Executive Summary

Come si sfrutta la debolezza del sistema operativo umano

Raj Samani, CTO EMEA

Charles McFarland, Senior Research Engineer per MTIS

intel Security

Molti attacchi informatici contengono un elemento di social engineering, che tenta di convincere il soggetto preso di mira a eseguire un'azione che provoca un'infezione o la divulgazione di informazioni preziose.

Benché in caso di attacco l'intervento di remediation sia di carattere tecnico, sul piano umano il risultato è la colpevolizzazione della vittima e la richiesta di una maggiore consapevolezza dei problemi di sicurezza. Eppure, in realtà, la maggior parte delle organizzazioni non si sforza più di tanto per capire perché l'obiettivo è stato sfruttato e, soprattutto, per capire che cosa fare per ridurre il rischio di ulteriori attacchi — a parte migliorare la consapevolezza degli utenti.

L'espressione "social engineering" può essere definita come:

> *L'applicazione deliberata di tecniche ingannevoli studiate per manipolare un soggetto e indurlo a divulgare informazioni o a eseguire azioni che possono determinare la divulgazione di informazioni.*

Durante un attacco di social engineering, la vittima non si rende conto che le azioni che esegue arrecano un danno. Il social engineer sfrutta gli istinti innocenti del suo obiettivo, non quelli criminali. Gli attacchi si possono suddividere in due categorie:

- Hunting - mira a ottenere informazioni con il minimo di interazione con l'obiettivo. In genere in questo tipo di attacco l'incontro è uno solo e l'aggressore interrompe la comunicazione una volta acquisite le informazioni.
- Farming - mira a instaurare un rapporto con l'obiettivo, e a "spremerlo" per ottenere informazioni per un periodo di tempo prolungato.

Gli attacchi di social engineering che sfruttano l'email come canale di comunicazione in genere adottano principalmente la tecnica dell'hunting, anche se non mancano le eccezioni: ad esempio, le "truffe alla nigeriana" o "419 scams", che tentano di prolungare l'attacco per estorcere ulteriori fondi. Solitamente, gli attacchi di social engineering che utilizzano l'hunting e il farming prevedono quattro fasi:

1. Ricerca: questa fase facoltativa ha lo scopo di raccogliere informazioni sull'obiettivo. L'aggressore cerca informazioni che lo aiutino a creare una trappola efficace, ad esempio individuando gli hobby, il luogo di lavoro o il fornitore di servizi finanziari della vittima.
2. Trappola: ha lo scopo di favorire il successo della fase di "esecuzione" coinvolgendo il soggetto e fornendo un pretesto per l'interazione. Lo psicologo Robert Cialdini cita sei fattori di influenza che mirano a far leva sul subconscio dell'obiettivo:
   - Scambio: viene fornito qualcosa per cui la persona si sente obbligata e in seguito cerca di ricambiare il favore.
   - Scarsità: la gente tende a soddisfare le richieste quando crede che qualcosa scarseggi.
   - Coerenza: quando gli obiettivi hanno promesso di fare qualcosa, manterranno la parola data perché non vogliono sembrare inaffidabili.
   - Gradimento: il social engineer ha maggiori probabilità di indurre gli obiettivi a soddisfare le sue richieste se le vittime lo trovano simpatico.
   - Autorità: sfrutta la tendenza dell'uomo a obbedire quando una richiesta proviene da una figura autorevole.
   - Convalida sociale: la tendenza a uniformarsi quando anche gli altri fanno la stessa cosa.

3. Esecuzione: l'attuazione della parte principale dell'attacco. Può trattarsi della divulgazione di informazioni, di un clic su un link, di un trasferimento di fondi, ecc.
4. Uscita: l'interazione viene interrotta. Anche se defilarsi senza destare sospetti può essere un vantaggio in molti attacchi di farming, non sempre è necessario. Ad esempio, quando manipolano le vittime inducendole a divulgare i dati di una carta di pagamento, gli aggressori in genere non desiderano destare sospetti, per paura che i malcapitati segnalino lo smarrimento o il furto della carta con conseguente annullamento. Se invece gli aggressori riescono a sottrarre codice sorgente o altre informazioni personali, la vittima non sarà in grado di recuperare i dati rubati, anche qualora abbia dei sospetti.

I tentativi di social engineering non sono necessariamente lineari; un singolo attacco può far parte di una campagna molto più ampia per la raccolta di più frammenti di informazioni correlate. Ad esempio, gli aggressori possono sferrare un attacco, recuperare le informazioni e sparire. Oppure possono sferrare una serie di attacchi di hunting e, con le informazioni così ottenute, avviare un attacco di farming.

Canali di attacco

I social engineer possono seguire varie strade per sferrare gli attacchi.

- Siti web: gli attacchi di social engineering spesso sfruttano come canale di attacco dei siti web malevoli. Secondo il *2014 Verizon Data Breach Investigations Report* (Rapporto investigativo Verizon sulla violazione di dati 2014), "il 20% degli attacchi a scopo di spionaggio si serve della compromissione di un sito web strategico per distribuire il malware".
- Email: le forme più comuni di social engineering tramite email sono il phishing e il più sofisticato spear phishing. Per i criminali informatici l'email è un metodo efficace, poiché secondo il rapporto Verizon "il 18% degli utenti fa clic su un link contenuto in un'email di phishing".
- Telefono: è un canale ampiamente sfruttato da chi commercia in informazioni.
- Contatto diretto: un dipendente può essere avvicinato e convinto con l'inganno o costretto a fornire informazioni.
- Servizio postale: anche se questo canale sembra meno diffuso di altri, sono stati comunque segnalati attacchi di social engineering attuati tramite posta tradizionale.
- Fax: ad esempio, email che fingono di essere messaggi inviati da servizi di pagamento online.

Difendersi dal social engineering

Per mitigare il rischio costituito dal social engineering si possono utilizzare i seguenti tipi di controlli, suddivisi in tre categorie: personale, processi e tecnologia. Non si tratta di un elenco completo, e queste forme di controllo potrebbero non essere applicabili a tutte le organizzazioni.

Personale

- Stabilire dei limiti precisi: tutto il personale deve essere perfettamente al corrente delle policy riguardanti la divulgazione di informazioni e sapere esattamente a quale superiore rivolgersi nel caso in cui una richiesta non rientri nei limiti previsti.
- Adottare la formazione continua: implementare un programma di sensibilizzazione ai problemi della sicurezza per la formazione continua dei dipendenti nel tempo. Utilizzare strumenti come il Quiz McAfee sul phishing per evidenziare le tattiche specifiche adottate con maggiore frequenza negli attacchi.
- Autorizzare alla verifica: autorizzare il personale a contestare senza timore anche le richieste apparentemente innocue. Un esempio può essere chiedere di identificarsi alle persone che tentano di intrufolarsi negli uffici.

- Insegnare l'importanza delle informazioni: anche informazioni apparentemente innocue come i numeri di telefono (un'informazione che conferisce potere) possono essere utilizzate per allestire un attacco.
- Creare una cultura che non colpevolizzi: gli obiettivi dei social engineer sono vittime. Punire determinati dipendenti perché si sono lasciati ingannare aumenterà la reticenza di tutto il personale ad ammettere di avere divulgato informazioni. Una volta subito il raggiro, questi soggetti potrebbero ritrovarsi alla mercé del social engineer, che in seguito potrebbe ricattarli.

Processi

- Segnalazione delle telefonate o delle visite sospette: quando si è verificata un'attività sospetta, il personale deve redigere un rapporto che spieghi in modo dettagliato come si è svolta l'interazione, per facilitare le indagini.
- Pagine di blocco informative: quando i dipendenti cercano di accedere a una pagina web malevola, utilizzare una pagina di blocco per spiegare loro perché non possono procedere. In questo modo rifletteranno sull'azione che li ha condotti a quella pagina e sarà più semplice individuare da dove proviene l'attacco.
- Notifiche ai clienti: quando un dipendente rifiuta di divulgare informazioni per telefono, l'organizzazione deve comunicarlo all'autore della telefonata e verificare se avesse effettivamente diritto di ottenere le informazioni richieste. Le organizzazioni devono inoltre riflettere su come comunicano con i clienti. Ad esempio, PayPal include nelle sue comunicazioni una dicitura che aiuta gli utenti a capire se le email che ricevono sono autentiche: "Nei nostri messaggi email non ti chiederemo mai il numero di conto corrente, il numero della carta di credito o di debito e simili. Inoltre, in un messaggio email non ti chiederemo mai nome e cognome, la password del tuo account o la risposta alle domande di sicurezza di PayPal."
- Percorso di escalation: un percorso di segnalazione chiaro che consenta al personale del front line di comunicare ai superiori eventuali dubbi in merito a interazioni con messaggi potenzialmente fraudolenti.
- Tiger test: sottoporre il personale a test periodici per verificarne la suscettibilità agli attacchi di social engineering sferrati mediante svariati canali di comunicazione. Si disporrà così di uno strumento per misurare l'efficacia dei programmi di formazione.

Tecnologie

- Registrazione delle telefonate: registrare tutte le telefonate in entrata per facilitare eventuali indagini.
- Linee fasulle: trasferire le chiamate sospette a un numero sottoposto a monitoraggio.
- Filtraggio delle email: eliminare le email fraudolente contenenti malware, sia di tipo noto che sconosciuto.
- Filtraggio web: bloccare l'accesso ai siti web malevoli e rilevare il malware inline con l'accesso a Internet.
- Autenticazione forte: anche se non azzera il rischio che gli utenti vittime del social engineering divulghino le loro credenziali, l'autenticazione a più fattori renderà l'operazione più difficile per i potenziali aggressori.

Segui McAfee Labs

Sintesi

Il social engineering è un pericolo estremamente concreto. I criminali informatici se ne servono per estorcere illegalmente informazioni e utilizzarle poi per svariate attività fraudolente. Per affrontare al meglio il problema è necessario capire la natura degli attacchi di social engineering: occorre dunque definire i probabili autori degli attacchi, i metodi che utilizzano e le loro risorse e applicare i controlli più adeguati per ridurre il rischio che un attacco vada a buon fine.

Una copia del rapporto completo è disponibile all'indirizzo **www.mcafee.com/hacking-human-os.**

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com