Il Phishing Assessment per la Sicurezza Aziendale

Il phishing è uno dei metodi di attacco più comune, sfrutta come tecnica principale il Social Engineering e viene utilizzato per compromettere le credenziali e rubare dati sensibili.

Attraverso il phishing, gli aggressori inviano messaggi di posta elettronica che sembrano essere legittimi e possono contenere nomi, indirizzi e-mail e loghi di organizzazioni fidate (es. Banche, negozi al dettaglio, agenzie governative).

La tecnica di contraffazione degli indirizzi di posta e dei nomi è chiamata spoofing e per tutta la mail sono spesso utilizzate parole che esprimono un senso di urgenza, puntando sulle emozioni umane al fine di forzare un errore dell'utente.

Nella totalità delle campagne di phishing c'è necessità di un fattore comune per andare a segno.
Questo fattore comune è l'uomo, infatti l'errore umano è essenziale per la riuscita di un attacco di questo genere.

Altre tipologie di phishing possono essere così classificate:

- **Spear phishing**
  Si tratta di un attacco mirato verso un individuo o una compagnia.
- **Clone phishing**
  Tipologia di phishing in cui una mail legittima viene modificata e reinoltrata ai medesimi interlocutori, dichiarando di essere una versione aggiornata.
- **Whaling**
  Si tratta di attacchi di phishing indirizzati verso alte figure aziendali o di enti.
  Lo scopo è di ottenere delle credenziali di un manager.
  Il contenuto della mail viene creato su misura per

l’obiettivo.

Negli ultimi mesi in Italia abbiamo avuto un’impennata di attacchi di phishing ai danni di aziende e privati.

Secondo le statistiche del mese di Giugno, elaborate dal C.R.A.M. (Centro Ricerche Anti-Malware), hanno fatto da padrone attacchi di tipo “commerciale”, che hanno come obiettivo, quello di ottenere credenziali di accesso a conti bancari, caselle di posta elettronica e altro.

Osservando anche il trend degli ultimi anni, facendo riferimento alla tabella presente in Wikipedia, possiamo notare un massiccio incremento annuale degli attacchi, ciò anche per via della maggiore disponibilità di apparati per la navigazione ormai alla portata di tutti.

https://it.wikipedia.org/wiki/Phishing

L’Italia è stata impattata maggiormente da Trojan di tipo bancario:

- *UrSnif*
- *ZeuS Panda*
- *GootKit*

Le funzioni principali di questi trojan sono:

- Catturare screenshot
- Rubare password di varia tipologia
- Rubare i cookie
- Rubare certificati
- Avviare un proxy SOCKS
- Esfiltrare le informazioni dell’utente
- Scaricare e installare nuovi malware

L’utente finale, molte volte, non si accorge neanche di cosa accade dopo aver cliccato un link o dopo aver aperto un

allegato, il più delle volte ha modo di capirlo solo dopo aver visto svuotarsi il proprio conto in banca o perché non ha più accesso alla propria casella di posta elettronica.

Quindi, dare ai dipendenti che cliccano su un link, la possibilità di avere un immediato riscontro in ambiente controllato, tramite un "alert" che indica che sono appena caduti vittime di un test, permette un apprendimento maggiore sul phishing e su come avrebbero potuto rilevare che si trattava di un attacco.

Le mitigazioni delle campagne di phishing si possono basare su due macro-categorie

1. Hardware e Software
2. Formazione dell'utente finale

Nella categoria *HARDWARE E SOFTWARE* possono essere raggruppati tutti quei dispositivi atti ad applicare determinate regole, signature o IoC (Indicator of Compromise) che bloccano il flusso prima che le email arrivino a destinazione.
Per citarne alcuni: firewall, antispam, feed ecc…

Per la formazione dell'utente finale, occorre pianificare degli attacchi simulati e organizzare piani di formazione continui, tenendo presente che gli attacchi di phishing, basandosi sul Social Engineering, mutano per essere sempre più sofisticati, anche perché per andare a segno, devono far leva sull'ingenuità dell'obiettivo.

Senza una corretta formazione e informazione, si è sempre soggetti a rischio tenendo conto che gli apparati Hardware e Software non sono infallibili.
Tale processo è utile per identificare quei dipendenti che potrebbero richiedere ulteriore formazione e, quindi, renderla partecipe dei rischi cibernetici che possono esserci dietro un semplice click.

Un proverbio della saggezza popolare recita:

“Chi si è scottato con l’acqua calda, ha paura anche di quella fredda”.

Il phishing assessment potrebbe essere quindi una soluzione completa per un’azienda che richieda un piano strategico sulla sicurezza informatica aziendale.

Un’attività di questo tipo si snoda principalmente in 3 fasi:

1. Analisi degli obiettivi
2. Campagna di phishing
3. Analisi dei risultati in base alle attività degli utenti

Nel primo punto, di regola, vengono richiesti gli indirizzi email oggetti di attacco e più informazioni possibili, in modo da poter creare template, URL e allegati in base alle richieste.
Alcune aziende fanno richiesta di una simulazione partendo dalle sole informazioni che si possono reperire in rete, in questo modo, l’attacco simulato sarà molto simile a un vero e proprio attacco mirato.

Nel secondo punto, si settano tutti i parametri prima dell’inizio della campagna, in modo da avere la possibilità di seguire l’evolversi degli eventi in tempo reale. Le mail possono contenere link oppure allegati e che spingono gli utenti ad effettuare delle azioni mentre sono monitorati.

Nel terzo invece, si ha l’analisi dei dati raccolti, la stesura di un rapporto e l’eventuale ingaggio di un formatore che possa istruire i dipendenti al corretto utilizzo della rete e fornire le basi della sicurezza informatica.

Le metriche di valutazione fornite nel rapporto, possono essere anche utilizzate per evidenziare e potenziare i punti deboli nelle policy di gestione e configurazione della posta elettronica aziendale e settare altri apparati hardware e software.

Buona regola sarebbe quella di prevedere più sessioni a distanza di pochi mesi per valutare l'efficacia del programma di formazione.

Sono presenti pochi tool online di tipo Open Source e la documentazione in rete, specialmente in lingua italiana non è proprio copiosa.

Uno strumento Open Source degno di nota è "Gophish Open-Source Phishing Framework ".

Repository ufficiale: https://getgophish.com

Ottimo strumento completamente personalizzabile, offre una dashboard dove osservare l'evolversi della campagna in tempo reale, gestire la lista degli obiettivi in maniera semplice e intuitiva.

Molto flessibile anche a riguardo dei sistemi operativi, poiché è disponibile per Windows, Mac OSX, e Linux.

Riferimenti:

*Statistiche del mese di Giugno elaborate dal C.R.A.M. (Centro Ricerche Anti-Malware),
https://www.tgsoft.it/italy/news_archivio.asp?id=944

URSNIF
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-the-multifaceted-malware/

ZeuS Panda
https://en.wikipedia.org/wiki/ZeuS_Panda

Gootkit
https://www.cyber.nj.gov/threat-profiles/trojan-variants/gootkit

Repository ufficiale Gophish:
https://getgophish.com

A cura di: **Sergio Caruso**

L’articolo Il Phishing Assessment per la Sicurezza Aziendale proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/il-phishing-assessment-per-la-sicurezza-aziendale/