Definizioni

Phishing

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale

Phishing

Cosa vuole l’attaccante?

L’attaccante vuole comporre e consegnare un messaggio plausibile, fingendosi un’entità di cui la vittima si possa fidare, in modo da spingerla a compiere una determinata azione desiderata, che può essere:

- Azione fisica (i.e.: bonifico bancario)
- Furto di dati
- Trasmissione di un payload

Phishing

Caso di Studio: Sony Data Breach

2015. Hacker entrano nella rete interna di Sony Picture Entertainment. Diversi executive di Sony hanno ricevuto phishing sotto forma di email per la verifica dell'Apple ID, che indirizzavano ad un falso form di verifica.

Da queste credenziali, sono risaliti alle credenziali dell'account Sony. Hanno iniettato un malware nella rete e rubato dati.

https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

Phishing

Caso di Studio: Ukraine Power Plant

2016. Advanced Persistent Threat. Hacker esperti che si sono infiltrati segretamente nel periodo di mesi e mesi. Non necessariamente state-sponsored in partenza.

Hanno rubato le credenziali di un operatore tramite phishing, e poi pianificato e lanciato un attacco coordinato. Rimpiazzato il firmware delle macchine. Non tutto è ancora stato ripristinato.

https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

Phishing

Call to Action

Gli attaccanti vogliono sollecitare la vittima ad agire, meglio se immediatamente, così da evitare che rifletta sul contenuto del messaggio di phishing.

Il Phishing sfrutta le tecniche di Social Engineering per suscitare un senso di urgenza e/o curiosità (e/o altri Motivatori), spingendola ad agire avventatamente.

Senza una “Call to Action”, la vittima difficilmente reagisce al messaggio.

Phishing

Tassonomia

Diverse modalità per categorizzare il phishing. Dipende da cosa volete comunicare, e dal vostro ambito di lavoro.

- Dispositivo da compromettere
- Vittima
- Obiettivo
- Tematica e Contenuto
- Metodo di “Exploitation”
- Tematica
- Motivatore
- ...

Tassonomia

Dispositivo da compromettere

- Computer personale
- Computer aziendale
- Tablet
- Smartphone
- Macchinario
- Dispositivo IoT
- Aereo
- ...

Tassonomia

Vittima

- “Una persona qualunque”
- “Quella persona specifica”
- Un gruppo di persone, accomunate da uno o più aspetti (lavoro, residenza, ideali...)
- Executives
- ...

Tassonomia

Obiettivo

- Guadagno economico
- Reputazione
- Senso di sfida
- Conoscenza
- Vendetta
- ...

Tassonomia

Tematica e Contenuto

- Titolo
- Mittente
- Testo
- Link
- Software (malware)
- Firma
- Tono
- ...

Tassonomia

Metodo di “Exploitation”

- Testo
- Link
- Malware
- ...

Tassonomia

Motivatore

- Intrattenimento
- Social
- Ricompensa / Riconoscimento
- Curiosità
- Lavoro
- Urgenza
- Paura
- Opportunità
- ...

Contromisure

Come identificare e/o difendersi dal phishing?

- Educazione alla cybersecurity
- Segnalazione rapida
- Blacklist, Whitelist, Greylist
- Gestore delle password
- Autenticazione a due fattori
- Machine Learning
- Computer Vision
- Ontologia
- ...

Contromisure

Educazione alla cybersecurity

Valgono gli stessi concetti visti per la Social Engineering:

- Scetticismo e non cedere agli impulsi
- Training alla cybersecurity continuo e costante
- Indicatori buoni ed indicatori inaffidabili

Possibili modalità di training:

- Lezioni frontali
- E-learning
- Simulazioni di phishing
- Pratica con strumenti anti-phishing

Estremamente costosa (denaro, tempo, organizzazione) e con risultati non garantiti.

Contromisure

Segnalazione rapida

Il tempismo è vitale per affrontare il phishing. Segnalare un'email sospetta permette di:

- Avvisare i tecnici informatici, che potranno a loro volta avvisare l'organizzazione di possibili tentativi in corso
- Correre ai ripari dopo la compromissione dell'account, limitando i danni e bloccando l'intrusione degli attaccanti

In particolare, **segnalare di aver cliccato un'email è fondamentale**, per questo dobbiamo assolutamente evitare che le vittime nascondano il fatto ma siano invece **incoraggiate ad ammettere l'errore**.

Utile al damage control, ma non molto per la prevenzione.

Contromisure

Blacklist e Whitelist

Blacklist: Lista di domini malevoli o sospetti, e ne impediscono completamente l'invio di messaggi. Anche le aziende possono implementare blacklist personali (i.e.: Firewall).

Email Blacklist Check https://mxtoolbox.com/blacklists.aspx

Whitelist: Lista di domini ritenuti affidabili e possono superare automaticamente i controlli. Attenzione a non abusarne, in quanto le whitelist possono essere exploitate nel caso un dominio venga improvvisamente compromesso.

Contromisure ottime ma macchinose e per nulla precise, specialmente contro domini appena creati.

Contromisure

Gestore delle password

Tipicamente sotto forma di una componente aggiuntiva dei browser. Ricordano siti e credenziali dell’utente.

Di fronte a siti malevoli con una grafica simile alla controparte legittima, ma con URL differente, avvertono l’utente di un possibile tentativo di phishing.

Molto efficaci verso questa modalità di phishing, ma poco popolari. Possono comunque creare altre falle di sicurezza.

Contromisure

Autenticazione a due fattori

Un metodo di accesso con un limitata adozione, se non per applicazioni che necessitano di alta sicurezza (e.g.: online banking). Prevede l'accesso tramite più di una modalità (solitamente login + codice sul telefono).

Contromisure estremamente efficace, ma scarsamente popolare per la scomodità causata agli utenti.

Può essere aggirata con Social Engineering ("ho sbagliato a scrivere il mio numero mi passi il codice che ti è arrivato?"), o se il telefono è stato compromesso.

Contromisure

Machine Learning

Grazie a machine learning e data mining, sono stati creati algoritmi altamente performanti per il riconoscimenti dei messaggi di phishing. Riconoscono pattern “inesistenti” per la mente umana, tramite clustering ed anomaly detection. Tutto questo grazie alla capacità di processare enormi quantità di dati per il training.

Una contromisura essenziale, adottata su vari livelli da qualsiasi provider di posta elettronica, ed in continua evoluzione.
Tende ad essere vulnerabile a nuove iterazioni degli attacchi.

Contromisure

Computer Vision

Gli algoritmi che sfruttano computer vision possono comparare, a livello grafico/visivo, se la pagina web attuale sia autentica oppure una copia dell'originale, grazie alla capacità di notare i più piccoli dettagli.

Come per i gestori delle password, questa contromisura è specializzata ad identificare i siti web clonati.
Più costosa di una semplice analisi del testo e non molto popolare.

Esempi

Advance Fee (“419”, “Nigerian Prince”) Esempio

La promessa di guadagnare un’enorme somma di denaro, al prezzo di un piccolo pagamento anticipato.

Esempi

Romance (Catphishing) Esempio

Messaggi volti a creare una relazione sentimentale con il destinatario, per poi chiedere denaro, informazioni e/ favori.

Esempi

Corriere Amazon / FedEx Esempio

Avvisi di consegna di pacchi inesistenti, per spingere il destinatario a pagare oppure a fare login su un sito web clonato.

Esempi

Gift Card / Lotteria Esempio

Messaggi che annunciano fantomatici premi vinti per caso.

Esempi

Rinnovo Password Esempio

Messaggi che avvertono il destinatario di dover aggiornare la propria password per motivi tecnici o di sicurezza.

Esempi

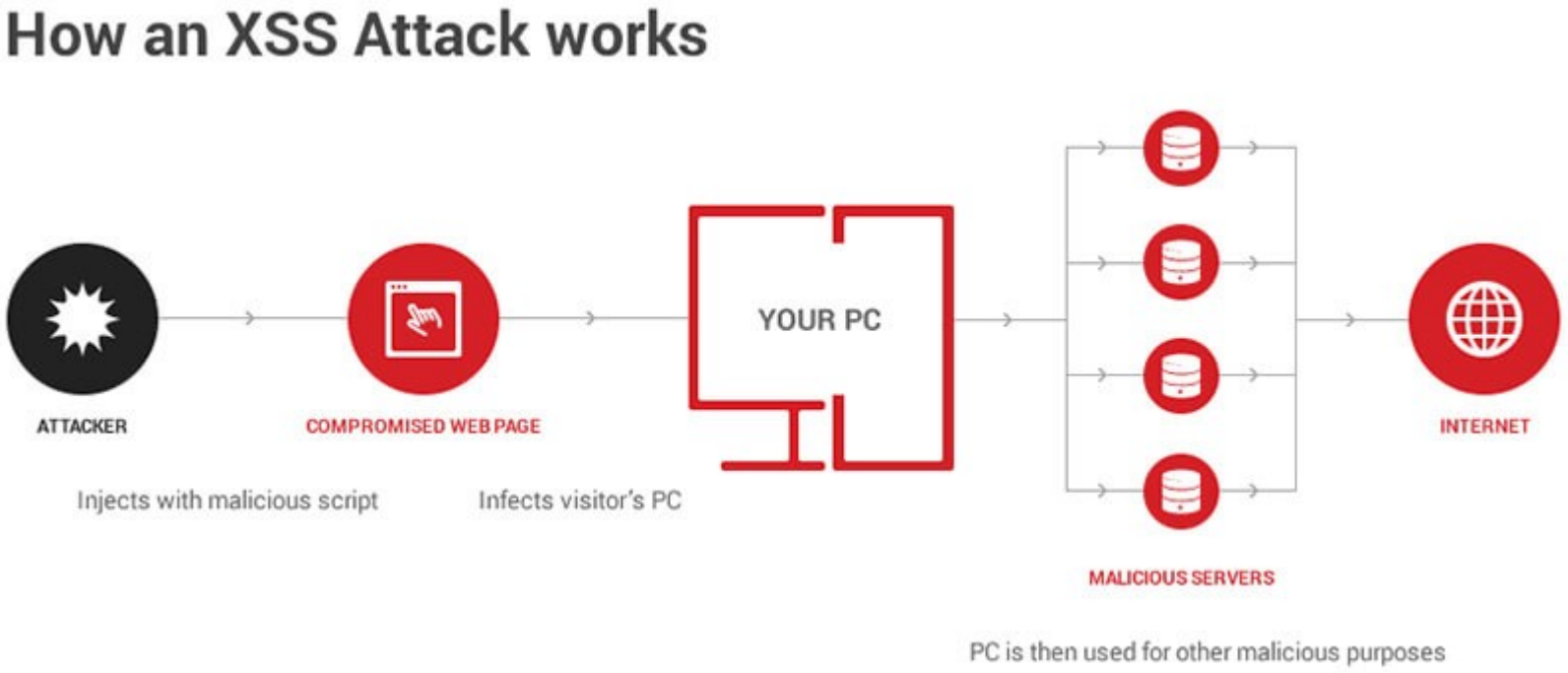
Spearphishing Example

Phishing perfezionato per essere il più efficace possibile contro un determinato gruppo di individui, che condividono una o più caratteristiche. Necessita di informazioni specifiche acquisite tramite recon.

Siti web

XSS (Cross Site Scripting) Per approfondire

Injection di script malevoli tramite pagine web, che permettono di ottenere cookie, sessioni, credenziali ed altri dati sensibili di un sito web.



Malware

Qualsiasi tipologia di software malevolo, che può essere incorporato in una grande varietà di formati file anche apparentemente innocui.

Ransomware

Uno tipo di malware che cripta i dati della vittima e chiede un riscatto, ma non è garantito che funzioni.

Office Macro

Microsoft Office (e software simili) permettono di eseguire script e macro, con funzionalità molto pericolose (e.g.: download ed esecuzione di file da Internet). Gli utenti spesso non sono consapevoli e prestano poca attenzione a tale rischio.

Manipolazione URL

URL contraffatti

Gli URL sono buoni indicatori della legittimità dei messaggi, ma solo se conosciuti. Se estremamente lunghi, oppure sconosciuti, non danno alcuna certezza.

In particolare, è facile creare nuovi domini estremamente simili a quelli legittimi, che differiscono di qualche lettera, oppure utilizzano manipolazioni ingannevoli.

Manipolazione URL

Esempi di URL contraffatti

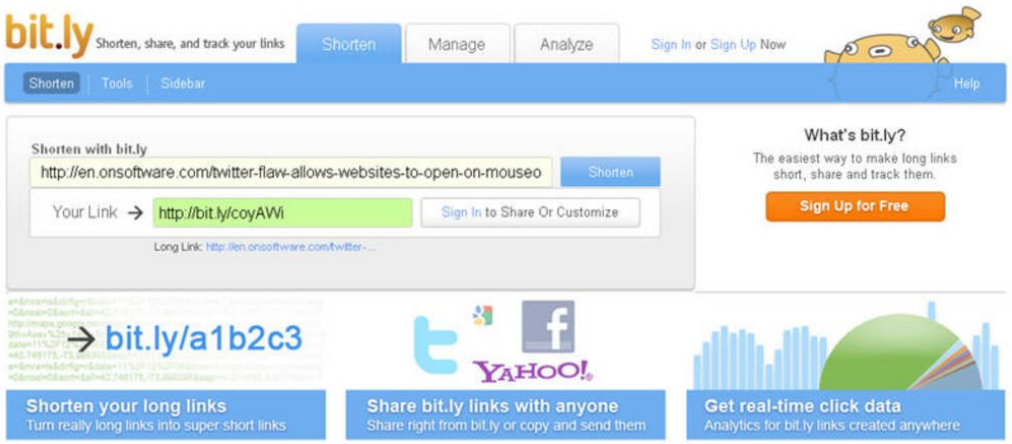
mario.rossi@scienze.unipd.it

mario.rossi@scienze-unipd.it
mario.rossi@scienze.uniqd.it
mario.rossi@scienze.unipd.it.uniweb.ru

URL Shorteners

Su Internet sono disponibili diversi servizi per abbreviare gli URL e renderli più comodi da usare.

Tuttavia, questo maschera il loro vero contenuto, senza possibilità di verifica preventiva (“hovering”) e dunque essi diventano un perfetto strumento per gli attaccanti.



Manipolazione URL

URL Padding

Su dispositivi con schermo ridotto (i.e.: smartphone), è molto più facile far “sforare” il nome dell’indirizzo web oltre la barra degli indirizzi del browser.

Indirizzo visto da computer

Indirizzo visto da smartphone

Education

Quattro punti chiave per difendersi dal phishing

1) Non cedere all’istinto (“call to action”)
2) Controllare la legittimità del dominio del mittente (“reply-to”)
3) Controllare la legittimità dei link esterni (“hovering”)
4) Nel dubbio, contattare il personale IT