proofpoint.

EBOOK

La sensibilizzazione: un firewall efficace contro gli attacchi informatici?

Quello che gli utenti ignorano sulle minacce informatiche e perché ciò può danneggiarli

Introduzione

Secondo un vecchio detto, ciò che non conosciamo non può farci del male. Nulla è meno vero quando si tratta di minacce informatiche.

La mancanza di conoscenze relativamente alle minacce informatiche può danneggiare non solo i tuoi utenti, ma anche l'azienda nel suo complesso. I tuoi collaboratori sono un obiettivo primario degli attacchi informatici. Gli errori dovuti alla loro mancanza di conoscenze possono causare interruzioni delle attività e perdite di dati, oltre ad avere conseguenze negative sul lungo termine.

Questo eBook prende in esame gli attacchi reali che evidenziano il duplice ruolo degli utenti quali bersaglio principale dei criminali informatici e prima linea di difesa delle aziende.

Tratteremo cinque categorie principali di attacchi informatici e di altri crimini informatici che iniziano con la violazione degli utenti, o si basano su di essa.

- Phishing
- Violazione dell'email aziendale (BEC, Business Email Compromise)
- Ransomware
- Attacchi cloud
- Attacchi tramite webmail

Inoltre, presenteremo alcune conclusioni del nostro report State of the Phish 2022 per mettere in evidenza le conoscenze, le vulnerabilità e la resilienza degli utenti in queste aree. Questi dati potranno servire ai responsabili della sicurezza che desiderano proteggere i loro utenti, i loro dati e i loro marchi. Inoltre, sottolineano il perché i collaboratori sono il nuovo perimetro e di conseguenza devono essere al centro delle tue iniziative di sicurezza informatica.

SEZIONE 1

Phishing

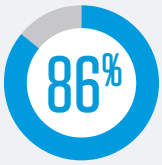
Il phishing è un tipo di social engineering.

Distribuito tramite email o SMS, i messaggi di phishing utilizzano una serie sempre più vasta di tecniche per sfruttare la psicologia umana. I criminali informatici ingannano gli utenti e li inducono a fidarsi di loro per ottenere informazioni finanziarie, credenziali d'accesso ai sistemi e altri dati sensibili.

Tendenze

Anno dopo anno, il phishing diventa uno strumento sempre più utilizzato dai criminali informatici. In base al *report 2021 sui reati di Internet* dell'FBI, il phishing e attacchi similari hanno rappresentato oltre il 38% di tutti i sospetti reati su Internet segnalati negli Stati Uniti lo scorso anno. Nel 2021 sono stati segnalati quasi 323.000 tentativi di phishing, quasi 83.000 denunce in più rispetto al 2020 e 209.000 in più rispetto al 2019[1].

La ricerca che abbiamo condotto per il report *State of the Phish 2022* mostra quanto siano diffusi ed efficaci gli attacchi di phishing. Infatti, nel 2021:



delle aziende ha subito attacchi di phishing inviati in blocco[2]

1 utente su 5

ha aperto un allegato durante una simulazione di attacchi di phishing

1 utente su 10

ha fatto clic su un link durante una simulazione di attacchi di phishing

Esempio reale: interruzione della rete elettrica ucraina

Nel dicembre 2015, la rete elettrica ucraina è stata violata, causando interruzioni di corrente fino a sei ore e per circa 225.000 cittadini. Si è trattato del primo attacco informatico riconosciuto pubblicamente a causare delle interruzioni di corrente[3].

I criminali informatici responsabili dell'attacco hanno dedicato diversi mesi all'elaborazione della loro strategia e alla raccolta di informazioni di threat intelligence. Lo spear-phishing è una delle tecniche utilizzate per portare a termine il loro piano. Gli obiettivi erano i team IT e gli amministratori di sistema di tre aziende di distribuzione dell'energia elettrica ucraine (o oblenergos)[4].

1 FBI IC3. "Internet Crime Report 2021" (Report 2021 sui crimini di Internet), marzo 2022. Disponibile all'indirizzo: https://www.ic3.gov/Home/AnnualReports.

2 Proofpoint definisce il phishing inviato in blocco come attacchi classici indiscriminati nei quali la stessa email viene inviata a numerosi collaboratori della stessa azienda.

3 SANS Industrial Control Systems (ICS) e Electricity Information Sharing and Analysis Center (E-ISAC). "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case." (Analisi dell'attacco informatico contro la rete elettrica ucraina: lezioni apprese in materia di difesa), 18 marzo 2016.

4 ICS and E-ISAC.

Svolgimento dell'attacco

Per violare questi utenti, i criminali informatici hanno inviato un allegato Microsoft Word dannoso all'interno di un'email che sembrava provenire da una fonte fidata. Una volta aperto, il documento mostrava un pop-up contestuale che richiedeva all'utente di abilitare le macro. Se l'utente eseguiva l'azione, un malware denominato BlackEnergy3 infettava il sistema e installava una backdoor per i criminali informatici[5].

Questi attacchi di spear-phishing hanno permesso ai criminali informatici di accedere alla rete della società di distribuzione elettrica. Gli hacker hanno quindi trascorso mesi a infiltrarsi nelle reti di controllo industriale e acquisizione dati in tempo reale (SCADA) delle società per organizzare il loro attacco. Hanno utilizzato varie tecniche, tra cui l'accesso ai controller di dominio Microsoft Windows per raccogliere un numero ancora maggiore di credenziali d'accesso degli utenti[6].

Risultato

Le interruzioni di corrente sono state di breve durata. Tuttavia, ci sono voluti diversi mesi prima che i centri di controllo degli oblenergos colpiti tornassero pienamente operativi. Come si legge in un report sull'attacco, l'incidente "ha creato un increscioso precedente per la sicurezza delle reti elettriche in tutto il mondo"[7].

Potenziali conseguenze del phishing

Takeover degli account | Perdite finanziarie | Perdita di dati | Danni alla reputazione

Come la sensibilizzazione degli utenti avrebbe potuto aiutare

Come la maggior parte degli attacchi informatici, l'interruzione della rete elettrica ucraina del 2015 è iniziata con un'email di phishing. Dopo aver indotto un collaboratore ad aprire un allegato infetto, i criminali informatici hanno passato mesi a raccogliere informazioni di threat intelligence e a infiltrarsi più a fondo nell'ambiente.

Una formazione di sensibilizzazione alla sicurezza informatica avrebbe potuto contribuire a neutralizzare l'attacco prima che venisse sferrato. Il collaboratore avrebbe saputo di non dover aprire l'allegato né di interagirvi, impedendo così al criminale informatico di ottenere l'accesso ai sistemi.

5 Kim Zetter *(Wired)*. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." (Analisi della violazione senza precedenti della rete elettrica Ucraina), 3 marzo 2016.

6 Ibid.

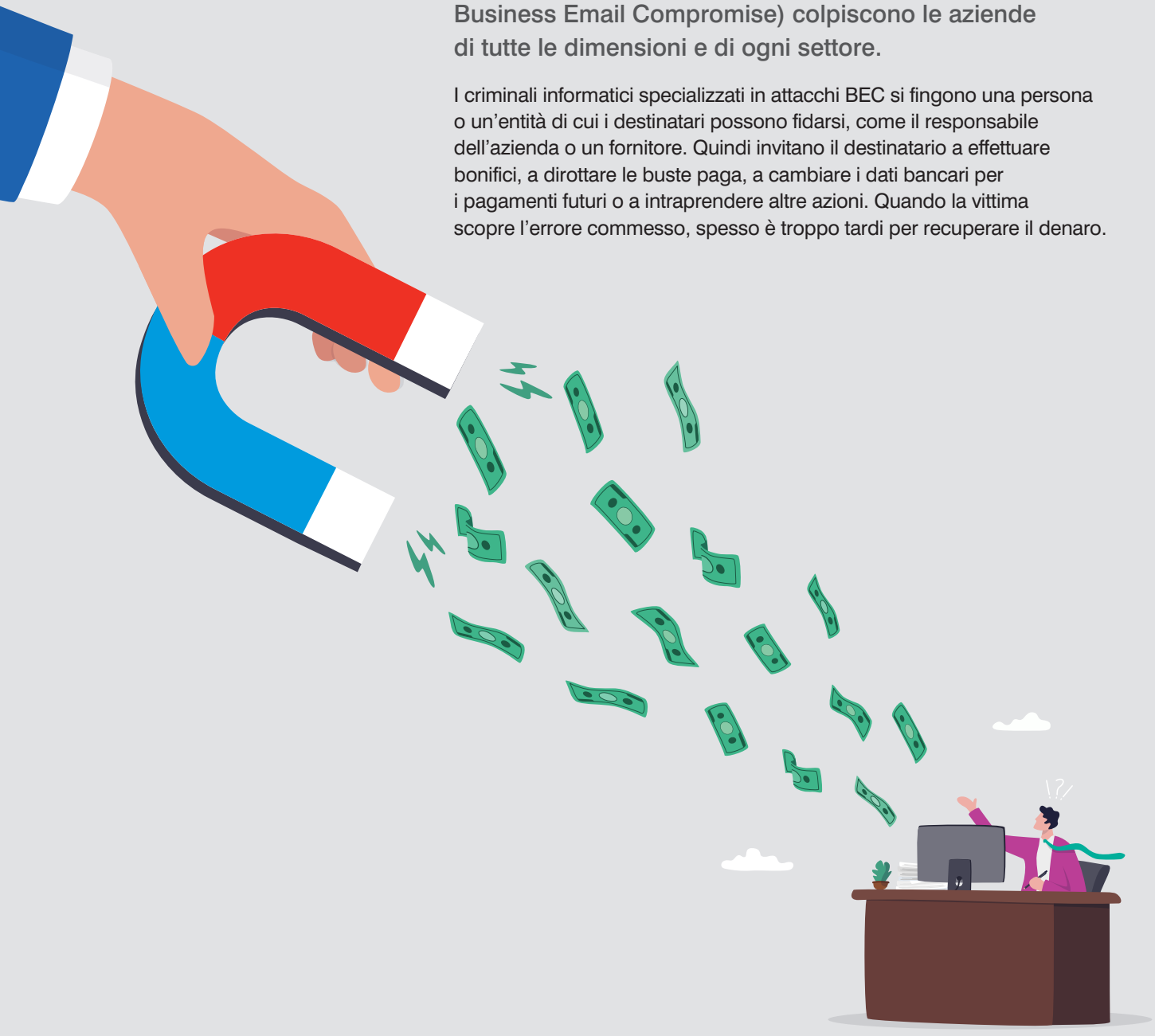
7 Ibid.

SEZIONE 2

Violazione dell'email aziendale (BEC)

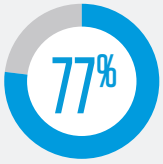
Gli attacchi di violazione dell'email aziendale (BEC, Business Email Compromise) colpiscono le aziende di tutte le dimensioni e di ogni settore.

I criminali informatici specializzati in attacchi BEC si fingono una persona o un'entità di cui i destinatari possono fidarsi, come il responsabile dell'azienda o un fornitore. Quindi invitano il destinatario a effettuare bonifici, a dirottare le buste paga, a cambiare i dati bancari per i pagamenti futuri o a intraprendere altre azioni. Quando la vittima scopre l'errore commesso, spesso è troppo tardi per recuperare il denaro.



Tendenze

Le campagne BEC possono essere molto redditizie. In base al *report 2021 sui reati di Internet* dell'FBI, gli attacchi BEC hanno comportato una perdita rettificata di 2,4 miliardi lo scorso anno solo negli Stati Uniti[8]. Dato i potenziali guadagni, non sorprende che secondo le ricerche effettuare per il report *State of the Phish 2022* il 77% delle aziende in tutto il mondo ha subito attacchi BEC nel 2021.



delle aziende in tutto il mondo è stata presa di mira da attacchi BEC nel 2021

Gli attacchi BEC sono spesso molto avanzati, ben finanziati e sostenuti da un'attenta pianificazione e da ricerche minuziose[9]. Molti criminali informatici concentrano i loro sforzi sulle frodi delle fatture dei fornitori date le ingenti transazioni tra aziende che possono violare. La frode delle fatture è una tecnica molto comune. In questi attacchi, il truffatore si spaccia per un fornitore e dirotta i pagamenti indirizzati a fornitori reali.

Esempio reale: Ubiquiti vittima di una frode dei fornitori pari a 46,7 milioni di dollari

La frode dell'amministratore delegato è un'altra strategia BEC di vecchia data ma efficace, in cui i criminali informatici si fingono l'amministratore delegato o un altro dirigente di alto livello di un'azienda. In genere, inviano un'email a un collaboratore che lavora nel reparto finanziario dell'azienda per richiedere un trasferimento di fondi. Il denaro spesso viene deviato su un conto internazionale controllato dai criminali informatici.

Ubiquiti Inc. è stata vittima di questo tipo di truffa BEC. I criminali informatici sono riusciti a estorcere 46,7 milioni di dollari dall'azienda tecnologica prima che qualcuno si rendesse conto del problema. Gli utenti che hanno l'autorità di trasferire fondi potrebbero non pensare di mettere in discussione le richieste di tipo finanziario da parte dei massimi dirigenti, anche se tali richieste sembrano insolite.

Svolgimento dell'attacco

A poche settimane dal suo ingresso in azienda, a metà maggio 2015, il nuovo direttore finanziario di Ubiquiti ha ricevuto delle email che credeva provenissero dall'amministratore delegato della società e da un avvocato con sede a Londra. Il truffatore, fingendosi l'amministratore delegato, spiegava che l'azienda si apprestava a effettuare un'acquisizione. L'email richiedeva al direttore finanziario di mantenere tale acquisizione segreta e spiegava che per concludere la transazione erano necessari diversi bonifici bancari. L'impostore ha in seguito inviato delle email contenenti istruzioni e informazioni bancarie fasulle autorizzando i pagamenti[10].

8 FBI IC3.

9 Proofpoint. "Attenzione alle frodi via email! Panoramica degli attacchi BEC più devastanti." aprile 2022.

10 Nathan Vardi *(Forbes)*. "How a Tech Billionaire's Company Misplaced $46.7 Million and Didn't Know It." (Come l'azienda di un miliardario della Silicon Valley ha perso 46,7 milioni di dollari senza rendersene conto), febbraio 2016.

Risultato

Nel giro di 17 giorni, il direttore finanziario ha effettuato 14 bonifici, per un totale di 46,7 milioni di dollari, su conti in Cina, Ungheria, Russia e Polonia. Quindi, a inizio giugno, il vero amministratore delegato dell'azienda è stato contattato da un agente dell'FBI, che lo ha informato del possibile furto di una grossa somma di denaro dal conto bancario della divisione di Hong Kong di Ubiquiti[11]. Fino ad allora l'amministratore delegato non era a conoscenza nemmeno dei bonifici effettuati.

Nell'agosto 2015, in una relazione finanziaria trimestrale depositata presso la SEC (Securities and Exchange Commission), Ubiquiti ha rivelato di aver scoperto una frode a giugno, descrivendo l'incidente come "furto d'identità di un dipendente e richieste fraudolente da parte di un'entità esterna".

Ubiquiti è riuscita a recuperare solo una parte delle perdite e la reputazione dell'azienda ne è uscita danneggiata. Il suo direttore finanziario ha rassegnato le dimissioni poco prima che l'azienda rendesse pubblico l'attacco BEC. Un'indagine interna ha messo in luce l'inefficacia dei controlli interni applicati alle attività finanziarie, controlli che sono stati successivamente consolidati dall'azienda[12].

Potenziali conseguenze degli attacchi BEC

Perdite finanziarie dirette

Perdita di dati

Come la sensibilizzazione degli utenti avrebbe potuto aiutare

Le frodi dei fornitori e altre forme di attacchi BEC sono attacchi intrinsecamente incentrati sulle persone. Hanno successo solo quando i destinatari dell'attacco pensano di interagire con qualcuno di cui possono fidarsi. Se avesse seguito una formazione efficace di sensibilizzazione sulla sicurezza informatica, quel direttore finanziario avrebbe potuto capire che le email provenivano da un impostore e non dall'amministratore delegato e dai legali dell'azienda.

Unitamente a controlli finanziari solidi, questa formazione può insegnare agli utenti a individuare istintivamente i domini fotocopia o non correlati, gli URL pericolosi e le tecniche di social engineering che possono ingannare gli utenti meno informati.

11 Ibid.

12 KrebsonSecurity. "Tech Firm Ubiquiti Suffers $46M Cyberheist." (L'azienda tecnologia Ubiquiti subisce un furto informatico di 46 milioni di dollari), agosto 2015.

SEZIONE 3

Ransomware

Il ransomware è fondamentalmente uno strumento per perpetrare estorsioni. È un malware che prende in ostaggio i dati e i sistemi informatici delle vittime fino al versamento di un riscatto.

Solitamente, il criminale informatico richiede il pagamento in criptomonete (per esempio Bitcoin) perché il denaro viene trasferito più rapidamente ed è difficile da rintracciare. La richiesta di riscatto spesso include una scadenza: se le vittime non pagano per tempo, perderanno definitivamente i loro dati o dovranno pagare un riscatto più alto per recuperarli. Per aumentare ulteriormente la pressione sulle vittime, i criminali informatici spesso minacciano di divulgare i dati. In alcuni casi, le vittime pagano senza recuperare comunque i loro dati.

Strumenti di crittografia e blocco schermo sono i principali tipi di malware utilizzati negli attacchi ransomware. I primi, come implica il nome, cifrano i dati di un sistema, rendendo i contenuti inutilizzabili senza la chiave di decrittografia. Gli strumenti di blocco schermo utilizzano una schermata di blocco per impedire all'utente di accedere al sistema compromesso.

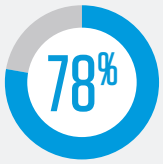
Gli attacchi ransomware esistono da decenni. Negli ultimi anni hanno attirato l'attenzione dei media in quanto causano gravi interruzioni, richiedono il pagamento di ingenti somme di denaro e prendono di mira le infrastrutture critiche, soprattutto nei settori della sanità e dell'energia.

Si sono anche evoluti nel tempo. I criminali informatici che distribuiscono il ransomware spesso acquistano l'accesso da gruppi di criminali informatici indipendenti che si infiltrano all'interno di obiettivi importanti e quindi vendono l'accesso ad altri pirati informatici in cambio di una parte dei guadagni illeciti. I gruppi criminali che già distribuiscono malware bancario o altri trojan possono anche diventare parte di una rete affiliata di organizzazioni di malware. Ciò crea un ecosistema criminale forte e redditizio in cui individui e aziende si sono specializzati nella massimizzazione dei profitti per tutte le parti coinvolte, tranne, ovviamente, le vittime.

Tendenze

Anche gli attacchi ransomware sono in aumento. Secondo il "*report 2022 sulle violazioni dei dati*" di Verizon gli attacchi ransomware sono aumentati del 13% dal 2020 al 2021, il che equivale a un aumento pari a quello dei cinque anni precedenti combinati[13].

Di seguito alcune conclusioni relative al ransomware del report *State of the Phish 2022*:



delle aziende ha subito attacchi ransomware tramite email nel 2021

delle aziende è stato infettato dal ransomware

delle aziende infettate ha pagato un riscatto

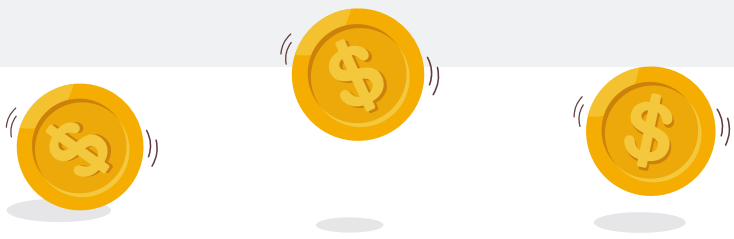
13 Verizon, "Data Breach Investigations Report" (Report sulle violazioni dei dati), maggio 2022.

Esempio reale: attacchi ransomware contro il governo della Costa Rica

Un grave attacco ransomware ha colpito il governo della Costa Rica nell'aprile 2022, colpendo quasi 30 istituzioni, tra cui il Ministero delle finanze, il Fondo di previdenza sociale e anche l'Istituto meteorologico nazionale. Il gruppo ransomware Conti ha rivendicato la campagna e chiesto un riscatto di 10 milioni di dollari per evitare la divulgazione di informazioni sensibili che aveva sottratto dai server del Ministero delle finanze prima dell'attacco[14].

Quando il governo si è rifiutato di pagare, Conti ha rivendicato l'attacco e ha aumentato la richiesta di riscatto a 20 milioni di dollari; poco dopo, il gruppo ha iniziato a caricare i file rubati sul suo sito web. In un tentativo vano e disperato di ottenere un pagamento, il gruppo Conti ha ridotto la richiesta di riscatto a 15 milioni di dollari[15]. Inoltre, i criminali informatici hanno minacciato di rovesciare il governo[16].

A fine maggio, mentre il governo costaricano stava ancora cercando di riprendersi dall'attacco del gruppo Conti, il Servizio sanitario nazionale (CCSS) ha subito un attacco ransomware lanciato da un gruppo noto come Hive. L'ente si è accorto dell'attacco quando le sue stampanti hanno iniziato a stampare in serie copie del messaggio di riscatto di Hive, che non includeva l'importo del riscatto[17]. Tale richiesta è arrivata successivamente, quando Hive ha chiesto al CCSS il pagamento di 5 milioni di dollari in Bitcoin per non divulgare informazioni sensibili[18].



14 Carly Page *(TechCrunch)*. "Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates." (Crescono i timori per le nazioni più piccole dopo l'intensificarsi dell'attacco ransomware in Costa Rica), 20 maggio 2022.

15 Carla Rosch *(Rest of World)*. "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting." (Un massiccio attacco informatico in Costa Rica semina il caos), 1 giugno 2022.

16 Matt Burgess *(Wired)*. "Conti's Attack Against Costa Rica Sparks a New Ransomware Era." (L'attacco del gruppo Conti contro la Costa Rica segna l'inizio di una nuova era del ransomware), 12 giugno 2022.

17 KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions." (La Costa Rica potrebbe essere una pedina nel tentativo del gruppo ransomware Conti di cambiare marchio ed eludere le sanzioni), 31 maggio 2022.

18 Alonso Martinez *(Delfino)*. "Cybercriminals Request $5 million in Bitcoins from the CCSS." (I criminali informatici chiedono 5 milioni di dollari in Bitcoin al sistema sanitario della Costa Rica), 2 giugno 2022.

Svolgimento dell'attacco

Secondo i ricercatori sulle minacce, un membro del gruppo Conti noto come "MemberX" ha utilizzato delle credenziali d'accesso compromesse per accedere, tramite una connessione VPN, a un sistema appartenente al Ministero delle finanze della Costa Rica[19]. Nel giro di 24 ore dal primo attacco di Conti, i criminali informatici hanno crittografato i file all'interno del Ministero delle finanze e bloccato due sistemi critici; il sistema di riscossione delle imposte digitale e il sistema informatico per il controllo delle dogane[20].

Alcuni ipotizzano che Conti possa aver ricevuto un aiuto da persone che lavorano per il governo della Costa Rica. In effetti, un messaggio rilasciato dal gruppo sul dark web dopo l'attacco recitava che "membri all'interno del governo [della Costa Rica]" gli avevano fornito un aiuto - affiliati identificati come "UNC1756"[21].

Il gruppo Hive, invece sfrutta un modello RaaS (Ransomware-as-a-Service) per sferrare i suoi attacchi. Il gruppo e i suoi affiliati inviano email di phishing con allegati pericolosi, cercano di impossessarsi delle credenziali VPN e utilizzano server RDP (Remote Desktop Protocol) vulnerabili per spostarsi lateralmente all'interno della rete compromessa. Secondo un avviso dell'FBI relativamente a Hive, il gruppo in genere esfiltra i dati e crittografa i file sulla rete. Quindi lascia una richiesta di riscatto in ogni directory colpita all'interno del sistema della vittima. La richiesta fornisce le istruzioni su come acquistare il software di decrittografia e minaccia di divulgare i dati esfiltrati dalla vittima sul sito Tor "HiveLeaks"[22].

Alcuni esperti di sicurezza informatica ritengono che gli stessi criminali informatici abbiano partecipato a entrambi gli attacchi ransomware verificatisi in primavera. Suggeriscono che Hive abbia utilizzato la sua campagna per aiutare Conti a ribattezzarsi e a eludere le leggi internazionali che vietano il pagamento di estorsioni a criminali informatici che operano in paesi noti per tollerare (se non addirittura sostenere) questa attività[23]. Hive ha affermato sul suo sito web di non essere affiliato a Conti[24].

Risultato

In seguito al primo attacco ransomware di metà aprile, l'economia costaricana perdeva circa 30 milioni di dollari al giorno. Il governo è stato costretto a chiudere molti sistemi critici durante la caotica fase di remediation. La sola Camera di Commercio Estero della Costa Rica ha stimato perdite per oltre 125 milioni di dollari nei soli primi due giorni successivi all'attacco[25].

19 Ionut Ilascu *(BleepingComputer).* "How Conti Ransomware Hacked and Encrypted the Costa Rican Government." (Come il gruppo ransomware Conti ha violato e cifrato i file del governo della Costa Rica), 21 luglio 2022.

20 Matt Burgess *(Wired).* "Conti's Attack Against Costa Rica Sparks a New Ransomware Era." (L'attacco del gruppo Conti contro la Costa Rica segna l'inizio di una nuova era del ransomware), 12 giugno 2022.

21 Claudia Glover *(Tech Monitor).* "'We will overthrow the government' – Does Conti have help inside Costa Rica?" (Rovesceremo il governo. Il gruppo Conti riceve l'aiuto di una persona interna al governo della Costa Rica?), 17 maggio 2022.

22 Report FLASH dell'FBI. "Indicators of Compromise Associated with Hive Ransomware." (Indicatori di violazione associati al ransomware Hive), 25 agosto 2021.

23 KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions." (La Costa Rica potrebbe essere una pedina nel tentativo del gruppo ransomware Conti di cambiare marchio ed eludere le sanzioni), 31 maggio 2022.

24 Ibid.

25 Carla Rosch *(Rest of World).* "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting." (Un massiccio attacco informatico in Costa Rica semina il caos), 1 giugno 2022.

Il governo ha anche dovuto chiudere le pagine web delle agenzie prese di mira. Ha richiesto l'aiuto tecnico di altri governi, tra cui quello statunitense, e di aziende tecnologiche come Microsoft. Gli Stati Uniti hanno persino offerto fino a 5 milioni di dollari per informazioni che potessero portare all'arresto o alla condanna di chiunque avesse cospirato in un attacco del ransomware Conti[26].

A inizio maggio, il nuovo presidente della Costa Rica, Rodrigo Chaves Robles, ha dichiarato lo stato di emergenza nazionale, definendo l'attacco lanciato dal gruppo Conti un atto di terrorismo. Nel giro di poche settimane, Hive ha lanciato il suo attacco.

La Costa Rica ha impiegato settimane per riprendersi dall'attacco. A metà giugno, alcune agenzie sono riuscite finalmente a riprendere le attività.

Potenziali conseguenze del ransomware

Interruzione delle attività

Perdite finanziarie
(dovute al pagamento del riscatto e alle misure correttive dopo l'attacco)

Perdita di dati
(se i criminali informatici danno seguito alle minacce di divulgazione dei dati se il riscatto non viene pagato)

Come la sensibilizzazione degli utenti avrebbe potuto aiutare

Alcune fonti suggeriscono che l'attacco ransomware contro la Costa Rica possa aver beneficiato dell'aiuto di utenti interni malintenzionati del governo. Ma molte infezioni di ransomware sono il prodotto di violazioni precedenti diffuse via email. I criminali informatici utilizzano tecniche come il phishing per rubare le credenziali di accesso per poter accedere a sistemi critici.

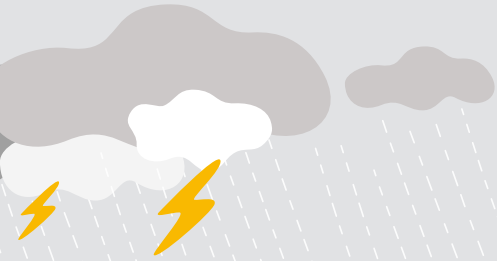
Insegnare agli utenti a individuare e segnalare le email sospette, soprattutto in combinazione con l'analisi automatica a ciclo chiuso, può ridurre drasticamente il rischio di ransomware e altre forme di malware.

Gli utenti dovrebbero diffidare istintivamente degli allegati di file e degli URL, soprattutto all'interno di email che fanno leva su sentimenti umani come il guadagno personale, la curiosità, la paura, l'indignazione e persino la disponibilità. E dovrebbero conoscere i segnali che indicano che il mittente potrebbe non essere chi dice di essere.

26 Elizabeth Montalbano *(Threatpost)*. "Conti Ransomware Attack Spurs State of Emergency in Costa Rica." (Dichiarato lo stato d'emergenza in Costa Rica a seguito dell'attacco del gruppo ransomware Conti), 10 maggio 2022.

SEZIONE 4

Attacchi cloud e takeover degli account



I criminali informatici seguono gli utenti come la loro ombra. La migrazione verso il cloud non fa eccezione. La pandemia di COVID-19 ha accelerato la migrazione verso il cloud con conseguente aumento degli attacchi cloud. Come spiega il nostro *report Il Fattore Umano 2022*, la violazione degli account cloud occupa ormai un posto importante e permanente nel panorama delle minacce informatiche, insieme a phishing e malware.

La violazioni dell'account è l'atto di ottenere in modo doloso il controllo dell'account email o di un servizio di collaborazione cloud di un utente legittimo per accedere a un'ampia gamma di dati, contatti, voci del calendario, email e altri strumenti di sistema. Sfruttando l'autenticazione Single Sign-On, i criminali informatici sono liberi di muoversi tra i diversi sistemi nell'ambiente e causare danni considerevoli.

Gli strumenti che i criminali informatici spesso utilizzano per violare gli account cloud e acquisirne il controllo includono:

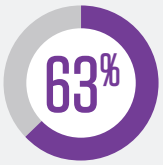
- Attacchi di forza bruta che automatizzano la ricerca sistematica delle credenziali di accesso
- Attacchi di phishing, incluso il phishing dei token OAuth
- Riciclo delle credenziali di accesso, o stuffing, utilizzando coppie di nome utente e password rubate in precedenza
- Malware, come keylogger e programmi di furto delle credenziali

La persistenza sembra essere un altro elemento chiave nelle violazioni degli account cloud.

Tendenze

In base ai dati del nostro *report Il Fattore Umano 2022* oltre il 90% dei tenant cloud monitorati è stato colpito ogni mese. Quasi un quarto (25%) è stato attaccato con successo, con quasi due terzi dei tenant (63%) violati nel corso dell'anno[27].

degli attacchi contro tenant cloud monitorati è andato a buon fine



dei tenant cloud è stato compromesso nel 2021

Gli attacchi di takeover degli account cloud sono spesso difficili da rilevare, complessi da neutralizzare e dannosi per i tuoi risultati finanziari. In base a un recente studio, le perdite finanziarie medie causate dalla violazione degli account cloud ammonta a 6,2 milioni di dollari all'anno per le aziende. In media, le aziende subiscono inoltre 138 ore di tempi di fermo delle applicazioni imputabili a questa attività[28].

Applicazioni cloud dannose

Le applicazioni non approvate (Shadow IT) contribuiscono al problema delle applicazioni cloud dannose. Un'applicazione cloud di terze parti è un'applicazione che si integra con un servizio cloud ma non sono fornite dal fornitore del servizio cloud. Le applicazioni di terze parti utilizzano OAuth, un protocollo di autorizzazione che permette alle applicazioni di ottenere un accesso limitato a un servizio cloud. Il protocollo OAuth permette alle applicazioni di terze parti di utilizzare le informazioni o i dati dell'account di un utente senza esporre le credenziali d'accesso[29].

A prima vista, questo processo sembra molto pratico e sicuro. Ma, sfortunatamente, le applicazioni di terze parti possono essere facilmente sfruttate. Quando gli utenti le installano, spesso fanno clic su "Accetta" senza prestare la dovuta attenzione alla portata delle autorizzazioni. Una volta ottenuto l'accesso OAuth, i criminali informatici possono utilizzarlo per violare gli account cloud e impadronirsene. Peggio ancora, hanno accesso persistente agli account e ai dati degli utenti finché il token OAuth non viene esplicitamente revocato.

27 Proofpoint. "Il fattore umano 2022." maggio 2022.

28 Ponemon Institute. "2021 Ponemon Report: The Cost of Cloud Compromise and Shadow IT." (Report 2021 del Ponemon Institute: costo delle violazioni degli account cloud e della Shadow IT), aprile 2021.

29 Proofpoint. "Tutto quello che i professionisti della sicurezza devono sapere sulle applicazioni OAuth di terze parti", maggio 2022.

File dannosi archiviati nel cloud

Una volta che un criminale informatico ha assunto il controllo di un account cloud, può caricare file dannosi per gettare le basi per altre azioni illecite, come il furto di dati o bonifici bancari fraudolenti. Ad esempio, in uno schema di phishing di Microsoft SharePoint, un criminale informatico carica un file dannoso su un account cloud compromesso. Le autorizzazioni di condivisione del file vengono modificate in "Pubblico", in modo che il nuovo link anonimo possa essere condiviso con chiunque. Il criminale informatico invia quindi il link via email o lo condivide con i contatti dell'utente compromesso o con altri destinatari. Quando questi destinatari aprono il file e fanno clic sul link dannoso, il criminale informatico ha gioco facile[30].

I nostri ricercatori delle minacce hanno recentemente scoperto una nuova variante degli attacchi cloud: i criminali informatici ora prendono di mira i dati cloud e lanciano attacchi di tipo ransomware utilizzando l'infrastruttura cloud. Durante il processo violano le applicazioni cloud aziendali diffuse, tra cui SharePoint Online e OneDrive all'interno della suite Microsoft 365[31].

Nonostante il pericolo reale rappresentato dai file compromessi da un criminale informatico nel cloud, il report *State of the Phish 2022* ha rilevato che solo il 37% degli utenti è consapevole che i file archiviati nel cloud possono essere dannosi.

Esempio reale: campagna OiVaVoii

Il cloud facilita la collaborazione e la condivisione dei dati. È anche un ambiente di minacce complesso che sta crescendo rapidamente nel contesto della trasformazione digitale e della diffusione del lavoro da remoto e ibrido.

Una recente campagna che ha preso di mira utenti di alto valore, tra cui membri della dirigenza aziendale, dimostra perché gli utenti di tutti i livelli aziendali devono essere cauti nel concedere le autorizzazioni alle applicazioni cloud, anche se sembrano inoffensive e provenire da mittenti legittimi.

30 Itir Clarke, Eilon Bendet e Doyle Groves *(Proofpoint)*. "Why OneDrive and SharePoint Attacks Are Successful and How to Fight Back." (Perché gli attacchi contro OneDrive e SharePoint hanno successo e come contrastarli), ottobre 2020.

31 Or Safran, David Krispin, Assaf Friedman e Saikrishna Chavali *(Proofpoint)*. "Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive." (Proofpoint scopre una funzionalità di Microsoft Office 365 potenzialmente pericolosa, in grado di prendere in ostaggio i file archiviati in SharePoint e OneDrive), giugno 2022.

Svolgimento dell'attacco

Nel gennaio 2022, i nostri ricercatori hanno rilevato per la prima volta una campagna dannosa di cloud ibrido, OiVaVoii, e hanno scoperto cinque applicazioni OAuth dannose associate alla campagna[32].

Almeno tre delle applicazioni dannose di terze parti sono state create da due diversi "editori verificatori". Questi editori probabilmente sono account amministrativi compromessi all'interno di tenant Microsoft 365 legittimi. Delle altre due app, almeno una è stata creata da un editore non verificato. Ciò suggerisce che i criminali informatici utilizzavano un terzo ambiente cloud violato o un tenant Microsoft 365 dannoso dedicato.

Risultato

Una volta create le applicazioni, i criminali informatici hanno inviato le richieste di autorizzazione via email a numerosi utenti designati, tra cui dirigenti di alto livello. Molti di questi utenti hanno autorizzato le applicazioni. Questa semplice azione ha permesso ai criminali informatici di generare token OAuth per conto dell'utente preso di mira e portato a termine il takeover degli account. Tutte le applicazioni associate alla campagna OiVaVoii richiedevano autorizzazioni similari agli utenti, principalmente per l'accesso alla casella di posta (lettura e scrittura). Una volta accettate le richieste da parte degli utenti, i criminali informatici erano liberi di inviare messaggi email dannosi sia all'interno che verso l'esterno, rubare informazioni preziose e molto altro ancora.

Potenziali conseguente degli attacchi cloud

Takeover degli account

Perdita di dati
(a causa dell'ingresso di malware nell'ambiente o dell'esfiltrazione diretta di dati da parte di applicazioni dannose)

Interruzione delle attività
(a causa di ransomware e altro malware che penetrano nell'ambiente)

Come la sensibilizzazione degli utenti avrebbe potuto aiutare

Come la maggior parte degli attacchi veicolati tramite email, quelli basati sul cloud sfruttano l'interazione umana per avere successo. Per questo motivo, spingono gli utenti a condividere le proprie credenziali d'accesso, a installare applicazioni dannose e a fare clic su URL che rimandano a siti di condivisione di file affidabili utilizzati per ospitare file dannosi.

Come parte del programma di sensibilizzazione alla sicurezza informatica, è fondamentale insegnare ai tuoi collaboratori a utilizzare i servizi cloud in modo sicuro e a non autorizzare applicazioni sconosciute.

32 Eilon Bendet, Assaf Friedman e David Krispin *(Proofpoint).* "OiVaVoii – An Active Malicious Hybrid Cloud Threats Campaign." (OiVaVoii, una campagna di cloud ibrido dannoso attiva), gennaio 2022.

Perché l'autenticazione a più fattori non è una soluzione miracolosa

Molte aziende attente alla sicurezza informatica insegnano ai loro utenti a utilizzare l'autenticazione a più fattori come strumento per salvaguardare i loro account, e a ragione. L'autenticazione a più fattori è un livello di sicurezza aggiuntivo che aiuta a proteggere gli account quando un criminale informatico cerca di collegarsi utilizzando credenziali d'accesso rubate. Al momento dell'accesso, l'utente viene invitato a inserire non solo il suo nome utente e la sua password ma anche un codice inviato al suo numero telefono, fob o chiave di sicurezza fisica. L'autenticazione a più fattori riduce in modo significativo le possibilità che i criminali informatici possano compromettere gli account tramite l'uso di credenziali d'accesso rubate e dovrebbe far parte di ogni programma di sensibilizzazione alla sicurezza.

Ma non è infallibile. Kit di phishing di facile utilizzo permettono ai criminali informatici di eludere facilmente questi meccanismi di protezione. Microsoft afferma che 10.000 aziende hanno subito attacchi che hanno aggirato l'autenticazione a più fattori a partire dal settembre 2021. Una volta ottenuto l'accesso, i criminali informatici utilizzano gli account compromessi per lanciare attacchi BEC[33].

Questi attacchi iniziano tipicamente con un'email di phishing; per questo motivo è fondamentale insegnare agli utenti a riconoscere e segnalare i messaggi sospetti. Nell'attacco contro Microsoft, le email di phishing includevano un allegato in formato HTML. Una volta aperto, il file reindirizzava gli utenti verso un server proxy che intercettava il traffico tra gli utenti e la schermata di accesso.

Gli utenti dovrebbero inoltre imparare a non aprire mai file allegati provenienti da mittenti sconosciuti, in modo particolare se si tratta di un tipo di file che solitamente non viene inviato tramite email.

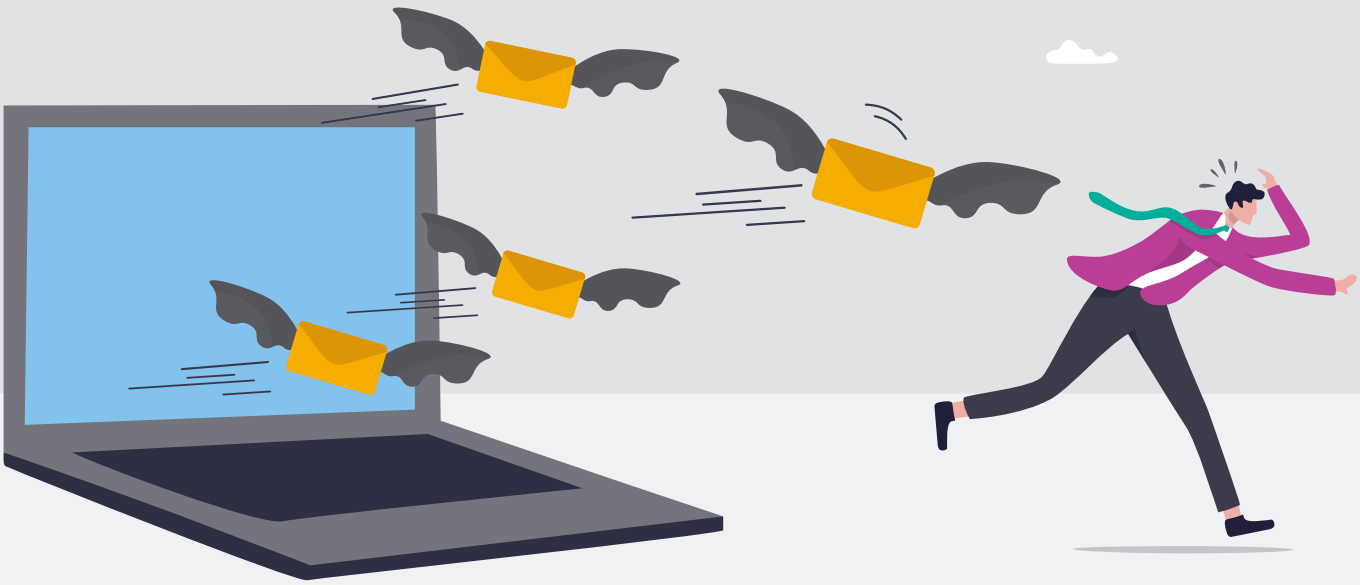
33 Microsoft, "From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud." (Dal furto di cookie agli attacchi BEC: i criminali informatici utilizzano siti di phishing AiTM come punto d'ingresso per perpetrare altre frodi finanziarie), luglio 2022.

SEZIONE 5

Attacchi tramite webmail

La diffusione del telelavoro fornisce ai criminali informatici ancor più possibilità per infiltrarsi nei sistemi aziendali. La maggior parte dei collaboratori utilizza una rete privata virtuale (VPN) per accedere alla rete della propria azienda quando lavora fuori ufficio. Inoltre utilizzano anche i loro dispositivi per collegarsi alle risorse aziendali, quegli stessi dispositivi che utilizzano per accedere ai loro account webmail personali. Al contrario, molti collaboratori utilizzano dispositivi aziendali per accedere ai loro account personali.

Se dei criminali informatici compromettono gli account personali di un utente, possono appropriarsi delle credenziali d accesso ad applicazioni, dati e sistemi aziendali. Possono anche sfruttare il fatto che molti collaboratori utilizzano i loro account email personali o i loro numeri di cellulare per l'autenticazione a due fattori o la reimpostazione della password. Queste informazioni sono sufficienti per permettere ai criminali informatici di infiltrarsi nelle reti aziendali.

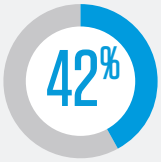


Tendenze

In base al report *State of the Phish 2022* numerosi utenti sono in pericolo a causa di attacchi tramite webmail che potrebbero danneggiare le loro aziende.

Inoltre, sembra che molti di loro presumano che il loro fornitore del servizio webmail li proteggeranno da questi attacchi.

La nostra ricerca ha rilevato che:



degli utenti consulta l'email personale su dispositivi forniti dall'azienda

degli utenti sa che il proprio fornitore del servizio di email personale non è in grado di bloccare tutte le email pericolose

Esempio reale: LAPSUS$

A volte, i criminali informatici sono altrettanto, se non più, interessati a creare disagi e a far parlare di loro piuttosto che a generare dei profitti. È il caso di LAPSUS$, un gruppo di criminali informatici specializzato nel furto e nell'estorsione di dati emerso alla fine del 2021. Il gruppo potrebbe essere ancora attivo, anche se diversi suoi membri, tutti di età compresa tra i 16 e i 21 anni, sono stati arrestati dalla polizia britannica a marzo[34].

Svolgimento dell'attacco

In pochi mesi, il gruppo LAPSUS$ ha cercato di estorcere dati al Ministero della salute del Brasile e ha pubblicato schermate di strumenti interni associati a NVIDIA, Samsung e Vodafone[35]. Il suo approccio non convenzionale all'estorsione non è passato inosservato. Ha rubato dati sensibili e ha minacciato di pubblicarli online se la vittima non avesse pagato. Fondamentalmente, si è trattato di un attacco ransomware senza ransomware.

Risultato

Come se non bastasse, il gruppo avrebbe pubblicato dei sondaggi nell'applicazione Telegram per consentire agli utenti di votare per i dati della vittima da pubblicare online per primi[36]. Per ottenere l'accesso alle reti aziendali che desiderava violare, il gruppo LAPSUS$ colpiva spesso gli account email personali dei collaboratori per ottenere delle credenziali per stabile un accesso remoto[37].

34 Scott Ikeda *(CPO Magazine)*. "Suspected Lapsus$ Hackers Arrested; London Group Between the Ages of 16 and 21." (Sospetti con età da 16 a 21 anni arrestati per i loro collegamenti con il gruppo londinese LAPSUS$), marzo 2022.

35 KrebsonSecurity. "A Closer Look at the LAPSUS$ Data Extortion Group." (Uno sguardo più da vicino al gruppo LAPSUS$, specializzato nell'estorsione di dati), marzo 2022.

36 Lily May Newman *(Wired)*. "The Lapsus$ Hacking Group Is Off to a Chaotic Start." (Il gruppo di hacker LAPSUS$ già nel caos), marzo 2022.

37 Microsoft, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction." (Il gruppo di criminali informatici DEV-0537 prende di mira le aziende per esfiltrare e distruggere i loro dati), marzo 2022.

I team di Microsoft Security denominano il gruppo LAPSUS$ “DEV-0537”.

“A differenza della maggior parte dei gruppi di criminali informatici che tengono un basso profilo, DEV-0537 non sembra cercare di dissimulare le sue attività”, afferma il gigante del software. “Si spinge fino ad annunciare i suoi attacchi sui social media e condivide le sue intenzioni di acquistare credenziali d’accesso ai collaboratori delle aziende che prende di mira[38]”.

La campagna pubblicitaria del gruppo includeva dei messaggi Telegram, nei quali LAPSUS$ cercava di reclutare collaboratori e altri utenti interni che lavoravano per operatori di telecomunicazioni, giganti dell’informatica e del gioco, operatori di call center e host di server. Il suo obiettivo: corrompere dei collaboratori per ottenere credenziali d’accesso alla VPN o qualsiasi altro tipo di accesso remoto. LAPSUS$ offriva anche denaro agli utenti interni in cambio di informazioni. Una pubblicità affermava che era possibile guadagnare almeno 20.000 dollari a settimana[39].

Microsoft Security ha anche riferito che LAPSUS$ ha ottenuto l’accesso iniziale alle vittime con altri mezzi, tra cui l’acquisto delle credenziali d’accesso e di token delle sessioni su forum clandestini e la ricerca delle credenziali esposte nei repository di codice pubblici.

Potenziali conseguenze degli attacchi tramite webmail

Perdita di dati | Interruzione delle attività | Perdite finanziarie | Danni alla reputazione

Come la sensibilizzazione degli utenti avrebbe potuto aiutare

Il gruppo LAPSUS$ utilizzava diverse tattiche, tra cui le seguenti:

- Violazione della webmail e dei metodi di accesso da remoto
- Reclutamento di collaboratori, fornitori o partner commerciali delle aziende prese di mira
- Furto di dati sensibili e di proprietà intellettuale
- Richieste di riscatto

Mostrare agli utenti come proteggere le loro credenziali d’accesso, consultare la posta personale in tutta sicurezza e segnalare le richieste di riscatto avrebbe contribuito in modo significativo a prevenire gli attacchi.

38 Ibid.

39 KrebsonSecurity. “A Closer Look at the LAPSUS$ Data Extortion Group.” (Uno sguardo più da vicino al gruppo LAPSUS$, specializzato nell’estorsione di dati), marzo 2022.

SEZIONE 6

Conclusioni e raccomandazioni

Identificare il modo migliore per formare i tuoi utenti sul panorama delle minacce in costante evoluzione e mantenerli informati è una sfida impegnativa. Essenzialmente, il tuo obiettivo è quello di motivarli a essere vigili tanto quanto i tuoi team della sicurezza in merito alle minacce informatiche. Questo permetterà loro di diventare dei difensori proattivi.

Affinché la formazione di sensibilizzazione alla sicurezza informatica sia efficace, gli utenti devono comprendere la posta in gioco. Perché dovrebbero preoccuparsi delle minacce informatiche? Perché la difesa dell'azienda rientra tra le loro responsabilità? In poche parole, perché rappresentano il nuovo perimetro. Per avere una reale possibilità di tenere a bada i moderni criminali informatici, l'azienda deve adottare un approccio alla sicurezza incentrato sulle persone.

I cinque tipi di minacce informatiche e gli esempi di attacco descritti in questo eBook hanno un punto in comune: prendono di mira le persone. I criminali informatici sfruttano gli utenti, volenti o nolenti, per far progredire le loro campagne e raggiungere i loro obiettivi.

Queste minacce e questi incidenti aiutano a dimostrare che i collaboratori rappresentano il fattore di rischio più critico nell'attuale panorama delle minacce. Per questo motivo la formazione di sensibilizzazione alla sicurezza informatica dev'essere una parte essenziale della tua strategia di cybersecurity.

Dai priorità agli argomenti più pertinenti

Tutti i collaboratori che possono influenzare il livello di sicurezza dell'azienda devono essere formati in merito alle best practice per la sicurezza informatica. Devi adottare un approccio deliberato e strategico per valutare e formare il personale e dare priorità agli argomenti che sono pertinenti al tuo settore e alla tua azienda, nonché ai tuoi collaboratori. Sentiti libero di utilizzare gli esempi di vita reale inclusi in questo eBook in modo che gli utenti possano riconoscervisi. Gli utenti subiranno inevitabilmente attacchi simili a causa della natura del loro lavoro, della loro funzione, della loro ubicazione e dei loro metodi di lavoro, nonché di altri fattori.

Sfrutta la threat intelligence

La threat intelligence può anche aiutarti a decidere quando offrire una formazione specifica a determinati collaboratori. Per sfruttare le informazioni sulle minacce note o emergenti, è essenziale identificare i seguenti utenti:

Utenti molto vulnerabili - In base al loro comportamento, alla loro tendenza a fare clic sulle email durante le simulazioni di attacchi di phishing e alla loro partecipazione alla formazione.

Utenti più esposti - Utenti che subiscono volumi elevati di attacchi, minacce particolarmente sofisticate, attacchi altamente mirati o tutti e tre.

Utenti con i privilegi più elevati - Utenti che hanno accesso a dati, sistemi e altre risorse critiche che l'azienda deve proteggere.

In sintesi, un approccio alla sicurezza incentrato sulle persone richiede di identificare i collaboratori e i dipartimenti dell'azienda che vengono attaccati e presi di mira in un determinato momento, nonché i metodi utilizzati dai criminali informatici per cercare di compromettere i tuoi utenti e il tuo ambiente.

Analizza costantemente i parametri chiave della sensibilizzazione alla sicurezza informatica per valutare il successo del tuo programma

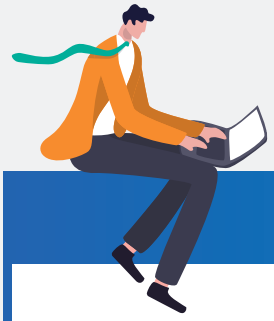
Evita di concentrarti su un solo parametro, come i tassi di insuccesso durante i test di phishing. Per valutare il successo dei tuoi programmi, devi basarti su diversi parametri e tenere conto di diversi fattori.

Prevedi di utilizzare i seguenti parametri:

- Fallimenti nelle simulazioni di attacchi di phishing
- Segnalazione di simulazioni di attacchi di phishing
- Valutazioni delle conoscenze
- Precisione delle email segnalate
- Partecipazione alla formazione

Un ultimo consiglio: non dimenticare di mantenere aggiornata la formazione di sensibilizzazione alla sicurezza informatica in un panorama delle minacce in costante evoluzione. Sapendo che anche la tua azienda evolve, assicurati che i tuoi consigli siano rilevanti per i tuoi utenti. I parametri sopra menzionati possono aiutarti a valutare costantemente l'efficacia dei tuoi programmi e a modificarli se necessario.

Per saperne di più su queste strategie per migliorare i programmi di formazione e sensibilizzazione alla sicurezza informatica, scarica il report *State of the Phish 2022* di Proofpoint.



Perché Proofpoint

Ogni giorno, analizziamo oltre:

2,6 MLD DI EMAIL	**49 MLD** DI URL	**1,9 MLD** DI ALLEGATI
1,7 MLD DI MESSAGGI MOBILE	**430 MIO** DI DOMINI WEB	**143,000** ACCOUNT SOCIAL MEDIA

Le nostre soluzioni sono state adottate da oltre:

- **75%** DELLE AZIENDE FORTUNE 100
- **60%** DELLE AZIENDE FORTUNE 1000
- **30%** DELLE AZIENDE FORTUNE GLOBAL 2000

- **8.000** GRANDI AZIENDE
- **200.000** PICCOLE IMPRESE

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui il 75% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.