SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Dicembre 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Il Phishing

Introduzione

La posta elettronica è uno dei principali strumenti con cui comunichiamo: non la usiamo solo per il nostro lavoro, ma anche per rimanere in contatto con amici e famigliari. L'email è anche un modo con cui le aziende forniscono servizi online, come la conferma di un acquisto o la comunicazione della disponibilità dell'estratto conto bancario. Dal momento che molte persone in tutto il mondo dipendono da questo mezzo di comunicazione, è diventato uno dei metodi di attacco primari utilizzato dai criminali e truffatori. In questa newsletter illustreremo il phishing, un metodo di attacco molto comune, e i metodi per usare l'email in modo sicuro.

L'autore di questo numero

Lance Hayden è Direttore Esecutivo di Berkeley Research Group. Esperto in cultura della sicurezza, è anche autore di "People-Centric Security: Transforming Your Enterprise Security Culture" edito da McGraw-Hill. Potete conoscerlo meglio su **www.linkedin.com/in/drhayden**.

Il Phishing

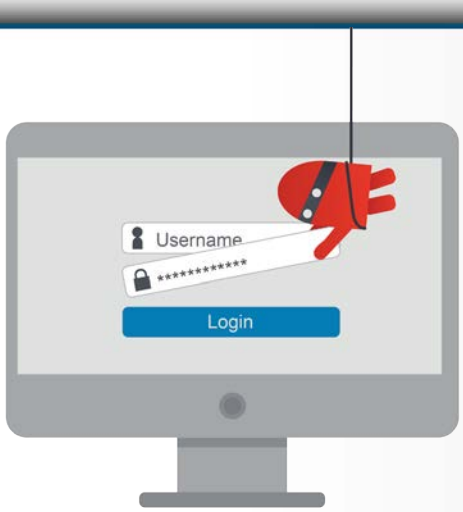
Con il termine Phishing ci si riferisce a un tipo di attacco che fa uso dell'email o di servizi di messaggistica, come quelli usati dai social network, con lo scopo di ingannare una vittima e portarla a compiere un'azione: cliccare un link o aprire un allegato. Chi cade vittima di questo tipo attacchi rischia il furto di informazioni sensibili e l'infezione di computer o smartphone. I truffatori fanno di tutto per rendere le loro email il più convicenti possibile: spesso i messaggi appaiono provenire da un conoscente, un amico, dalla propria banca, in sostanza, da entità di cui aver fiducia. Nel caso di un messaggio della banca o dell'emittente della carta di credito, per conferirvi maggior credibilità, il messaggio potrebbe contenere anche il logo dell'azienda e potrebbe provenire dall'indirizzo email dell'istituto di credito. In realtà, una volta studiato e realizzato, il messaggio viene inviato a milioni di persone. I criminali non sanno chi ne cadrà vittima, poiché ciò che conta è inviarne il maggior numero possibile per aumentare la probabilità di successo dell'operazione. Il Phishing è assimilabile a una pesca con la rete: non si sa ciò che si pescherà, ma più la rete è grande, maggiore è il numero dei pesci che vi cadranno. Un'operazione di phishing può essere caratterizzata da uno o più dei seguenti elementi:

- **la raccolta di informazioni**: lo scopo dell'attaccante è di raccogliere informazioni personali, come password, numeri di carte di credito, dettagli dei conti bancari. Per ottenere questi dati, viene inviato un link che conduce la vittima a un sito web apparentemente legittimo. Nel sito verrà richiesto di inserire username e password o altri dati personali. Si tratta naturalmente di un sito falso: ogni informazione che invierete finirà direttamente ai criminali;

Il Phishing

- **link maligni**: scopo dell'attaccante è ottenere il controllo del vostro dispositivo (computer, smartphone, tablet) attraverso una mail contenente un link che conduce direttamente a un sito web in grado di scatenare un attacco al vostro dispositivo che, se avrà successo, infetterà il sistema;
- **allegati maligni**: l'obiettivo dell'attaccante è sempre quello di infettare e prendere il controllo del dispositivo. Anziché un link, vi verrà inviato un file infetto, ad esempio un documento Word. Aprendo l'allegato scatenerete un attacco che potenzialmente permetterà il controllo remoto del vostro sistema;
- **truffe**: alcune email di phishing non sono altro che la versione digitale di una truffa classica. Cercheranno di ingannarvi dicendo che avete vinto alla lotteria o vi chiederanno di fare beneficenza per un ente caritatevole o, ancora, chiederanno il vostro aiuto per trasferire ingenti quantità di denaro.

Se risponderete a questi messaggi, vi chiederanno di anticipare dei soldi per dei servizi, o di inviare i dati della vostra carta di credito, in modo da potervi sottrarre quanto più denaro possibile.



La vostra miglior difesa è il buon senso. Se un messaggio è strano, vi fa nascere qualche sospetto o è troppo bello per essere vero, potrebbe trattarsi di un attacco phishing.

Come proteggersi

Nella maggior parte dei casi, aprire e leggere un'email non comporta alcun problema. Perché un attacco di phishing abbia successo, i criminali vi devono ingannare per portarvi a compiere un'azione. Fortunatamente, possiamo individuare degli indizi che indicano che un messaggio è un attacco: vediamo di seguito i più comuni.

- Il messaggio crea un senso di urgenza, chiedendo una "azione immediata" prima che accada qualcosa di brutto (la chiusura del vostro account, ad esempio). L'hacker vuole costringervi a fare un errore senza riflettere
- Ricevete un'email con un allegato che non stavate aspettando e il messaggio vi chiede di aprirlo. Esempi di questo sono le comunicazioni dalla vostra banca o da un'istituzione della pubblica amministrazione
- Anziché usare il vostro nome, il messaggio inizia con un generico "Caro Cliente". La maggior parte delle aziende o dei conoscenti che vi contattano, conoscono il vostro nome
- L'email vi chiede informazioni molto sensibili, come il numero di carta di credito o una password
- Il messaggio sembra provenire da un'azienda reale, ma è caratterizzato da evidenti errori di ortografia e proviene da indirizzi personali con domini come @gmail.com, @yahoo.com, @hotmail.com.

Il Phishing

- I link contenuti sono strani e non “ufficiali”: se portate il mouse su un link senza cliccare, vi verrà mostrato il collegamento reale. Se i due link non corrispondono, non cliccate. Su uno smartphone,
- I link sembrano strani e non “ufficiali”. Un metodo per verificarli consiste nel portare il mouse sul link senza cliccare, in modo che si apra un popup che mostra il reale collegamento. Se i due link non corrispondono, non cliccate. Potete inoltre copiare e incollare l’URL dall’email al vostro browser
- Ricevete un messaggio da qualcuno che conoscete, ma il tono o le parole non suonano come fossero realmente sue. Se avete un sospetto, chiamate il mittente per verificare che l’abbia inviato lui. È semplice per un truffatore creare un’email che appare come provenire da una persona conosciuta.

Se pensate che un’email sia un attacco di phishing, cancellatela. Il buon senso è la vostra miglior difesa.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un’azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Social Engineering:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf
Sicurezza in cinque punti:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_it.pdf
Il computer è stato compromesso. E ora?:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis