PHISHING

COS'È E COME EVITARLO

AGID CERT-PA

Le pillole di sicurezza

Chi siamo

Il CERT-PA è una struttura che opera all'interno dell'Agenzia per l'Italia Digitale (AGID) ed è preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle pubbliche amministrazioni.

Contattaci

Se sei vittima di phishing e sei una PA accreditata puoi contattarci:
AGID CERT-PA

Email: cert-pa@cert-pa.it

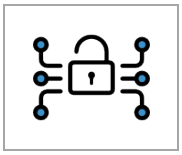
Web: www.cert-pa.it

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA

INDICE

I NOSTRI SERVIZI

ANALISI E INDIRIZZO



Supporto alla definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica

SERVIZI PROATTIVI

Raccolta e elaborazione di dati significativi ai fini della sicurezza cibernetica, emanazione di bollettini e segnalazioni di sicurezza, implementazione e gestione di basi dati informative

SERVIZI REATTIVI

Gestione degli allarmi di sicurezza e supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA

FORMAZIONE E COMUNICAZIONE

Promozione della cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni

COSA È IL PHISHING?

Il phishing è una frode informatica, realizzata con l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illegali, di dati riservati oppure a far compiere alla vittima determinate operazioni che, di solito, comportano il download di un determinato file oppure il collegamento a uno specifico sito web.

Il phishing è un tipico attacco di social engineering, in cui si sfrutta l'interazione umana e in cui è richiesta la partecipazione attiva della vittima. E' basato sulla normale tendenza alla fiducia delle persone, sulla curiosità, sull'autorevolezza dell'interlocutore, sulla sorpresa, sull'intimidazione o sull'ignoranza. Un'aspetto sicuramente curioso del phishing è la sua connotazione "etnica". È stato verificato da uno studio che i vari popoli sono più o meno sensibili a forme di phishing differenti. Ad esempio, sembra che gli italiani siano portati maggiormente a cadere in frodi in cui si annuncia la vendita di cellulari a prezzi particolarmente vantaggiosi mentre gli americani tendano a cadere di più in trappole legate a premi o vincite online.

COME SI VIENE ATTACCATI?

Di solito, si riceve una e-mail in cui la vittima viene invitata a compiere determinate operazioni magari sotto l'azione di una pressione psicologica opportuna, come un conto scaduto o bloccato o un procedimento non andato a buon fine con possibile minaccia, talvolta, di ritorsioni legali.

QUALI SONO I RISCHI?

I rischi che si corrono quando si è vittima di un attacco di phishing sono diversi e in continua evoluzione:

- furto di identità
- partecipazione ad attività illegali, ad esempio una botnet
- cessione di risorse all'attaccante
- inserimento della mail della vittima in una lista di spam

COSA È IL FURTO DI IDENTITÀ?

Una *identità* è un sottoinsieme di attributi di una persona che caratterizza univocamente questa persona all'interno di un gruppo. L'unione degli attributi di tutti questi possibili sottoinsiemi viene definita *identità completa* di una persona. Ad esempio, nel caso di un gruppo piccolo di persone un attributo potrebbe essere il colore dei capelli, "Mario è quello con i capelli biondi"; nel caso di un gioco online potrebbe essere un determinato nickname, "Mario è quello che ha come nick Tempesta47"; nel caso di una banca potrebbe essere il possesso di una carta e la conoscenza di un PIN "Mario è il proprietario di un conto che ha il bancomat e conosce il PIN di accesso".

Di solito, quando l'utente vuole o deve farsi riconoscere per compiere determinate operazioni, sia nel mondo reale che virtuale, deve dimostrarlo tramite una procedura di autenticazione. Questa procedura si può basare su tre controlli di base:

1. “ciò che si ha” – è il possesso di un determinato oggetto, come una chiave, una carta, un badge ecc.
2. “ciò che si sa” – è la conoscenza di qualcosa, come un PIN, una password o la risposta a una domanda segreta
3. “ciò che si è” – è riferito a una caratteristica biometrica dell’utente, come le impronte digitali, l’impronta dell’iride, la forma dell’orecchio ecc.

La procedura di autenticazione è tanto più solida quanti più fattori vengono controllati. Ad esempio, nell’autenticazione a un solo fattore potrebbe bastare il possesso di un badge, come quando si accede ai tornelli della metro, oppure la conoscenza di una coppia username/password; in quella a due fattori potrebbe essere il possesso di una scheda e la conoscenza di un PIN, come è il caso del bancomat; in quella a tre fattori si potrebbe unire all’ultimo controllo e cioè possesso di un badge e conoscenza di un PIN anche il controllo della retina

Un Furto di identità consiste nel furto di un’identità parziale dell’utente, cioè di un sottoinsieme di attributi che lo identificano in un certo contesto, allo scopo di compiere atti illeciti.

Se, ad esempio, un ladro riesce ad entrare in possesso del nostro bancomat e del relativo PIN può recarsi a un ATM e compiere operazioni sul nostro conto corrente venendo a tutti gli effetti scambiato dal sistema come noi. Ci sta, cioè, completamente impersonando.

CHE COS’È L’IDENTITÀ NEL MONDO DIGITALE?

Nel mondo digitale, le transazioni che l’utente compie durante la sua navigazione in Rete rappresentano gli attributi che in generale consentono di identificarlo.

L’utente Mario Rossi, dopo essersi collegato al suo provider ed aver ricevuto un indirizzo IP univoco per tutta la durata della sua connessione, si collega ad una chat dove immette un nickname e dice delle cose, scambia informazioni, con altri utenti come lui; successivamente, esegue un bonifico dalla propria casella di internet banking; sul sito di posta immette le sue credenziali e legge la sua posta privata e, infine, decide di acquistare una macchina fotografica digitale in un noto sito di e-commerce.

Ognuno di questi esempi è una transazione o un gruppo di transazioni che costituiscono un’identità parziale dell’utente.

PERCHÉ STO RICEVENDO E-MAIL NON RICHIESTE?

Gran parte delle e-mail che riceviamo oggi non sono semplicemente testuali ma sono, a tutti gli effetti, delle pagine web contenenti banalmente immagini e testo. La visione delle immagini richiede che l’utente effettui il loro scaricamento dal sito web dove risiedono. In questo modo la vittima fa sapere all’attaccante, proprietario del sito web, che “è vivo” nel senso che la sua casella di e-mail, che magari l’attaccante ha trovato per caso su Internet, è attiva ed effettivamente controllata da un utente reale. A questo punto

l'attaccante la inserirà in una lista di spam, magari rivendendola a soggetti terzi, e la vittima inizierà a ricevere e-mail non volute che potrebbero essere anche il preludio ad un attacco di tipo diverso.

COSA È UN MALWARE?

Un malware è un particolare tipo di software creato per compiere operazioni non volute e dannose sul PC di una vittima, di solito a sua insaputa. L'obiettivo dell'attaccante è quello di installare in modo permanente e difficilmente individuabile il malware stesso, in modo da evadere il controllo dell'utente e anche di un eventuale antivirus. Per fare questo, vengono di solito sfruttate funzionalità avanzate del sistema operativo del PC o del software legittimo usato come veicolo (ad es. una macro di un file Word).

Esistono vari tipi di malware, tra cui virus, trojans, ransomware, rootkit ecc. Questi tipi non sono mutuamente esclusivi, nel senso che possono esistere malware con caratteristiche comuni a più di un tipo.

Il phishing è un metodo molto usato per diffondere malware.

COME SI SVOLGE UN ATTACCO DI PHISHING?

Un tipico attacco di phishing si svolge seguendo delle fasi, descritte di seguito:

4. La vittima riceve una e-mail contenente dei link contraffatti, spacciati per veri, ad esempio una e-mail dalla banca in cui viene richiesto l'aggiornamento dei dati personali oppure degli allegati da scaricare (file pdf, zip, exe, word ecc.)
5. Nel caso del link, facendo click, la vittima viene invitata a scaricare un determinato software o ad accedere a una pagina in cui deve inserire le credenziali per autenticarsi con i meccanismi descritti sopra
6. Se l'obiettivo dell'attaccante è l'installazione di un determinato software sul pc della vittima, questo viene installato. Se invece l'obiettivo è il furto di identità questo può avvenire sia direttamente, attraverso l'inserimento in un'opportuna pagina web delle credenziali da parte della vittima che verranno salvate dall'attaccante, sia indirettamente attraverso una determinata categoria di software, denominati keylogger, che hanno l'obiettivo di inviare all'attaccante tutte le lettere digitate dalla vittima sulla tastiera del PC.

COSA È UNA BOTNET?

Una botnet è una rete di computer collegati ad internet che, a causa di falle nella sicurezza o mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, vengono infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto. Questi ultimi possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali.

COME RICONOSCERE UNA E-MAIL DI PHISHING?

Ci sono vari modi, più o meno raffinati, con cui capirlo. Facciamo ad esempio riferimento alla figura:

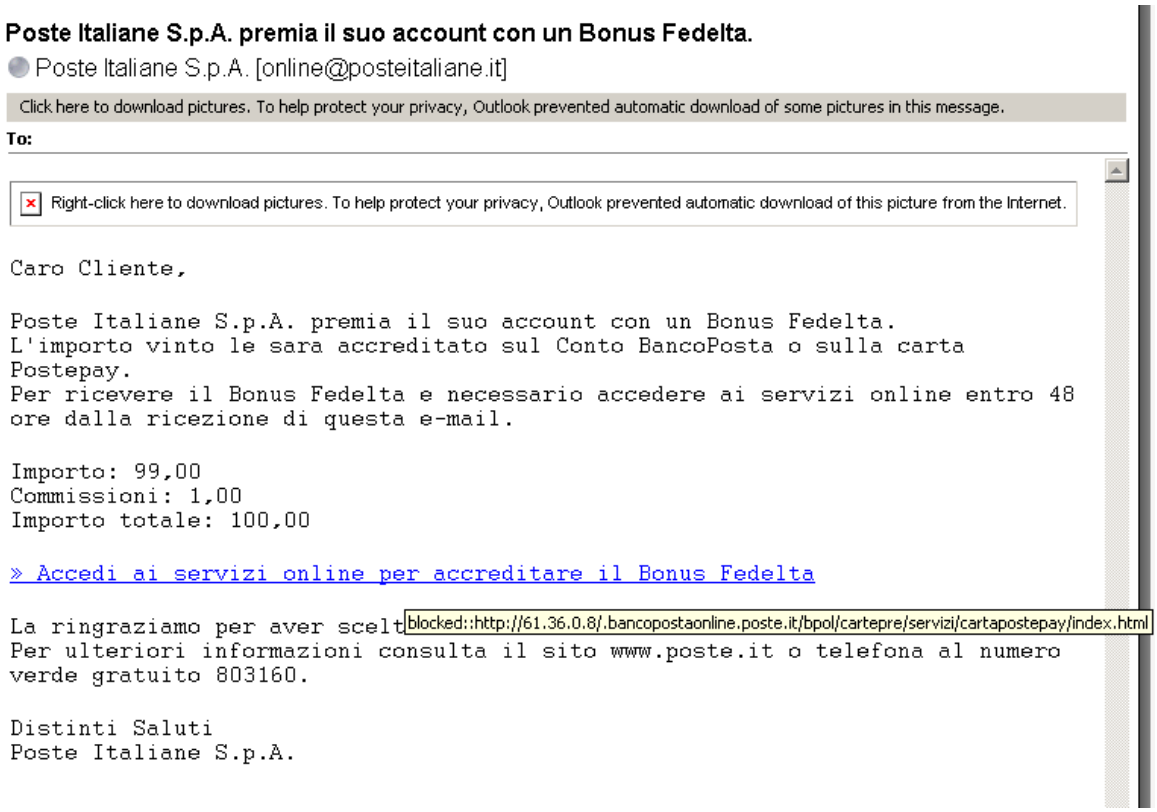
7. L'e-mail non è scritta in italiano corretto
8. È intestata a un generico "cliente", "utente", "signore" ecc. e non contiene il nome o il cognome dell'utente.
9. Passando il mouse sul link (ma NON cliccando) possiamo vedere dove il link ci porterà. E' quello che ci aspettavamo? Quello che conta è il primo pezzo, quello tra http:// e il primo / successivo (nel nostro caso http://61.36.0.8/ che NON è una URL usuale di Poste, anzi..una ricerca ci dice che è coreano!). Non guardate a quello che c'è scritto dopo!! Se abbiamo dei dubbi sul contenuto, NON clicchiamo sul link proposto dalla mail, ad esempio Bancopostaonline, ma apriamo il browser e andiamo alla URL da noi normalmente usata e verifichiamo l'eventuale contenuto della mail. Nel caso esista un servizio clienti, contattiamolo per verificare la correttezza o meno e, nel caso, segnalare l'attacco di phishing

Supponiamo di aver cliccato il link e di essere arrivati a una pagina dove ci chiedono username e password. Abbiamo dei dubbi? Inseriamo una username/password fasulle (pippo/pippo vanno benissimo). Un sito vero non riconoscerà le credenziali inserite e non ci farà passare. Uno falso SI, perchè non conosce le nostre vere credenziali!

COSA È IL MALSPAM?

Il Malware Spam o Malspam è il termine che si riferisce al malware che viene veicolato in allegato ai messaggi di posta elettronica. Questi ultimi, spesso, hanno come oggetto tematiche commerciali, bancarie o fiscali accompagnate da toni di urgenza per indurre nella vittima ansia e preoccupazione, emozioni che di solito portano ad agire in modo sconsiderato e privo delle opportune difese.

I consigli che si possono dare per evitare di rimanere infettati sono: 1) mai scaricare o visualizzare allegati di e-mail da mittenti sconosciuti 2) dubitare sempre di e-mail non sollecitate 3) non abilitare le macro di Office, anche se il documento ci invita a farlo 4) non eseguire mai file eseguibili 5) far attenzione anche ai file PDF; questo tipo di file può eseguire flash o javascript o addirittura lanciare applicazioni esterne 6) molti attaccanti usano nomi di file con un doppia estensione, tipo pippo.jpg.exe; Windows mostrerà il file come pippo.jpg nascondendo il fatto che in realtà è un eseguibile; per ovviare a questo, disabilitare nelle opzioni di Esplora Risorse la voce "nascondi estensioni per tipi di file noti" 7) nei casi dubbi, contattare sempre il mittente e utilizzare un servizio online come www.virustotal.com per fare una verifica.



VOGLIAMO SAPERNE DI PIÙ?

Ci sono alcuni strumenti che possono essere utilizzati da utenti esperti per capire meglio una mail di phishing. Il primo è WHOIS (https://www.whois.com/whois/) a cui possiamo sottoporre il pezzo del link tra http:// e il primo / successivo per capire a chi appartiene il sito web a cui l'e-mail ricevuta sta cercando di farci collegare. Viene fornita una casella di ricerca in cui dobbiamo inserire il dato (nel nostro caso metteremo 61.36.0.8) e vengono restituite tutte le informazioni, da cui vediamo, appunto, che il server web si trova in Corea, cosa un po' strana dato che dovrebbe essere di Poste italiane.

Whois IP 61.36.0.8

Updated 6 minutes ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '61.32.0.0 - 61.39.255.255'

% Abuse contact for '61.32.0.0 - 61.39.255.255' is 'hostmaster@nic.or.kr'

inetnum:        61.32.0.0 - 61.39.255.255
netname:        BORANET
descr:          LG DACOM Corporation
admin-c:        IM646-AP
tech-c:         IM646-AP
country:        KR
status:         ALLOCATED PORTABLE
mnt-by:         MNT-KRNIC-AP
mnt-irt:        IRT-KRNIC-KR
last-modified:  2017-02-03T00:55:02Z
source:         APNIC

irt:            IRT-KRNIC-KR
address:        Seocho-ro 398, Seocho-gu, Seoul, Korea
e-mail:         hostmaster@nic.or.kr
abuse-mailbox:  hostmaster@nic.or.kr
admin-c:        IM574-AP
tech-c:         IM574-AP
auth:           # Filtered
mnt-by:         MNT-KRNIC-AP
last-modified:  2017-10-19T07:36:36Z
source:         APNIC

person:         IP Manager
address:        Seoul Yongsan-gu Hangang-daero 32
country:        KR
phone:          +82-2-10-1
e-mail:         ipadm@lguplus.co.kr
nic-hdl:        IM646-AP
mnt-by:         MNT-KRNIC-AP
last-modified:  2017-08-07T01:06:21Z
source:         APNIC

% Information related to '61.32.0.0 - 61.39.255.255'

inetnum:        61.32.0.0 - 61.39.255.255
```

Nel caso, invece, in cui l'e-mail avesse un allegato e volessimo controllarne l'eventuale pericolosità (operazione comunque molto rischiosa) è possibile utilizzare il servizio online di controllo dei malware di virustotal. Esso permette di fare l'upload del file sospetto e ci restituirà un rapporto completo sulla sua pericolosità. Occorre fare attenzione al fatto che, pur essendo aggiornatissimo l'insieme dei malware su virustotal, potrebbe anche non essere riconosciuto da esso come pericoloso in quanto troppo recente. Per questo è importante sempre trattare con cura gli allegati delle mail sospette lasciando a chi ha le competenze adeguate l'analisi degli stessi. Meglio, quindi, cancellare immediatamente l'e-mail sospetta.

PERCHÉ IL COMPUTER MI SI È IMPROVVISAMENTE RALLENTATO?

L'obiettivo di un attaccante potrebbe essere quello di farci installare un software il quale sfrutterà le risorse del sistema (memoria, processore, spazio disco, rete ecc.) per effettuare le operazioni per le quali è stato disegnato. Ci sono attacchi di phishing il cui obiettivo è proprio quello di usare le risorse della vittima. Un esempio è Trojan.BitCoinMiner che sfrutta il processore del computer attaccato per generare cryptovaluta.

COSA DEVO FARE SE PENSO DI ESSERE STATO INFETTATO?

Nella malaugurata eventualità in cui l'attaccante abbia raggiunto il suo scopo e sia riuscito a scaricare e installare il suo software nel nostro PC la cosa migliore da fare è quella di reinstallare da capo il PC partendo da un supporto sicuro (ad es. il CD del vendor) non fidandosi mai di software scaricato illegalmente da siti insicuri e di cui non siamo certi della provenienza. Per questo è importante fare sempre dei backup periodici (magari anche più di uno, ad esempio uno su un hard disk esterno e uno su cloud) dei nostri file importanti.

Ci sono poi accortezze relative all'uso di password:

- non usare mai la stessa password su siti importanti e non (ad es, la stessa password usata per accedere a Facebook usata anche per l'home banking)
- usare sempre password complesse
- cambiare la password con regolarità

preferire inoltre, quando possibile, sistemi di autenticazione multipli, come la conoscenza di una password e di un PIN inviato sul cellulare

COME POSSO SAPERE SE SONO STATO INFETTATO (PER UTENTI ESPERTI)?

Se siamo fortunati, la scansione effettuata con un antivirus aggiornato potrà segnalare e gestire il problema. D'altra parte, se il malware è particolarmente raffinato e soprattutto di recente creazione è possibile che l'antivirus non sia in grado di identificarlo.

L'utilizzo di un firewall personale, installato sul PC, può segnalarci connessioni di rete sospette o azioni strane (come il tentativo di sovrascrivere files di sistema o di scrivere voci sul registro, per i sistemi Windows) effettuate da qualche software.

Tra le cose da fare è possibile verificare, magari con l'aiuto di un tecnico, se

- Il browser che usiamo per accedere a internet ha delle estensioni (plugin o moduli) che noi non abbiamo installato
- Il browser utilizza un proxy a nostra insaputa
- Il file hosts (sia su un sistema windows che unix) ha delle righe che non abbiamo inserito
- Il DNS che viene utilizzato per la risoluzione di nomi in indirizzi IP non è un server ufficiale o comunque di provenienza certa
- Il router usato per accedere a internet non è quello che dovrebbe essere (questo per esempio è particolarmente importante quando si usa una wifi pubblica. Esistono software che un attaccante può installare sul proprio computer per fingere di essere un access point legittimo)
- Il computer carica in fase di avvio software di cui non siamo sicuri (ad es. su windows è possibile verificare dal Pannello di Controllo o dal Registro di Sistema in Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run e

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce)

- Ci sono processi attivi di cui non siamo sicuri (su Windows ad es. tramite Gestione attività)
- Il computer si collega a siti esterni di cui non siamo sicuri (ad es. per Windows è possibile installare il software tcpview https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview che mostra tutte le connessioni di rete effettuate dal nostro PC)

Occorre fare attenzione al fatto che continuamente vengono creati nuovi malware che sfruttano meccanismi per nascondersi particolarmente insidiosi sempre più raffinati e in grado anche di disabilitare temporaneamente antivirus e firewall nonché di eludere uno qualsiasi dei meccanismi descritti sopra.

Autore
Alessandro Sinibaldi, senior security expert CERT-PA
Graphic designer
Daniela De Blasis, visual designer, UX/UI designer at AgID