TECNICHE DI PHISHING

Alessandro Sigismondi
Consulente osservatoriocards

conference
CARDS2008

27 MAGGIO 2008

Come consulente dell'osservatoriocards ci siamo occupati di diversi casi di phishing ,ai danni di istituti di credito e di ignari cittadini e aziende

Quest'anno sono arrivate all'osservatorio diverse segnalazioni di vittime della truffa del phishing ,con email in cui era manifesta la tipologia dell' inganno (truffa da phishing) di diversi istituti di credito italiani,in alcuni casi l'ignaro utente ha effettuato le procedure indicate e si è ritrovato il conto corrente svuotato.

Possiamo riconoscere un'email falsa e non cadere nella trappola che il truffatore ci tende?

Osservatorio Internazionale
cards
Servizi e Nuovi Sistemi di Pagamento

Tecniche utilizzate per creare email false

Osservatorio Internazionale cards
Servizi e Nuovi Sistemi di Pagamento

conference
CARDS2008

Il metodo della chiocciolina (@)

Supponiamo che uno si spaccia per nostro amico e ci invii un'email dicendo di aver scoperto che dal sito della microsoft è possibile raggiungere un sito del "louvre" di Parigi,e ci invia l'indirizzo,
http://www.microsoft.com&item=q209354rexsddiuyjkiuylkuryt2583453453fsesfsdfsfasfdfdsf@www. www.louvreparigi.com
Se si guarda distrattamente il chilometrico link,si penserà che si tratti davvero di una pagina del sito Microsoft. In realtà il link porta alle normali pagine di del museo di Parigi, ma l'illusione è perfetta.Questo metodo funziona grazie alle regole di funzionamento di Internet, che consentono ai browser di interpretare indirizzi Web redatti in questo modo:sito_apparente@sito_reale.

conference
CARDS2008

27 MAGGIO 2008

Qualsiasi cosa venga scritta prima della chiocciolina viene sostanzialmente ignorata, e quindi si può usare una stringa lunga a piacere: più è lunga, più è improbabile che la vittima dell'inganno se la legga tutta e scopra il trucco. Certo, un navigatore attento può accorgersi della presenza di quel link finale e quindi sospettare l'inganno. Ma si può mascherare in vari modi il nome del sito dopo la chiocciolina.

Osservatorio Internazionale
cards
Servizi e Nuovi Sistemi di Pagamento

Il metodo dell'indirizzo numerico semplice

A ogni nome di sito Internet corrisponde un indirizzo IP, per esempio, al momento in cui scrivo, c'è un sito di museo, , che ha l'indirizzo IP 216.170.137.3. I browser interpretano questo indirizzo IP e lo usano per portarvi a visitare il sito corrispondente. In combinazione con il metodo della chiocciolina, questo permette di architettare truffe come questa:http://www.microsoft.com&item= q209354@216.170.137.3Indirizzo e-mail protetto dal bots spam , deve abilitare Javascript per vederlo In questo modo, ogni riferimento visivo alla vera destinazione di questo link è scomparso.

Un navigatore attento potrebbe accorgersi dell'inganno notando che dopo la chiocciolina c'è appunto un indirizzo IP, ossia quello del sito che viene effettivamente raggiunto cliccando sul link, e insospettirsi. Ma ci sono altri modi meno evidenti, descritti qui sotto, per esprimere un indirizzo IP.

Il metodo del nome mascherato

Si può anche codificare l'URL (il nome) del sito-truffa anziché il suo indirizzo IP Normalmente, quando vogliamo visitare un sito, ne digitiamo il nome. Se voglio visitare ad esempio la CNN, digito nel mio browser il nome del suo sito (che è CNN. COM). Tuttavia esiste anche un altro modo di rappresentare il nome di un sito: codificandolo in modo che ogni carattere del nome sia sostituito dal suo equivalente ASCII esadecimale preceduto dal simbolo di percentuale) Ad esempio, la lettera "c" di cnn.com si codifica come %63, la lettera "n" come %6E, il punto come %2E, e così via (più sotto trovate la tabella completa delle equivalenze). In questo modo, cnn. com diventa un incomprensibile %63%6E %6E%2E%63%6F%6D. Provare per credere: il link http://cnn.com e il link http://%63%6E%6E%2E%63%6F%6D portano entrambi al sito della CNN.

A questo punto è facilissimo creare un'email falsa usando i metodi descritti prima.

Supponiamo che io voglia far credere a un utente che un link porta al sito Microsoft, mentre in realtà porta al sito www.attivissimo.net e in particolare al file nn10.htm nella sottodirectory /b/.

http://www.microsoft.com&item= q209354@attivissimo.netIndirizzo e-mail protetto dal bots spam , deve abilitare Javascript per vederlo /b/nn10.htm. Fatto questo, converto la parte che voglio nascondere usando le equivalenze. E già che ci sono, nascondo anche la chiocciolina, sostituendola con %40. Ed ecco il risultato: http://www.microsoft.com&item=q209354%40a%74t%69v%69s%73i%6Do%2En%65t/b/nn10.htm

conference
CARDS2008

27 MAGGIO 2008

Come non cadere in queste truffe

Per non cadere in queste truffe si deve imparare a leggere l'email dal punto di vista tecnico,cioè leggere gli "header"Gli header sono quella parte del messaggio (che normalmente non si vede) che contiene tutti i dati dell'e-mail, i campi from e TO, i server usati per l'invio. Il metodo per leggere gli header dipende dal sistema utilizzato per leggere le e-mail (direttamente su internet con la web mail o tramite un programma di posta elettronica), se si usa la web mail nella pagina di lettura del messaggio è presente il collegamento apposito, se si usa un programma esterno per la lettura delle e-mail (come Outlook) la modalità per leggere gli header varia a seconda del programma utilizzato (con Outlook Express basta premere ALT+INVIO mentre si legge il messaggio e cliccare su "Dettagli").

Osservatorio Internazionale cards
Servizi e Nuovi Sistemi di Pagamento

conference
CARDS2008

27 MAGGIO 2008

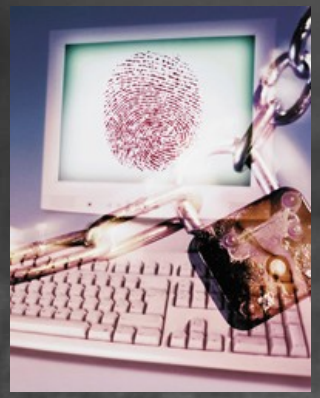
Cosa fare in caso di email ingannevoli

Per prima cosa non bisogna assolutamente rispondere a queste e-mail indesiderate, altrimenti si darà la conferma che l'indirizzo esiste e lo spam aumenterà. Per evitare di ricevere altre e-mail dallo stesso mittente basta aprire il messaggio e cliccare su "posta indesiderata", automaticamente le e-mail ricevute da quel mittente non saranno recapitate.

Osservatorio Internazionale
cards
Servizi e Nuovi Sistemi di Pagamento

conference CARDS2008

27 MAGGIO 2008



“SPEAR PHISHING”

"pesca con la fiocina" o"*phishing* con la fiocina

conference
CARDS2008

27 MAGGIO 2008

Fino ad ora abbiamo sempre sentito parlare di **phishing** che è una frode informatica, realizzata con l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illeciti, di dati riservati,quali i dati di accesso alla propria banca online.

Osservatorio Internazionale cards
Servizi e Nuovi Sistemi di Pagamento

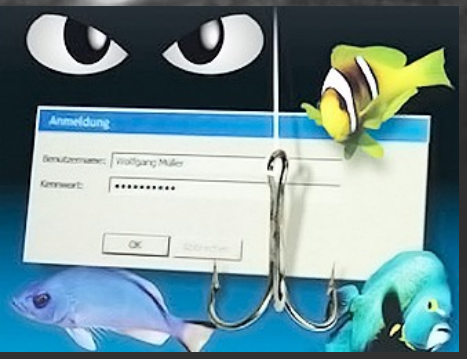
Chi perpetrava questo reato ha capito che gli scam diventano sempre più difficili da mandare a segno, per via della **crescente consapevolezza degli utenti**; per cui è stato ideato un **sistema di truffe più sofisticato**, non più indirizzato ad una moltitudine di utenti, ma le truffe sono **indirizzate verso piccoli gruppi**, dove può rivelarsi più semplice ottenere la fiducia di poche persone per il tempo strettamente necessario a ottenere le loro informazioni.

Il contenuto della lettera sarà credibile, dal momento che contiene informazioni riguardanti l'azienda stessa e magari viene inviata indicando l'esatto nome di un dirigente come mittente.

conference CARDS2008

Lo “spear phishing” utilizza **messaggi di posta elettronica falsificati apparentemente attendibili** che inducono tutti gli appartenenti a una determinata organizzazione a rivelare i propri dati di accesso ai sistemi aziendali**.**

E' **quasi impossibile quindi per il destinatario non aprire il contenuto della e-mail**, permettendo all'autore anonimo di carpire informazioni preziose presenti sul computer di quella persona**.**



Osservatorio Internazionale cards
Servizi e Nuovi Sistemi di Pagamento

A differenza del tentativo di phishing generico, più comune, l'**attacco di *spear phishing* è molto più difficile da ostacolare**. Vi sono almeno due motivi per questo:
gli attacchi sono diretti a piccoli numeri di individui, ed è quindi più difficile per gli addetti alla sicurezza venirne a conoscenza e fornire protezione e avvisi;
dal momento che gli attacchi hanno come obiettivo il personale di un'organizzazione specifica, le tecniche di social engineering possono essere molto specifiche e personalizzate per i dipendenti di tale organizzazione.

Il phishing, è subdolo e sarcastico perché sfrutta l'ingenuità e l'ignoranza degli utenti, e il messaggio di posta elettronica del phisher è generalmente scritto in un italiano improbabile (il che lascia supporre che il fenomeno non abbia ancora preso piede presso i criminali del nostro paese), con gli accenti sbagliati, con verbi coniugati male, con improbabili espressioni idiomatiche.

conference
CARDS2008

27 MAGGIO 2008

Un trucco diffuso è **quello di spacciarsi per un collega di un ufficio** che ha motivo e titolo di chiedere tali informazioni, ad esempio sistemi informativi o gestione del personale. A volte il messaggio dirotta l'utente su una versione falsificata del sito o della Intranet aziendale.
Lo spear phishing consente di confezionare **e-mail-trappola molto più convincenti**, la struttura del messaggio lascia intendere che il mittente è il datore di lavoro o un altro dipendente o collega

I messaggi di spear phishing, invece, indicano nome, cognome e altri dati personali dei loro bersagli. La reazione istintiva è di fidarsi di chi dimostra di sapere già tutte queste informazioni personali.

Osservatorio Internazionale cards
Servizi e Nuovi Sistemi di Pagamento

conference
CARDS2008

27 MAGGIO 2008

La **conseguenza** non è solo il **furto di informazioni finanziarie personali**, ma anche le **possibili perdite di proprietà intellettuale, segreti commerciali e altri dati altamente sensibili**. Gli spammer inviano messaggi per consigliare l'acquisto di azioni che poi possono essere vendute con profitto.

Osservatorio Internazionale
cards
Servizi e Nuovi Sistemi di Pagamento

Il consiglio è sempre lo stesso, come per i messaggi spam: **non acquistare, non provare, non rispondere.**