linea di testo.**

- ***NUMERI DI ATTACCHI UNICI DI PHISHING***

A Luglio, si produssero 1974 nuovi e unici attacchi di phishing denunciati alla APWG. Questo significa un aumento del 39% sul numero di attacchi registrati nel messe di Giugno(1422). La media di attacchi giornalieri registrati a Luglio fu di 63.7 (dato molto significativo considerando che a Giugno la media fu di 47.6). L'ultima settimana di Luglio fu la peggiore al registrarsi più di 500 attacchi.

Grafica di attacchi unici mensili



Fonte: Anti-Phishing Working Group

- ***¿QUALI ORGANIZZAZIONI O COMPAGNIE SONO STATE PIÙ ATTACATE DA PHISHING?***

Quando parliamo di organizzazioni più attaccate, vogliamo far riferimento ai messaggi elettronici fraudolenti che simulano la provenienza di una organizzazione concreta. Ovviamente, i più attaccati e realmente pregiudicati sono gli utenti e clienti di quella organizzazione.

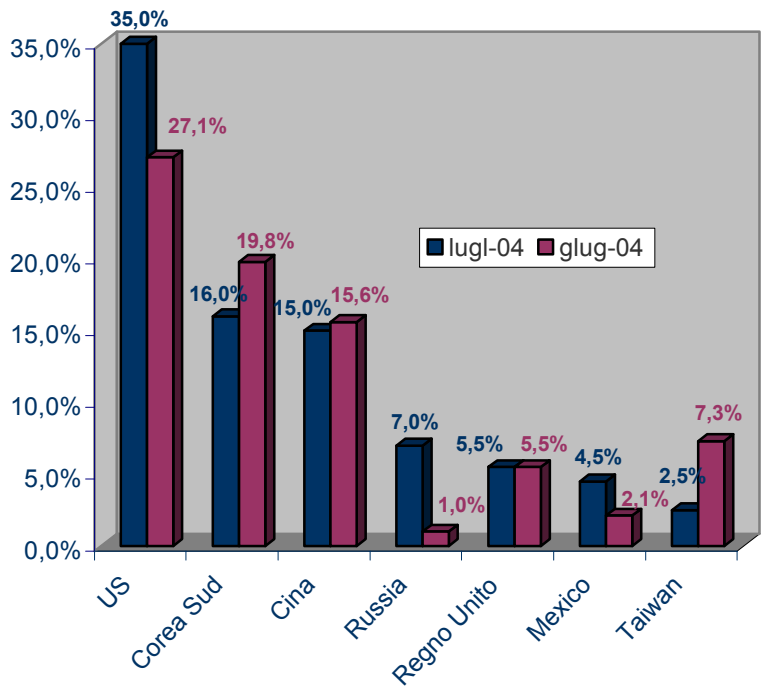
Imprese pregiudicate	**Lug-04**	**Giu-04**	**Mag-04**	**Apr-04**	**Mar-04**	**Feb-04**	**Gen-04**
Citibank	682	492	370	475	98	58	34
U.S.Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
Lloyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9

Fonte: Anti-Phishing Working Group

- ***PAESI CON MAGGIOR NUMERO DI WEBS DI PHISHING***

Gli Usa sono il Paese con il maggior numero di webs con phishing. Altri paesi, inclussi Russia, Regno Unito e Mexico hanno mostrato un incremento significativo in "alloggiare" queste pagine.

Paesi che "alloggiano" il maggior numero di webs di Phishing



Fonte: Anti-Phishing Working Group

6.3 LONGEVITÀ MEDIA DI WEBS PHISHING

La media di "vita" di questo tipo di webs fraudolente, misurata secondo il tempo in cui appaiono fino al momento della loro scoperta, è di 6.1 giorni. Fino ad ora, la web phishing più longeva durò 31 giorni(in altre parolle, questa web continuò a funzionare per un messe intero)

BIBLIOGRAFIA

Giornali:

- Personal Computer: Ottobre 2004. Nº 21
- PC Pro: Nº 51 2004

Internet:

- www.hispasec.com/unaaldia/2163
- www.vnunet.es/Actualidad/Noticias/ Seguridad/Privacidad/20040927017
- www.el-mundo.es/navegante/ 2004/09/27/seguridad/1096287700.html
- http://www.antiphishing.org/

Informes:

- Anti-Phishing Working Group. "Phishing Attack Trends Report - July 2004." Julio 2004