NOTA SINTETICA

Perché l'e-mail è il principale vettore di minacce

La maggior parte delle attuali e devastanti violazioni ha inizio con una semplice e-mail.

Sommario

Il phishing non consiste semplicemente nell'indurre un utente a cliccare su un link per lanciare il malware. In maniera più insidiosa, il phishing consente di rubare le credenziali degli utenti avanzati. In tal modo i criminali possono accedere al sistema, inviare e-mail, inoltrare richieste finanziarie e diffondere codice dannoso ovunque l'identità dell'utente sia autorizzata ad accedere.

La posta elettronica rimane uno dei principali vettori di minacce. Le aziende devono assicurarsi di proteggere i dipendenti da attacchi di phishing e malware avanzati che hanno inizio con metodi come Business Email Compromise (BEC), impersonificazione e frodi e-mail.

Introduzione

Ogni giorno vengono inviati circa 320 miliardi di messaggi e-mail. La posta elettronica rimane uno dei metodi principali utilizzati dalle persone per condividere informazioni e ... minacce. La pandemia di COVID-19 e le iniziative di telelavoro hanno contribuito a rendere le e-mail il canale preferenziale per ogni forma di attacchi phishing e ransomware.

Dalle violazioni di dati più recenti abbiamo imparato che gli attacchi avanzati comportano spesso diverse tattiche, tecniche e procedure per compromettere l'utente. In genere, l'e-mail è il punto di partenza per attacchi di social engineering come BEC o phishing delle credenziali.

Ad esempio, il rapporto di Verizon sulle violazioni di dati del 2020 afferma che il 22% delle violazioni ha riguardato l'ingegneria sociale e il 96% di tali violazioni è arrivato attraverso la posta elettronica. Nel rapporto si legge che un altro 22% delle violazioni è stato causato da errori umani, in cui dati sensibili sono stati inviati per errore al destinatario sbagliato.

Un altro studio condotto da 451 Research ha rilevato che, mentre l'87% delle aziende ha già installato un prodotto di sicurezza e-mail, il 46% ammette che l'e-mail rappresenta ancora il rischio più significativo per i dati. Inoltre, il 46% ha indicato la posta elettronica come la più grande vulnerabilità, quasi cinque volte superiore alla problematica immediatamente inferiore.

Microsoft e Google dominano il mercato globale della posta elettronica basata sul cloud, grazie a soluzioni integrate nelle loro suite per ufficio. La quota di mercato mondiale delle tecnologie per l'ufficio è divisa tra Google e Microsoft. A livello globale, Gmail è la piattaforma e-mail più popolare con oltre 1,8 miliardi di utenti. Alla fine del 2020, la suite Microsoft Office 365 era utilizzata da oltre un milione di aziende in tutto il mondo, di cui oltre 650.000 negli Stati Uniti.

I cybercriminali, allettati da questo enorme gruppo di potenziali vittime, investono costantemente in nuovi strumenti per truffare gli utenti di questi servizi e-mail basati sul cloud. La posta elettronica basata sul cloud è quindi uno dei vettori di attacco preferiti e più redditizi per gli hacker.

L'efficacia persistente del phishing e delle frodi e-mail

Le e-mail di phishing sono create in modo da apparire autentiche e inviate da identità note rubate o false, e possono ingannare anche gli utenti più esperti e attenti alla sicurezza. Nonostante l'impegno delle aziende nella formazione sulla sicurezza, le e-mail di phishing sono spesso l'anello debole della sicurezza. I responsabili della sicurezza con cui abbiamo parlato riferiscono di utenti che continuano a cliccare su e-mail di phishing mirate, basate su temi o eventi e personalizzate per sembrare e-mail legittime. Molti utenti non sono in grado di distinguere le e-mail legittime da quelle false, riconoscere link sospetti o adottare misure di precauzione come l'autenticazione

dell'URL, dell'identità del mittente e del sito web aziendale.

Del resto, la propagazione è una caratteristica intrinseca della natura umana. I messaggi e-mail e gli allegati scambiati tra dipendenti, partner e clienti – per non parlare della famiglia e degli amici – sono un elemento distintivo della forza lavoro remota e collaborativa di oggi. Li accettiamo perché sappiamo che provengono da identità attendibili e perché abbiamo bisogno di accedere a contenuti e informazioni per svolgere il nostro lavoro collettivo.

Business Email Compromise

La compromissione della posta elettronica aziendale (BEC) è il principale tipo di attacco di impersonificazione e frodi via e-mail. Questo tipo di attacco consiste in genere nell'utilizzare l'account di posta elettronica compromesso di un amministratore delegato o di un altro dirigente di alto livello. I truffatori utilizzano l'account compromesso per inviare richieste finanziarie fraudolente, ad esempio il pagamento di una fattura falsa o il versamento di denaro per un affare concluso telefonicamente.

Nella maggior parte dei casi, il dirottamento degli account dei dirigenti di alto livello viene realizzato tramite attacchi di social engineering o whaling delle credenziali. L'Internet Crime Complaint Center (IC3) dell'FBI riferisce che il crimine informatico ha superato i 4,1 miliardi di dollari nel 2020, con attacchi BEC pari a 1,8 miliardi di dollari, confermandosi come il vettore di minacce unico che ha causato il danno finanziario più elevato.

Quando un'azienda si accorge che le credenziali di un dirigente sono state compromesse, in genere è già troppo tardi. È sufficiente un solo account compromesso per creare una reazione virale tra gli utenti, i dispositivi o le applicazioni che può essere impossibile da contenere prima che si verifichino danni.

La sicurezza nativa del cloud non è sufficiente

Gli sviluppatori delle soluzioni di sicurezza e-mail hanno creato dei metodi per proteggere gli utenti dai link dannosi che eludono i filtri preliminari e raggiungono la casella di posta, come ad esempio la protezione click-time, il richiamo delle mail dopo l'invio e i filtri del browser web. Tuttavia, gli aggressori sono altrettanto interessati a creare metodi per entrare nella casella di posta elettronica degli utenti.

Un recente rapporto ATP di Microsoft del 2020 ha rivelato che più di un'e-mail di phishing su dieci può raggiungere la casella di posta dell'utente. Ogni singolo attacco utilizza diverse combinazioni di metodi di offuscamento appositamente progettati per eludere i filtri EOP (Exchange Online Protection) e ATP (Advanced Threat Protection) di Microsoft.

Diversi attacchi trasmessi tramite e-mail aggirano i filtri di sicurezza e-mail con un elevato grado di successo. Un esempio di questi attacchi è un'e-mail di phishing mirata a basso volume e di alta qualità che sembra provenire da Office 365 o Gmail. Ha una grafica curata, è personalizza e viene inviata a una fascia specifica di utenti piuttosto che tramite una campagna ad alto volume. Questi attacchi sono sofisticati sia per quanto riguarda la tecnica per raggiungere la casella di posta sia per l'esperienza offerta all'utente. Ogni link include generalmente l'indirizzo e-mail dell'utente, in modo che la pagina di login sembri la seconda pagina che appare quando si esegue l'accesso come amministratore. Questa pagina sa chi è l'utente ed esegue analisi in background.

Le tecniche di phishing si stanno quindi evolvendo anche nella fase successiva alla consegna: invece di inserire l'URL dannoso nell'e-mail, i criminali collegano l'utente a un server di reindirizzamento, il quale agisce come un gateway che invia richieste da un'azienda di sicurezza a un sito legittimo. In realtà, i dati inviati dalle vittime designate vengono inoltrati al server di phishing.

Sebbene Microsoft ATP utilizzi quattro motori principali con regole per anti-phishing, spoof intelligence, collegamenti sicuri e allegati sicuri, si tratta comunque di una tecnologia di sicurezza basata su regole. L'analisi di sicurezza si basa esclusivamente sul filtraggio statico basato sulla reputazione, per cui gli hacker possono utilizzare tecniche di reverse engineering finché non trovano il modo di aggirare questi filtri. Questa debolezza a livello di sicurezza mette le imprese in una condizione di rischio costante, con la minaccia che qualcuno in azienda apra un file sbagliato, clicchi su un URL dannoso o digiti una password nel posto sbagliato.

La visibilità e l'accesso per un grande numero di utenti che usano l'e-mail nel cloud rendono le aziende un obiettivo semplice per ogni hacker. Le aziende non hanno mai concesso tanti account utente e caselle di posta elettronica con una protezione identica. Gli hacker sfruttano anche il fatto che questi account cloud sono utilizzabili per autenticarsi ad altre applicazioni SaaS aziendali per diffondere il malware o rubare i dati. Questo è il pericolo reale e attuale della "monocultura" della sicurezza nel cloud. Una volta eluso un controllo, si può accedere all'intero sistema.

SiteCloak è un buon esempio di questa tecnica attualmente utilizzata per eludere Safe Links, la protezione da minacce avanzate (ATP) di Microsoft 365 nota anche come protezione Click-Time. SiteCloak porta l'offuscamento del phishing a un livello superiore utilizzando diverse tattiche e tecniche per nascondere il vero intento della pagina di destinazione, che spesso è una pagina di raccolta delle credenziali.

Le vittime di SiteCloak non devono inserire il loro indirizzo e-mail. Vengono indirizzate direttamente alla pagina di immissione della password, che utilizza la tecnica "Zero Font" per eludere i controlli e-mail di Microsoft e raccogliere le credenziali. Questa tecnica inserisce caratteri casuali di dimensione zero tra i caratteri della pagina, in modo che i filtri in linguaggio naturale di Microsoft vedano il testo casuale, mentre i lettori umani vedono quello che gli aggressori vogliono che vedano. In altre parole, Safe Links la valuta come una pagina innocua, mentre in realtà è una pagina dall'aspetto realistico che raccoglie le credenziali della vittima. Gli aggressori abilitano il contenuto dannoso solo dopo che il messaggio e-mail ha raggiunto la casella di posta della vittima.

Conclusioni

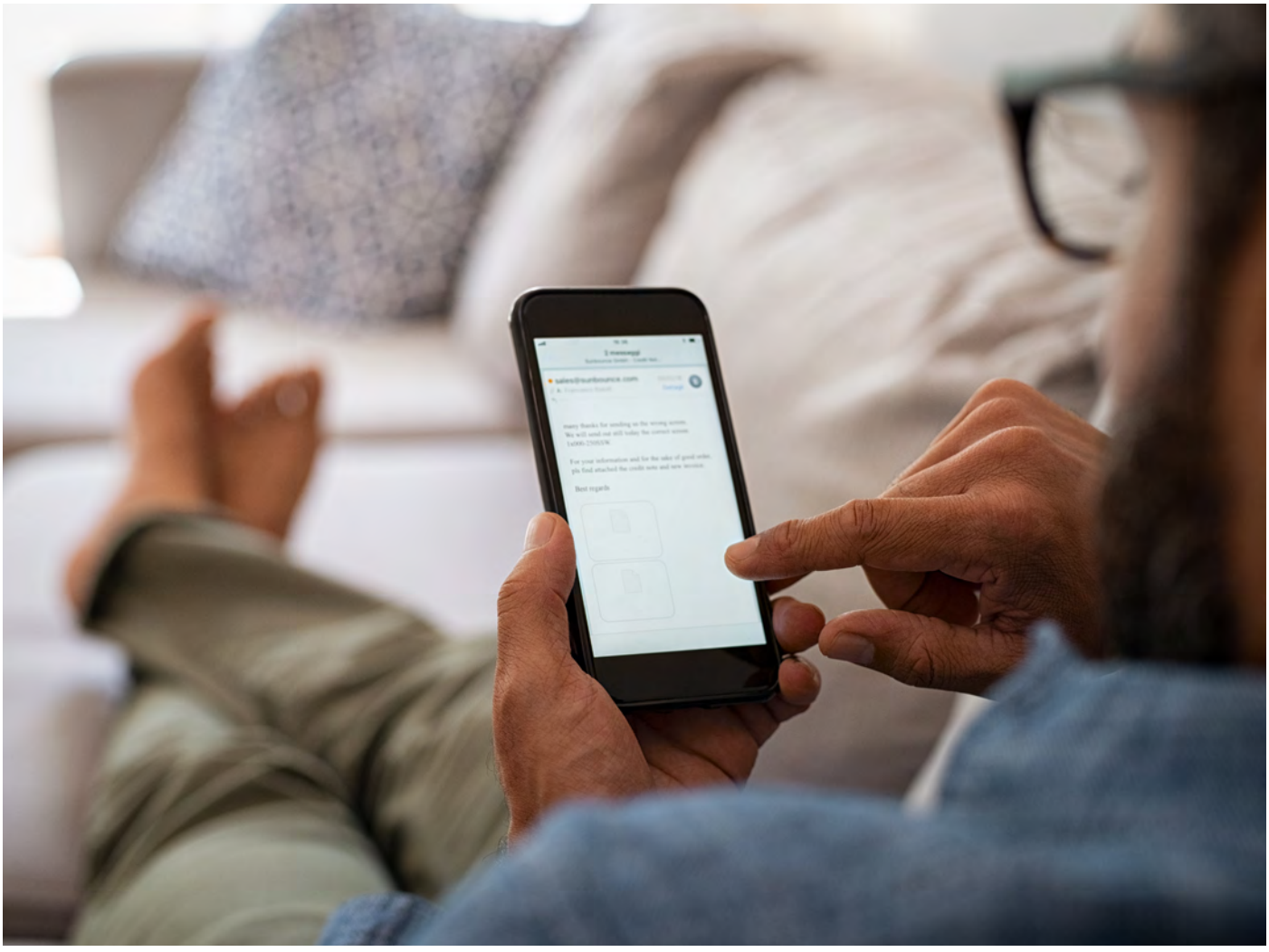
SiteCloak e altre forme di frode tramite e-mail dimostrano che gli hacker possono eludere i sistemi di rilevamento con attacchi di phishing accuratamente preparati e personalizzati. Purtroppo, questi non saranno gli ultimi attacchi in grado di eludere i filtri di sicurezza dei fornitori cloud. Le aziende hanno quindi bisogno di ulteriori livelli di protezione oltre agli strumenti di sicurezza integrati nelle suite per ufficio basate sul cloud.

SonicWall Email Security può essere utilizzato come robusta appliance virtuale, applicazione software, servizio in hosting o appliance fisica hardened, ideale per le aziende che necessitano di una soluzione on-premise dedicata. La soluzione multilivello di SonicWall offre protezione completa in entrata e in uscita. Protegge da minacce avanzate provenienti dalla posta elettronica come ransomware, minacce zero-day, spear phishing e compromissione della posta elettronica aziendale (BEC).

Per ulteriori informazioni, visitare il sito www.sonicwall.com/email-security.

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla nuova "normalità iperdistribuita", in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni, visitare www.sonicwall.com.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

ExecBrief-EmailThreatVector-A4-COG-5264