Email Security: Tipologie di attacchi veicolati tramite email e pratiche di sicurezza

Spam

Anche note con l'acronimo **UCE** (**Unsolicited Commercial Email**), sono messaggi pubblicitari indesiderati inviati tendenzialmente a un elevato numero di utenze. Gli spammer e i cybercriminali con l'invio di mail di spam hanno l'obiettivo di:

- Raccogliere informazioni dai destinatari;
- Diffondere codice malevolo;

Può essere considerato come spam anche tutto ciò che proviene da un'utenza sconosciuta con qualsiasi tipo di contenuto indesiderato.

Phishing

Sono mail inviate da fonti apparentemente affidabili e note (come, ad esempio, istituti finanziari o aziende) e inducono l'utente che l'ha ricevuta a compiere delle azioni al fine di ottenere informazioni sensibili come: username, password, dati finanziari e/o indurlo all'esecuzione di malware. I messaggi di phishing spesso contengono link fraudolenti in cui si invitano gli utenti a fornire informazioni confidenziali rispondendo direttamente all'email o cliccando sul link malevolo. Gli attacchi di phishing possono avere una vasta gamma di obiettivi a seconda dell'attaccante, come ad esempio, la generica truffa che mira ad ottenere informazioni bancarie/postali. Il phishing può essere di numerose categorie, tra cui:

- **Spear Phishing**: più mirata e specifica, in quanto i cybercriminali si concentrano su un individuo o un'organizzazione specifica. Utilizzano informazioni dettagliate per personalizzare i messaggi rendendo così più probabile che le vittime cadano nella trappola. In alcuni casi le campagne di phishing possono essere mirate alle alte sfere aziendali (CEO, CISO ecc), in questo caso si parla anche di **Whale Phishing.**
- **Smishing**: è un attacco che, per la sua esecuzione, utilizza i messaggi di testo o gli SMS. Una tecnica comune di smishing consiste nell'inviare un SMS contenente un collegamento cliccabile o un numero di telefono da richiamare. Un esempio comune è un SMS che sembra provenire dal proprio istituto bancario. Il contenuto afferma che il conto è stato compromesso e che è necessario agire immediatamente. L'attaccante chiederà di cliccare nel link dell'SMS e di verificare numero di conto corrente bancario, codice fiscale, ecc. Una volta inserite, l'aggressore potrà utilizzarle per acquisire il controllo del conto bancario e realisticamente svuotarlo in breve. In figura 3 due chiari esempi di smishing:

Figura 3. Esempi di smishing

- **Vishing:** questo attacco viene eseguito tramite una chiamata vocale, da qui la "v" al posto delle lettere "ph" nel nome. Un comune attacco di vishing include una chiamata da qualcuno che afferma di essere un rappresentante di un'azienda o un determinato ente (Microsoft e simili). Questa persona, fingendo di voler aiutare, informa l'utente di aver rilevato, ad esempio, una violazione nella sua macchina o l'individuazione di un malware e chiede quindi al malcapitato di fornire informazioni personali (come possono essere carta di

credito o username e password) per poi successivamente indurlo a installare un software malevolo o ad effettuare operazioni in suo favore.

Spoofing

E’ una tecnica che utilizza l’impersonificazione come mezzo per rubare informazioni importanti o accedere a conti bancari. Questa pratica viene usata in vari contesti come:

- **Spoofing dell’indirizzo IP**, l’invio di messaggi ad una macchina usando un indirizzo IP mascherato come attendibile.
- **Spoofing di mail**, la modifica dell’header from di una mail per farla sembrare proveniente da qualcuno o qualcosa di diverso dalla fonte effettiva.
- **Spoofing del DNS**, modifica del server DNS al fine di dirottare un nome di dominio specifico verso un indirizzo IP diverso.

Lo spoofing, quindi, è un tipo di impersonificazione che cerca di ingannare una rete o un essere umano per fargli credere che la fonte di determinate informazioni sia attendibile. Gli attaccanti, ad esempio, utilizzano questa tecnica per inviare mail che appaiono come provenienti da qualcuno di fidato, in modo da spingere l’utenza a fornire dati sensibili. In alternativa, possono provare ad utilizzare lo spoofing dell’IP e del DNS per dirottare l’utenza su siti fraudolenti che tenteranno poi di infettare la macchina destinataria.

Business Email Compromise (BEC)

Gli aggressori compromettono un account aziendale e utilizzano l’accesso per condurre frodi finanziarie e truffe. Possono inviare richieste di trasferimenti di denaro e/o ottenere informazioni aziendali sensibili. Secondo un report dell’FBI,

nel 2018 ogni giorno, circa 400 aziende sono state vittime di attacchi tramite BEC e che nella maggior parte dei casi gli obiettivi erano gli addetti dello staff finanziario. È stato stimato inoltre che il totale delle perdite, solo nel periodo tra ottobre 2013 e maggio 2018, salì all'astronomica cifra di 12.536.948.299 USD.

Malware tramite email

I cybercriminali possono distribuire malware inviando email con allegati dannosi. Se l'utente viene indotto ad aprire l'allegato, il malware può infettare il sistema, consentendo agli aggressori di prendere il controllo e/o rubarne i dati. Tra i malware più noti vi è "**Emotet**" un malware bancario diffuso nel 2014 e ancora tutt'oggi utilizzato. La sua peculiarità di questo malware è quella di favorire la propagazione di altri malware scatenando un'infezione multipla. Tra i malware più diffusi da Emotet ci sono: **Trickbot** (trojan bancario), **Quakbot** (trojan) e **Ryuk** (ransomware). In questa categoria viene inclusa dunque anche una delle minacce più rilevanti degli ultimi decenni, ovvero il **Ransomware**. Gli utenti, in questo caso, ricevono un'email contenente un link o un allegato dannoso. Se l'utente apre il file o clicca sul link, il ransomware infetterà il sistema cifrandone tutti i file. Successivamente, gli aggressori chiederanno un riscatto per rilasciare la chiave di decriptazione. Secondo l'IBM Security X-Force Threat Intelligence, gli attacchi ransomware hanno rappresentato il 17% di tutti gli attacchi informatici solo nel 2022. Questa tipologia di malware è talmente diffusa che da molti anni ormai si parla anche di "**Ransomware-as-a-service (RaaS)**" ovvero un modello di business per i criminali informatici in cui viene venduto il codice ransomware ad altri hacker che a loro volta metteranno in atto attacchi ransomware per poi successivamente quindi chiedere un riscatto (tipicamente in bitcoin) per decriptarne i dati dei mal capitati. In quest'ultimo caso è fondamentale avere e programmare dei

backup periodici (salvati su sistemi esterni) per evitare di pagare e/o perdere i propri dati.

Man-in-the-Middle (MitM)

In questo tipo di attacco, viene intercettata e/o modificata la comunicazione tra due parti. Gli attacchi MitM possono essere eseguiti anche attraverso email, dove gli aggressori cercano di intercettare e/o manipolare i messaggi in transito. Per questo tipo di minacce è fondamentale:

- Non usare comunicazioni non cifrate;
- Utilizzare protocolli sicuri come SSL/TLS e HTTPS;
- Utilizzare almeno la WPA2 encryption;

Zero-Day

Ovvero vulnerabilità di un software non note, ai suoi sviluppatori o da essi conosciuta ma non gestita, utilizzate per compromettere molteplici sistemi. Gli aggressori possono inviare email con allegati o link che sfruttano queste vulnerabilità prima che vengano corrette. Per fronteggiare queste questo fenomeno molte case produttrici di software utilizzano dei “mercati intermediari” in cui vengono convalidate le vulnerabilità zero-day scoperte e, in base alla loro criticità, pagano coloro che l’hanno segnalata. Tra le realtà più consolidate ci sono:

- zeronomi.com
- zerodium.com
- netragard.com
- zerodaytechnology.com
- zerodayinitiative.com

I siti di questo tipo sono completamente legali, in quanto si limitano a validare e retribuire le vulnerabilità scoperte dai diversi “ethical hacker” e simili. Un altro modo per mitigare e/o individuare queste vulnerabilità, oltre alla condivisione

delle informazioni (fondamentale per la cyber defense), è fare un uso di **sandbox** al fine di individuare prontamente comportamenti "inattesi".

Per proteggersi dagli attacchi veicolati tramite email, è quindi fondamentale adottare pratiche di sicurezza come:

- L'uso di soluzioni di email security;
- Investire sulla formazione dei dipendenti aumentandone la consapevolezza delle minacce veicolate tramite email;
- L'implementazione di politiche di sicurezza rigorose;

Tra i sistemi di sicurezza necessari al rafforzamento del perimetro difensivo in merito all'email security abbiamo:

- **Antivirus e antimalware** necessari a rilevare e bloccare malware e/o ransomware presenti negli allegati delle email.
- **Firewall perimetrali** multilivello per monitorare, filtrare ed eventualmente bloccare attività considerate non legittime. L'uso dei firewall va combinato anche con gli IPS/IDS.
- **Filtri antispam** per bloccare messaggi indesiderati (spam, phishing ecc.) riducendo così il rischio di cadere in truffe o fornire informazioni sensibili.
- **Sistemi di autenticazione** e **firme digitali** per garantire che le email provengano da fonti non malevole e che quindi non siano state compromesse durante il trasferimento. Rigettando quindi ogni mail che non abbia la configurazione attesa.
- Algoritmi di **crittografia** per proteggere i contenuti delle email durante la trasmissione in modo che solo il destinatario autorizzato possa decifrarli garantendo così l'integrità del messaggio.
- **Training per i dipendenti**, con apposite "campagne awareness" allo scopo di sensibilizzarli sulle minacce informatiche provenienti dalla posta elettronica. Tra le pratiche su cui si deve lavorare, ad esempio, c'è quella

di indurre i dipendenti a porre maggior attenzione alle mail provenienti da utenze sconosciute invitandoli quindi ad evitare di aprire allegati o cliccare su link sospetti.

- **Politiche di sicurezza aziendali** regolando l'uso delle email definendo procedure di sicurezza che stabiliscano criteri per la gestione delle informazioni sensibili. Ad esempio, come in figura 4, utilizzando appositi tag per classificare le comunicazioni (public, internal, confidential e strictly confidential) tramite email.


Figura 4. Classificazione delle comunicazioni

- **Sistemi di monitoraggio e rilevamento delle minacce** per individuare attività sospette e/o tentativi di accesso non autorizzato alle caselle di posta elettronica. Attività che può essere supportata da un team di security operation center (SOC)
- **Riduzione della superficie d'attacco**, riducendo al minimo tutti i servizi esposti e utilizzando protocolli sicuri per le comunicazioni disabilitando anche tutto ciò che non è necessario.



Questo articolo è stato estratto dal white paper "Email Security: Intelligenza Artificiale, Protocolli e Best Practice Contro gli Attacchi Informatici" disponibile in maniera libera e gratuita al seguente link: https://www.ictsecuritymagazine.com/pubblicazioni/email-security-intelligenza-artificiale-protocolli-e-best-practice-contro-gli-attacchi-informatici/

Articolo a cura di **Fabrizio Giorgione**

Profilo Autore


Fabrizio Giorgione è nato a Napoli (NA) nel 1992. Si è

laureato in ingegneria informatica presso l’università degli studi del Sannio il 17 dicembre del 2018 con una tesi dal titolo: “Analisi della superficie di un sistema SCADA”. Ha sviluppato, presso il laboratorio ISWATlab, un’applicazione Android denominata “Privacy Guard” la quale valuta il rischio di privacy leakage, ovvero il furto di informazioni, sugli smartphone (http://www.iswatlab.eu/?page_id=499). Ha effettuato il tirocinio presso lo “ZLab” di “Cse Cyber Sec” nell’ambito “SOC”, “Forensic” e “Malware Analysis”. Attualmente lavora presso la società di “NTT DATA” come “Cyber security Analyst” nel SOC di Napoli. Il suo compito è quello di effettuare analisi di log, di malware e di prevenire minacce interne ed esterne alla sua azienda e ai clienti della società. Si è occupato, inoltre, del montaggio e della gestione di sonde IDS/IPS presso Telecom Italia nella sede di Roma (RM).

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/email-security-tipologie-di-attacchi-veicolati-tramite-email-e-pratiche-di-sicurezza/