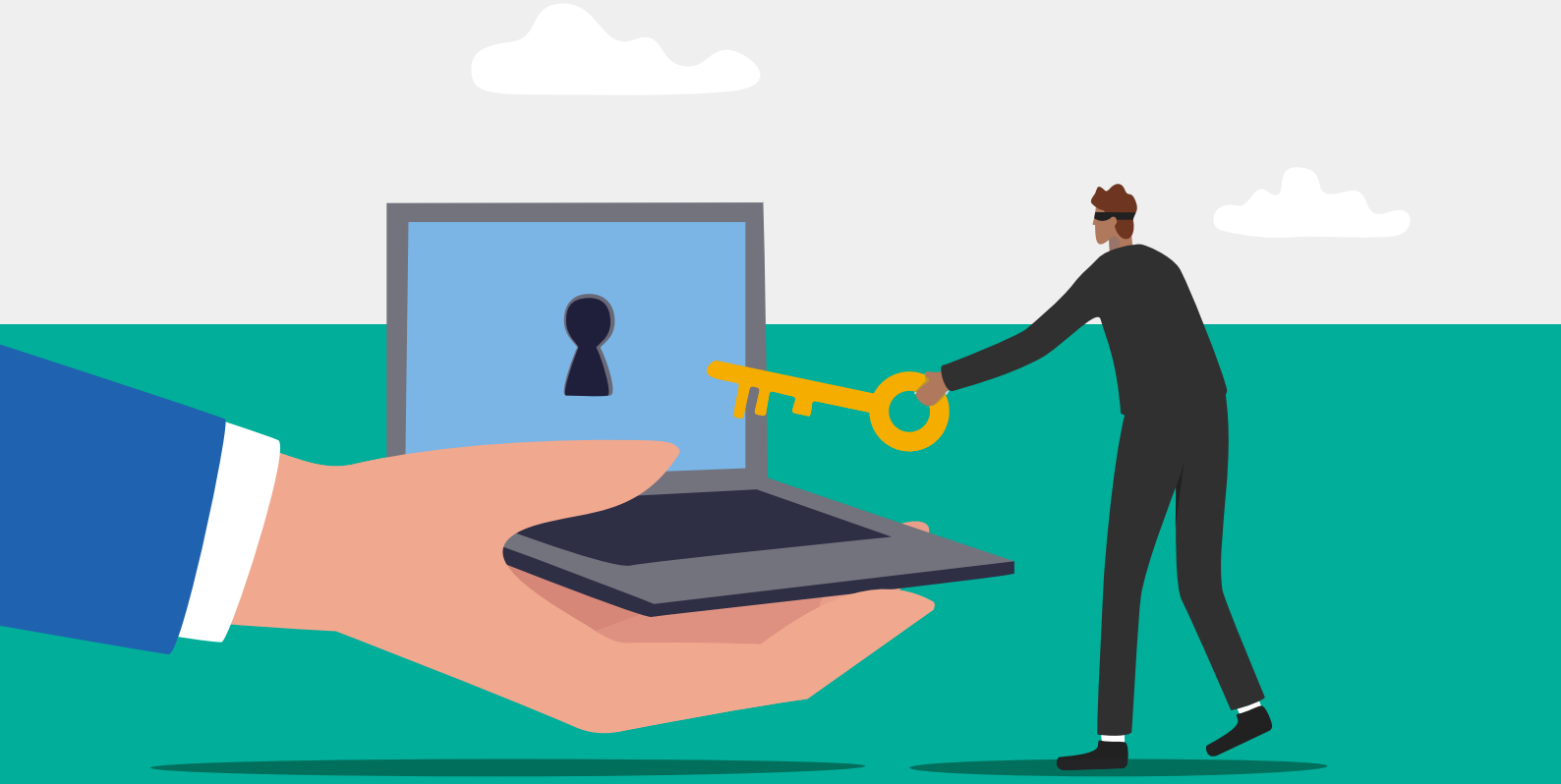
proofpoint.

EBOOK

Cinque attacchi informatici reali e come neutralizzarli, vol.1

Vol. 1: attacchi di social engineering



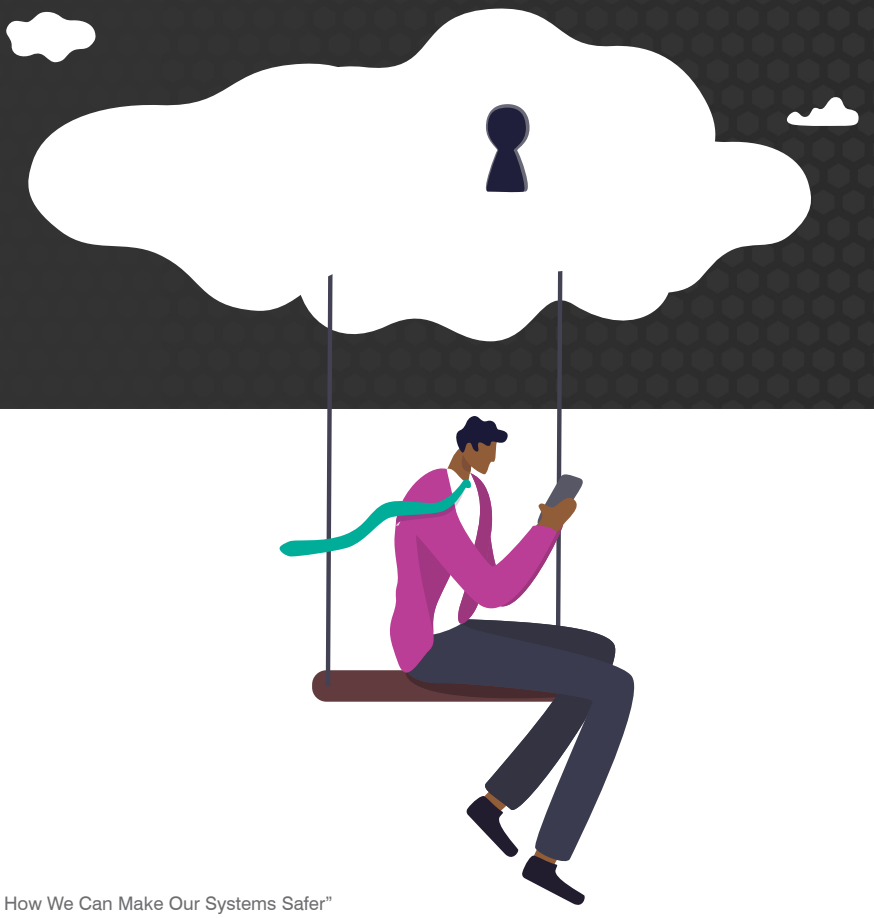
Introduzione

I criminali informatici sono astuti e estremamente motivati. Perché non dovrebbero esserlo? Operano in un settore in forte crescita dove i rischi sono bassi e i benefici così elevati che si prevede che entro il 2027 il crimine informatico costerà al mondo 23,8 bilioni di dollari all'anno[1].

Con una tale prospettiva di guadagno, la creatività dimostrata negli attacchi informatici sembri infinita. Nuove campagne malware, attacchi phishing e e tattiche di social engineering ingegnose appaiono ogni giorno, mentre i team della sicurezza giocano al gatto con il topo con i criminali informatici. Sebbene queste nuove minacce possono sembrare infinitamente varie, hanno tutte alcuni punti in comune: sono veicolate tramite l'email e prendono di mira le persone.

In questa serie di eBook, abbiamo raccolto alcuni dei più insidiosi attacchi email attualmente in circolazione. Molti di questi sono riusciti a eludere le difese di diversi strumenti di sicurezza prima di essere rilevati. Per aiutarti a comprenderne il motivo, ti illustriamo passo-passo ogni attacco per mostrarti il funzionamento di ciascuno e come i criminali informatici hanno cercato di sfruttare le vulnerabilità umane. Quindi ti spiegheremo come sono stati neutralizzati.

Questo volume copre gli attacchi che utilizzano il social engineering. Nel volume 2, prenderemo in considerazione attacchi più tecnici.



1 World Economic Forum. "2023 Was a Big Year for Cybercrime—Here's How We Can Make Our Systems Safer" (Il 2023 è stato un ottimo anno per il crimine informatico. Ecco come rafforzare la sicurezza dei nostri sistemi), gennaio 2024.

Sommario

SEZIONE 1

Attacchi BEC e della supply chain

Negli attacchi di violazione dell'email aziendale (BEC, Business Email Compromise), un criminale informatico si finge una persona o un'entità di cui il destinatario si fida, come un collega, un fornitore o un partner. Molti degli schemi BEC attuali sono estremamente sofisticati, ben finanziati e sostenuti da un'attenta attività di ricerca e pianificazione.

Negli ultimi cinque anni, questi attacchi sono stati molto redditizi per i criminali informatici. Secondo il report *2023 Internet Crime Report* dell'FBI, sono costati 17 miliardi di dollari alle aziende statunitensi. A livello globale, le aziende hanno perso ben 50 miliardi di dollari[2], mentre le vittime di ransomware hanno perso 1,1 miliardi di dollari[3].

2 FBI, "Business Email Compromise: The $50 Billion Scam" (Violazione dell'email aziendale: una truffa da 50 miliardi di dollari), giugno 2023.

3 Wired. "Ransomware Payments Hit a Record $1.1 Billion in 2023" (I pagamenti dei riscatti raggiungono la cifra record di 1,1 miliardi di dollari nel 2023), febbraio 2024.

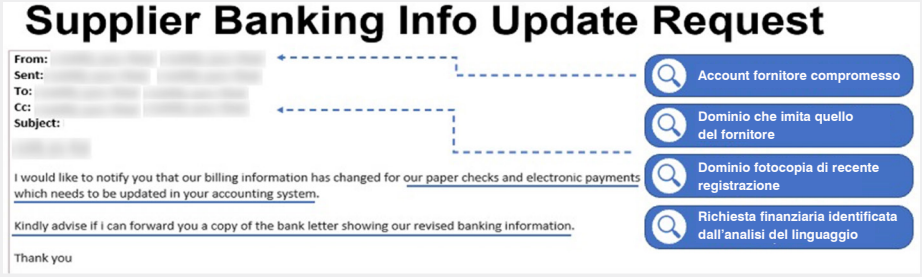
Lo scenario

Proofpoint ha rilevato questo incidente BEC presso un gruppo globale della grande distribuzione che conta più di 40.000 utenti. La minaccia proveniva dalla supply chain del gruppo e lo strumento di sicurezza esistente non è riuscito a rilevarlo. Questo esempio è utile perché mette in evidenza la rapidità con cui evolve il panorama delle minacce.

Svolgimento dell'attacco

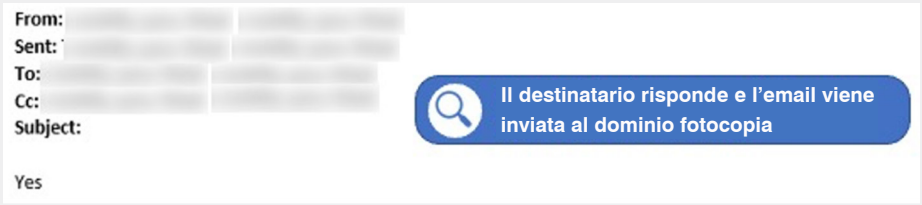
Esaminiamo più da vicino come si è svolto l'attacco:

1. **Il messaggio ingannevole.** Il gruppo globale della grande distribuzione ha ricevuto un'email da un mittente della sua supply chain che richiedeva un aggiornamento delle sue informazioni di pagamento. Questa richiesta in apparenza inoffensiva era in realtà dannosa, poiché l'account del mittente era stato compromesso.



Email iniziale del criminale informatico, che include le osservazioni del team di investigazioni forensi di Proofpoint

2. **Il dominio fotocopia dannoso.** Il criminale informatico voleva reindirizzare le email di risposta su un dominio fotocopia di recente registrazione, con l'obiettivo di intercettare dati sensibili e dirottare denaro.



Risposta del cliente, inviata a un dominio fotocopia

Perché queste minacce sono difficili da rilevare

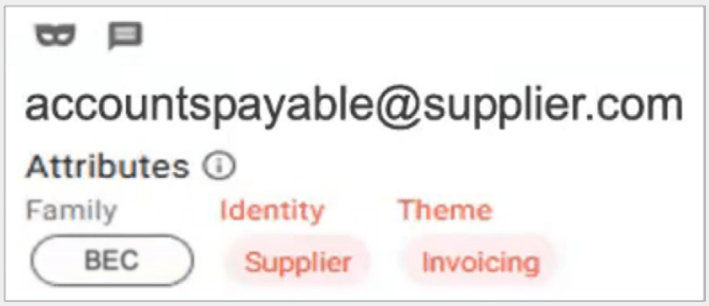
Gli attacchi BEC molto difficili da rilevare perché non includono i payload che siamo soliti analizzare, come gli URL o gli allegati dannosi. I criminali informatici sfruttano invece il furto d'identità e altre tecniche di social engineering per ingannare gli utenti.

Lo strumento di sicurezza del gruppo non ha rilevato questa minaccia per diversi motivi. In primo luogo, si basava troppo sull'età del dominio come fattore di rilevamento. Inoltre, non era in grado di identificare i domini fotocopia e non analizzava l'indirizzo di risposta, che gli avrebbe permesso di rilevare il reindirizzamento verso un nuovo dominio.

Come Proofpoint ha rilevato l'attacco

Per identificare molti tipi di minacce, come gli attacchi BEC e il phishing delle credenziali di accesso, è fondamentale combinare l'età del dominio con altri elementi che identificano l'intento dannoso. Per questo motivo Proofpoint utilizza un approccio multilivello. Il nostro motore di rilevamento utilizza l'intelligenza artificiale (IA), il machine learning e l'analisi comportamentale per identificare i principali indicatori di violazione. Identifica gli schemi email sospetti.

In questo esempio, Proofpoint ha identificato dei termini che indicavano che l'email includeva una richiesta di tipo finanziario. Sebbene di per sé la richiesta non sembrasse insolita, se combinata con il cambio dell'indirizzo di risposta, risultava sospetta. Inoltre, il dominio era stato registrato lo stesso giorno dell'invio dell'email.



La dashboard di Proofpoint Targeted Attack Protection (TAP) categorizza ogni minaccia. In questo esempio, mostra che abbiamo identificato la minaccia come attacco BEC, che proveniva da un fornitore e che era coinvolta la fatturazione.

SEZIONE 2

Phishing tramite firma elettronica

Il phishing della firma elettronica è una minaccia che incita un destinatario a divulgare le proprie credenziali d'accesso o altre informazioni personali tramite un messaggio che richiede la loro firma. Il messaggio può includere un contratto o una fattura che devono essere firmati.

In un solo mese nel 2023, Proofpoint ha rilevato oltre 75.000 minacce diverse come quella qui di seguito.

Lo scenario

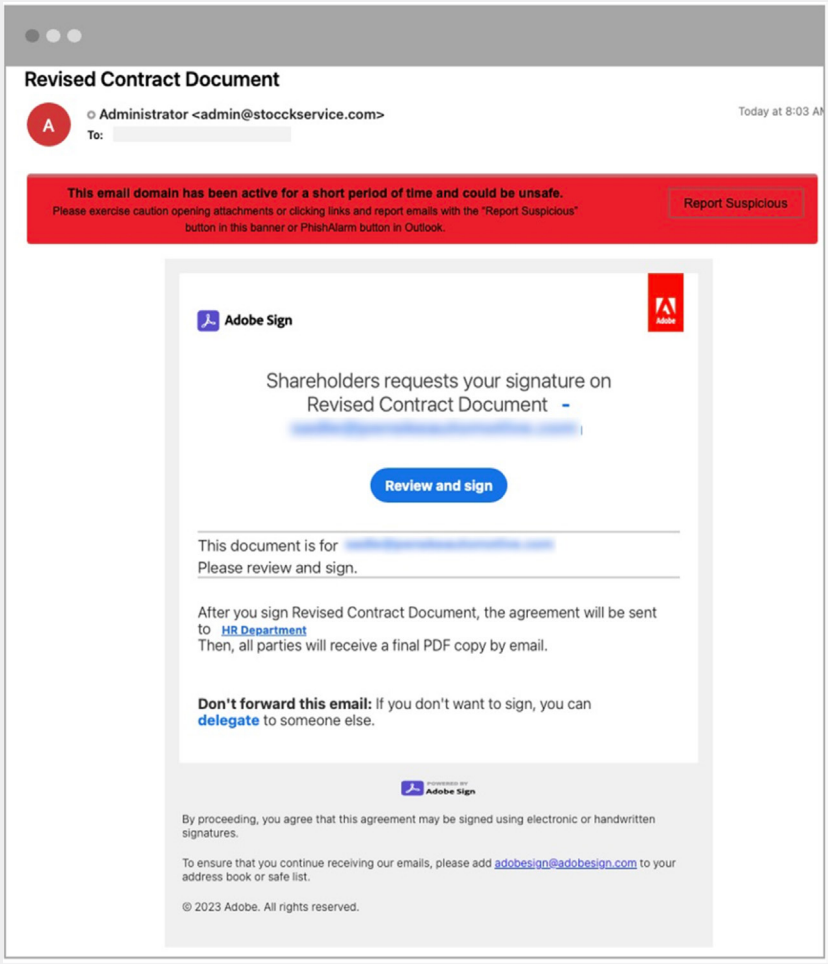
Proofpoint ha rilevato una minaccia di raccolta delle credenziali di accesso ospitata sull'applicazione SaaS Amazon Web Services (AWS) Amplify. L'applicazione è stata utilizzata dal nostro cliente, un'azienda automobilistica con 2.000 collaboratori.

Un criminale informatico aveva creato un'esca di phishing che sembrava un link a un documento sensibile, un contratto aggiornato che doveva essere controllato e controfirmato. L'obiettivo era un collaboratore che gestisce i contratti e con altre responsabilità fiduciarie, che comunica spesso con membri del consiglio, clienti e fornitori come parte della sua attività. Non era perciò insolito che ricevesse questo tipo di richiesta.

Svolgimento dell'attacco

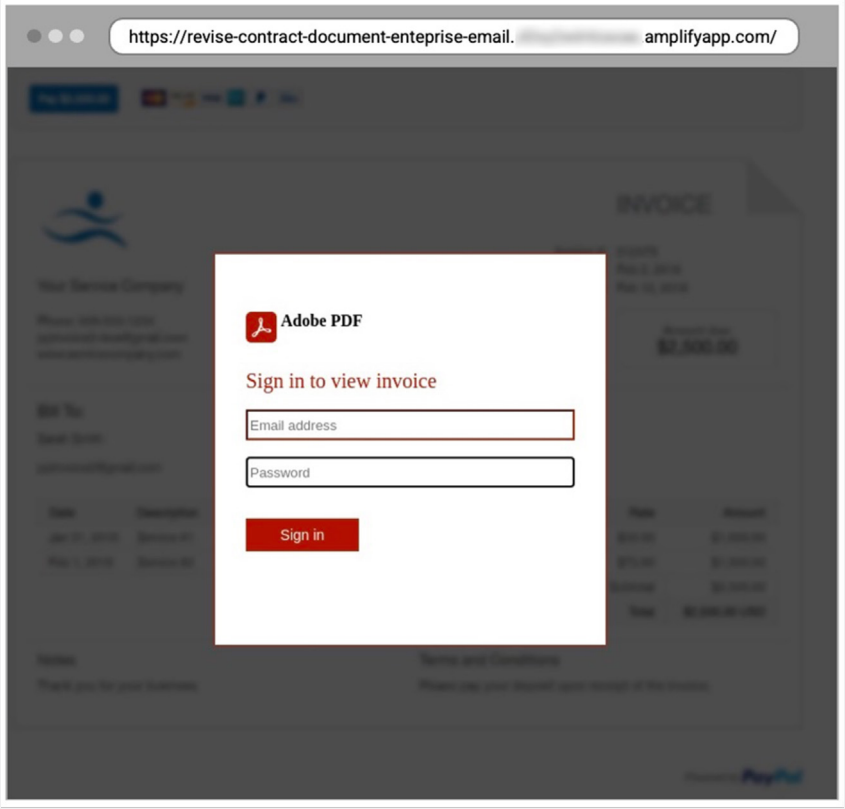
Esaminiamo più da vicino come si è svolto l'attacco:

1. **Il messaggio ingannevole.** Il nostro cliente ha ricevuto un'email che invitava il collaboratore a visualizzare e firmare un contratto aggiornato.



L'email dannosa

2. **L'URL dannoso.** Se il collaboratore avesse fatto clic sull'URL dannoso, avrebbe visualizzato una schermata d'accesso creata per assomigliare ad altre schermate d'accesso legittime. L'obiettivo del criminale informatico era incitare il collaboratore a condividere le sue credenziali d'accesso.



Falsa pagina di login su amplifyapp.com

Perché queste minacce sono difficili da rilevare

Le applicazioni come AWS Amplify e altri servizi SaaS come DocuSign, Adobe Sign e OneSpan Sign vengono spesso utilizzati in questi attacchi. Forniscono ai criminali informatici un modo semplice per distribuire contenuti dannosi, in apparenza legittimi.

In questo scenario, il dominio URL era stato creato cinque anni prima e l'indirizzo IP apparteneva a Amazon, per cui sarebbe stato valutato come legittimo. La maggior parte dei fornitori di soluzioni di sicurezza può rilevare un attacco standard di phishing delle credenziali d'accesso. Tuttavia, il dominio affidabile del fornitore SaaS aggiunge un livello di complessità per la maggior parte dei motori di rilevamento. In particolare, diciannove altri fornitori di sicurezza dell'email, molti dei quali dichiarano di utilizzare tecnologie di IA e machine learning avanzato per bloccare questi attacchi, non hanno rilevato questa minaccia.

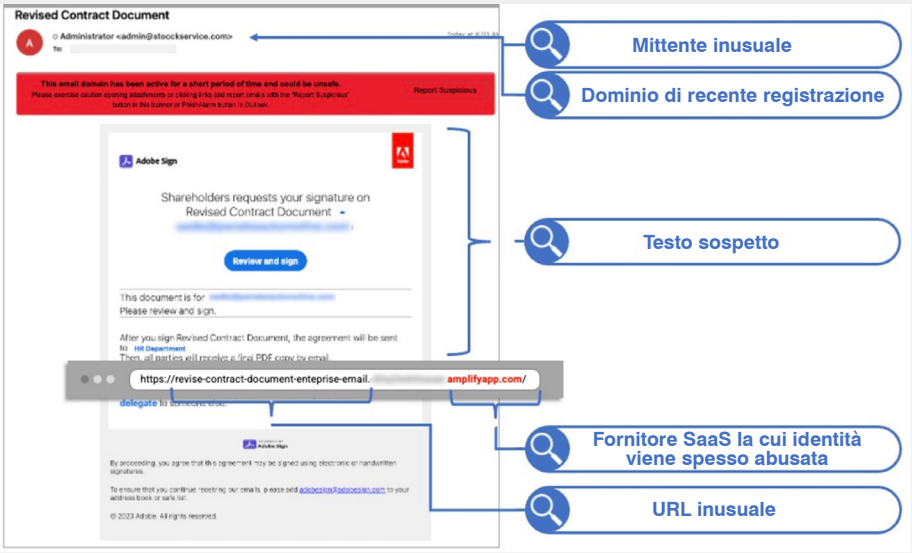
Come Proofpoint ha rilevato l'attacco

Il motore di IA comportamentale utilizza diversi segnali a livello di messaggi per rilevare e bloccare una serie di minacce. Ciò significa che possiamo rilevare le minacce di phishing mai osservate in precedenza e farlo in anticipo nella catena d'attacco in modo da bloccarle prima della loro consegna.

Proofpoint ha eseguito un'analisi multilivello approfondita del profilo dell'utente e ha trovato un mittente/destinatario insolito sulla base di schemi di comunicazione precedenti. Abbiamo scoperto che il mittente comunicava di rado con il destinatario o qualunque altro collaboratore dell'azienda automobilistica.

Utilizzando l'IA comportamentale e il machine learning, Proofpoint ha eseguito un'analisi approfondita dell'URL, per valutare la rilevanza dell'URL sulla base di punti di dati storici precedenti e altre attività anomale. A seguito della disamina dei comportamenti d'invio di tutta l'azienda, è stato stabilito che l'URL non era mai stato utilizzato dal destinatario o da altri collaboratori dell'azienda.

Proofpoint ha anche rilevato l'utilizzo del dominio di un fornitore SaaS legittimo e ben noto. In altre aziende che proteggiamo, abbiamo rilevato criminali informatici che sfruttano questo stesso dominio per distribuire contenuti dannosi.



Sunto delle osservazioni di Proofpoint sulle email di firma elettronica che hanno portato alla sua segnalazione

SEZIONE 3

Minacce TOAD

Le tattiche di social engineering continuano a evolvere con i criminali informatici che cercano modalità nuove e creative per ottenere l'accesso iniziale ai sistemi sensibili. Gli attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery) ne sono una prova. I criminali informatici inviano email ai destinatari e cercano di indurli a chiamare un criminale informatico presso un call center fasullo.

Gli utenti generalmente non sono protetti dalle telefonate dannose. Per questo motivo bloccare queste email è fondamentale. Questi attacchi sono molti difficili da rilevare perché spesso non contengono URL o allegati.

Tra tutte le valutazioni delle minacce in un solo mese nel 2023, Proofpoint ha rilevato oltre 19.000 minacce TOAD che hanno eluso 14 diversi strumenti di sicurezza dell'email.

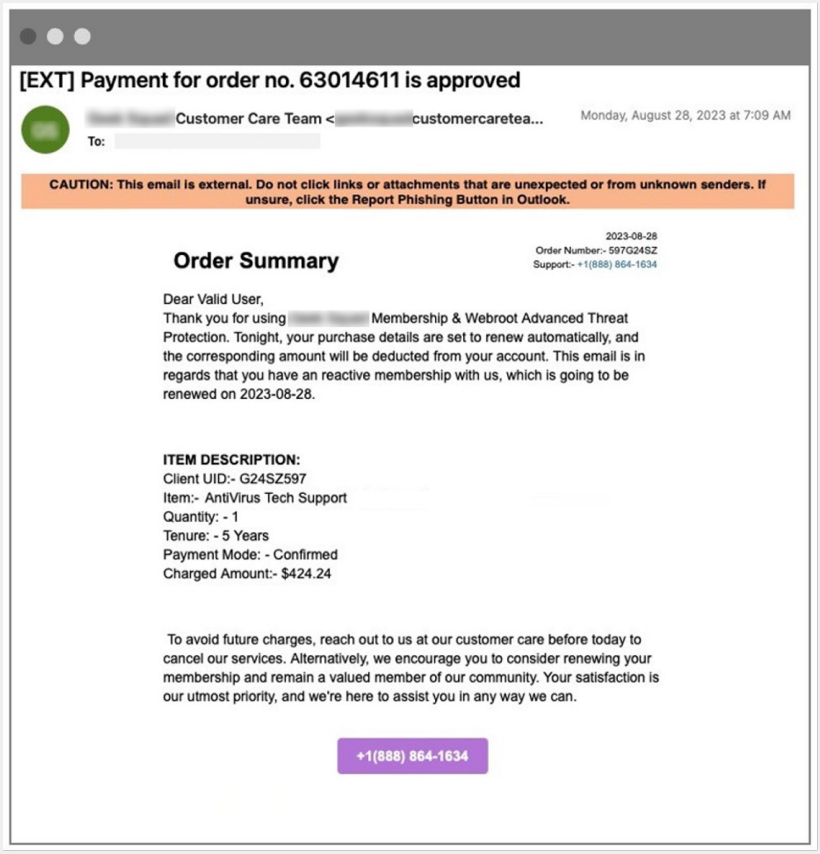
Lo scenario

Proofpoint ha rilevato una minaccia TOAD presso un'azienda manifatturiera con oltre 45.000 collaboratori. Un criminale informatico che millantava di lavorare per una nota azienda di soluzioni antivirus ha inviato un messaggio fraudolento a uno dei suoi collaboratori. Invece di aggiungere un URL o allegati al suo messaggio, il criminale informatico ha incluso un numero di telefono.

Svolgimento dell'attacco

Esaminiamo più da vicino come si è svolto l'attacco:

1. **Il messaggio ingannevole.** Un'email che sembra confermare un acquisto da una nota azienda di tecnologia.



Email dannosa iniziale recapitata alla casella email del destinatario

2. **La sequenza dell'attacco TOAD.** Se il collaboratore avesse chiamato quel numero, il criminale informatico lo avrebbe convinto a fare clic su un link dannoso sul suo computer per innescare varie minacce, tra cui l'accesso remoto, il furto di dati sensibili o un'infezione ransomware.

Panoramica di una sequenza di un attacco TOAD

Perché queste minacce sono difficili da rilevare

Le minacce TOAD possono essere difficili da rilevare perché raramente includono payload dannosi. Inoltre, i criminali informatici spesso utilizzano domini noti che appartengono a Google, Microsoft o altri servizi email legittimi.

Poiché questa particolare minaccia TOAD è stata inviata da un dominio di proprietà di Google, il messaggio ha superato i controlli di autenticazione dell'email come SPF (Sender Policy Framework) e DMARC. Questo messaggio non includeva un payload dannoso, il che potrebbe spiegare perché lo strumento di sicurezza esistente dell'azienda manifatturiera non ha intercettato la minaccia.

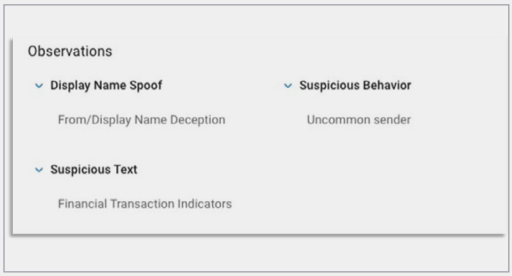
Come Proofpoint ha rilevato l'attacco

Proofpoint utilizza IA e machine learning avanzati per analizzare e combinare diversi indicatori comportamentali e rilevare le minacce TOAD. Questo approccio è più affidabile che limitarsi a tracciare e mantenere un database di numeri di telefono dannosi precedentemente identificati associati ad attacchi TOAD.

Quando il motore di IA comportamentale di Proofpoint ha analizzato il messaggio, ha trovato riferimenti a una transazione finanziaria e la necessità di agire con urgenza, due indicatori di un'email potenzialmente dannosa. Un ulteriore indizio è che le minacce TOAD includono sempre un numero di telefono e sollecitano il destinatario a chiamarlo con urgenza. Per questo motivo Proofpoint analizza i messaggi alla ricerca di un numero di telefono.

Abbiamo eseguito un'analisi a più livelli, in base alla quale abbiamo trovato che il destinatario non aveva mai ricevuto email da quel mittente, sulla base di schemi di comunicazioni precedenti. In realtà, nessun collaboratore in azienda aveva mai ricevuto un'email da questo mittente.

Come è tipico degli attacchi TOAD, i criminali informatici inviano spesso messaggi che sembrano provenire da un marchio legittimo per cercare di creare una relazione di fiducia implicita. Le nostre analisi hanno rilevato questa tattica.



Sintesi delle osservazioni di Proofpoint che hanno portato alla segnalazione

SEZIONE 4

Dirottamento degli stipendi

Il dirottamento degli stipendi è una forma di attacco BEC. Gli obiettivi principali di questi attacchi sono generalmente collaboratori che completano richieste legate agli stipendi. In generale, un criminale informatico si finge un collaboratore che deve aggiornare le informazioni del conto su cui viene accreditato il suo stipendio. Le nuove informazioni in realtà corrispondono a un account che appartiene al criminale informatico. Una volta completato il cambio, il denaro perso non può essere recuperato dall'azienda.

Il dirottamento degli stipendi non è una nuova forma di attacco BEC, ma la sua frequenza è in aumento. Proofpoint continua a osservare questo tipo di minaccia superare le difese di altri strumenti di sicurezza dell'email. Tra tutte le nostre recenti valutazioni delle minacce, abbiamo rilevato che più di 400 di questi attacchi hanno eluso 12 altri strumenti di sicurezza dell'email.

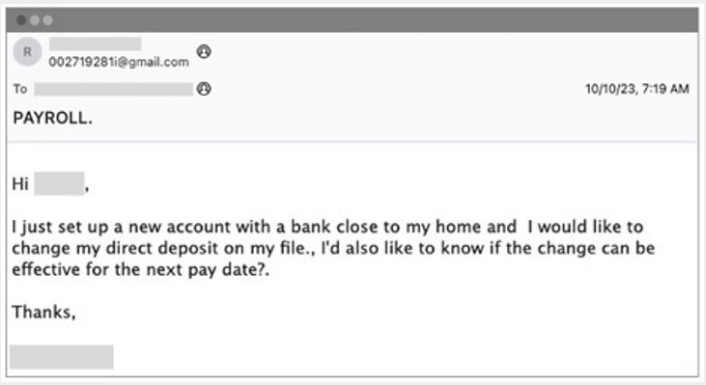
Lo scenario

Proofpoint ha rilevato una di queste minacce presso una società del settore dell'energia e dei servizi pubblici con 300 collaboratori. In questo caso, un criminale informatico si è finto un impiegato e ha inviato un'email al direttore delle risorse umane dell'azienda. Il messaggio non solo è stato consegnato dallo strumento di sicurezza delle email esistente nell'azienda, ma anche lo strumento di correzione dopo la consegna basato su API non è riuscito a rilevarlo e ritirarlo.

Svolgimento dell'attacco

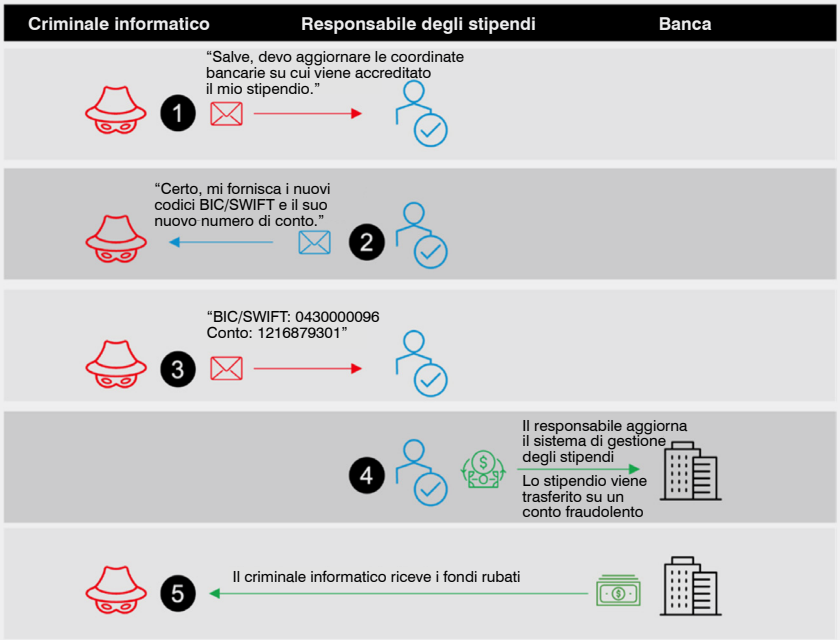
Esaminiamo più da vicino come si è svolto l'attacco:

1. **Il messaggio ingannevole.** Il criminale informatico ha inviato una richiesta alle risorse umane chiedendo l'aggiornamento delle sue informazioni di accredito del suo stipendio. Questo messaggio era stato inviato da un account che sembrava un account email personale di un collaboratore legittimo.



Messaggio dannoso iniziale recapitato alla casella email del destinatario

2. **La sequenza d'attacco del dirottamento degli stipendi.** Se il destinatario avesse risposto al messaggio, l'obiettivo del criminale informatico sarebbe stato convincerlo a trasferire denaro su un altro conto bancario non appartenente al collaboratore vittima del furto d'identità.



Sequenza d'attacco tipica di dirottamento degli stipendi

Perché queste minacce sono difficili da rilevare

Queste minacce raramente includono payload dannosi come allegati o URL. Inoltre, solitamente vengono inviate dai servizi di email personale come Google, Yahoo e iCloud e prendono di mira utenti specifici.

In particolare, gli strumenti di sicurezza delle email basati su API, che eseguono l'analisi delle minacce dopo la consegna, sono quelli che con più probabilità non rileveranno questo tipo di minaccia. Ciò in parte è dovuto al loro funzionamento. Affinché questi strumenti siano efficaci, i team IT e della sicurezza devono alimentarli manualmente con un dizionario di possibili nomi visualizzati di tutti i collaboratori, attività dispendiosa in termini di tempo e difficile da applicare su grande scala.

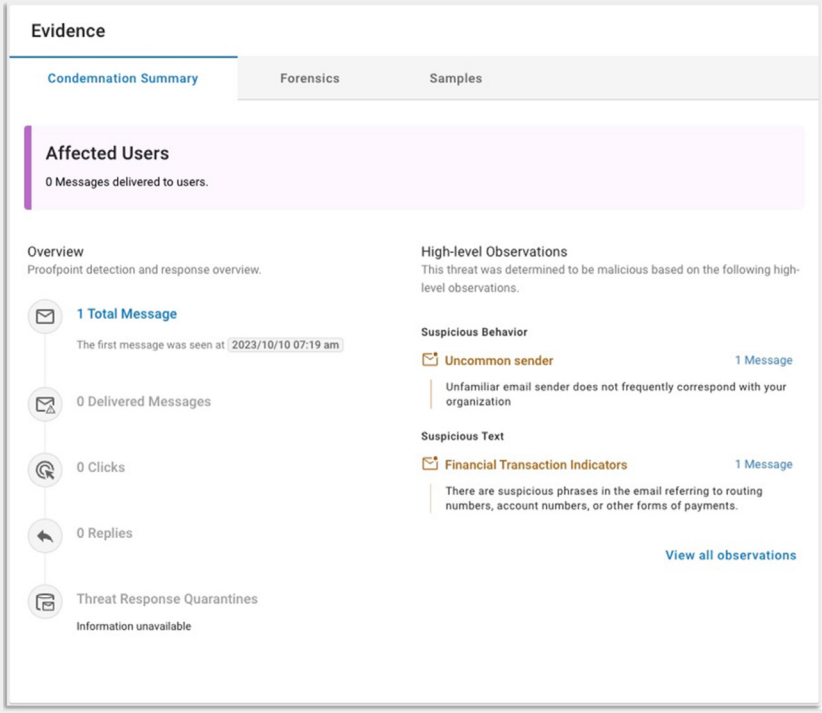
Per evitarlo, molte aziende semplicemente scelgono di nascondere il nome visualizzato solo per i dirigenti senior. Ma i criminali informatici autori del dirottamento degli stipendi non si limitano a rubare l'identità dei dirigenti, ma prendono di mira chiunque in azienda abbia accesso alle finanze aziendali. Nel nostro precedente esempio, un criminale informatico ha sfruttato proprio questo punto debole.

Come Proofpoint ha rilevato l'attacco

Per comprendere l'obiettivo reale di un'email, uno strumento di sicurezza dell'email deve interpretare il tono e l'intento del messaggio. Per farlo, Proofpoint utilizza diversi segnali di rilevamento, motori d'analisi e l'IA comportamentale. I nostri motori di rilevamento basati su IA e machine learning vengono costantemente istruiti con milioni di email al giorno provenienti dal nostro ecosistema mondiale di threat intelligence.

Uno dei segnali che utilizziamo per rilevare le email dannose è l'analisi delle comunicazioni tra mittente e destinatario nonché la frequenza dei loro messaggi. Nell'esempio qui sopra, il direttore delle risorse umane riceveva raramente email dall'indirizzo email personale di quel particolare collaboratore.

La maggior parte degli strumenti di sicurezza utilizza segnali studiati per identificare i mittenti insoliti. Per questo motivo creano un elevato numero di falsi positivi. Proofpoint opera in modo diverso. Combiniamo diversi segnali per assicurarci di non dipendere troppo da uno o due segnali. Combinando il segnale che permette di identificare i mittenti insoliti con un'analisi del linguaggio utilizzato nel corpo del messaggio, Proofpoint estrapola il tono e interpreta l'intento di un'email.



Sintesi della minaccia neutralizzata da Proofpoint che evidenzia i segnali che ci hanno portato a segnalare questa minaccia

SEZIONE 5

Violazione alla supply chain

Le violazioni della supply chain sono un'altra forma di attacco BEC in aumento. In questi attacchi, un criminale informatico prende di mira un'azienda violando la sicurezza dei suoi fornitori e altre terze parti della sua supply chain. I criminali informatici sanno che le aziende con supply chain mature tendono a avere difese di sicurezza informatica più solide, rendendoli obiettivi più difficili da colpire.

Per questo motivo, piuttosto che lanciare un attacco diretto, il criminale informatico si infiltra in una delle entità di fiducia dell'azienda assumendone l'identità. Spesso, utilizzano l'hijacking del thread di discussione, nel quale i criminali informatici prendono di mira account email specifici e li compromettono in modo da poter spiare le conversazioni. Al momento giusto, i criminali informatici si inseriscono nella conversazione. Alcune volte, sono abbastanza audaci da avviare una nuova conversazione.

Questi attacchi sono sempre più diffusi e sofisticati. Nel 2023, la più importante violazione della supply chain è costata oltre 9,9 miliardi di dollari alle aziende coinvolte. E oltre mille aziende e 60 milioni di persone ne hanno subito gli effetti[4].

4 TechCrunch, "MOVEit, the Biggest Hack of the Year, by the Numbers" (MOVEit, la violazione più grande dell'anno in cifre), agosto 2023.

Lo scenario

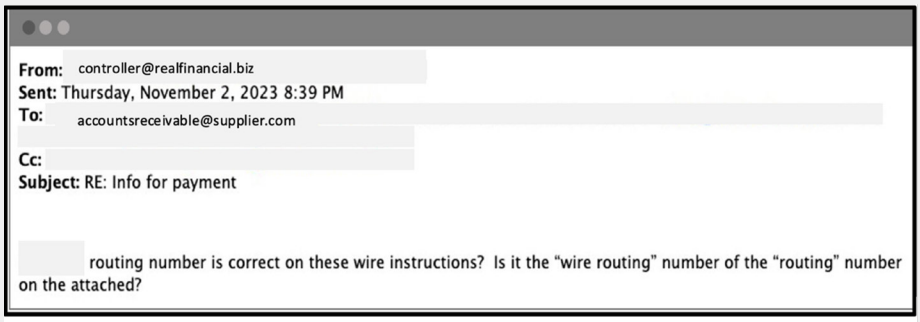
Proofpoint ha rilevato un messaggio fraudolento che sembrava provenire da un collaboratore del reparto creditizio di una piccola società di servizi finanziari in Florida. Tuttavia, si trattava in realtà di un criminale informatico che aveva rubato l'identità di qualcun altro, con l'obiettivo di lanciare un attacco della supply chain contro un grande studio legale di Boston.

In un'email indirizzata al controller finanziario dello studio legale, il criminale informatico richiedeva che i pagamenti venissero effettuati su un altro conto.

Svolgimento dell'attacco

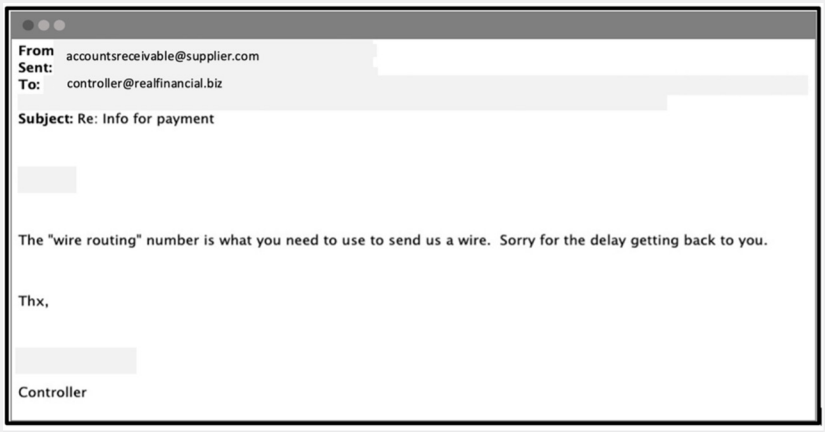
Esaminiamo più da vicino come si è svolto l'attacco:

1. **Messaggio legittimo del cliente.** Il cliente ha inviato un'email al fornitore per confermare la correttezza delle coordinate bancarie da utilizzare per i pagamenti.

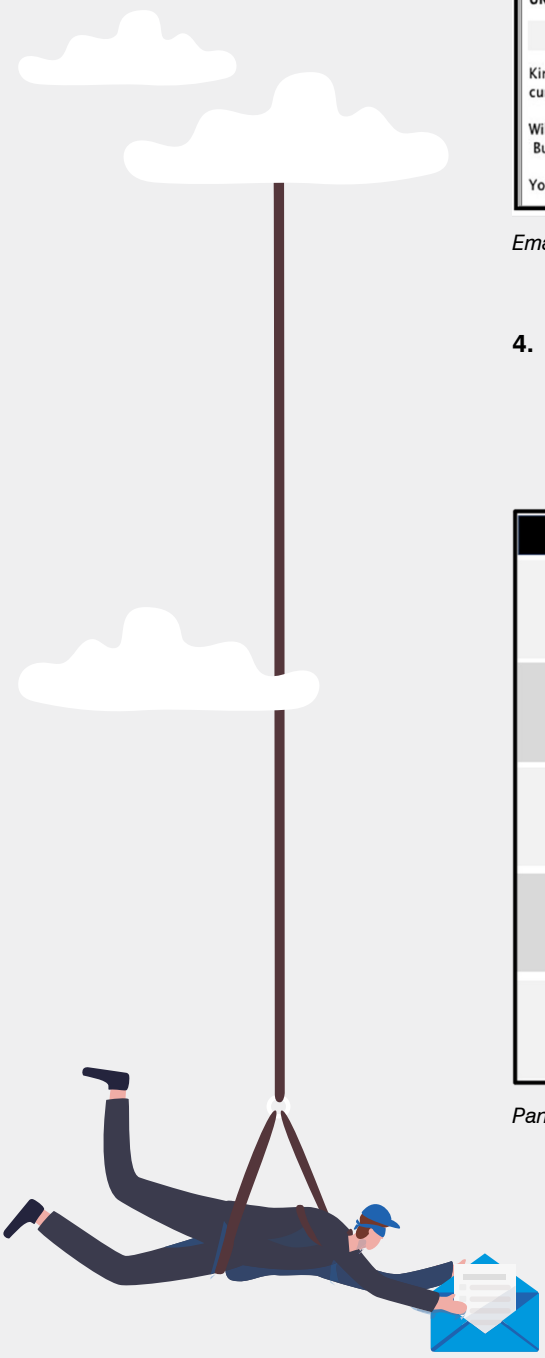


Messaggio legittimo del cliente che conferma le coordinate bancarie da utilizzare per i pagamenti

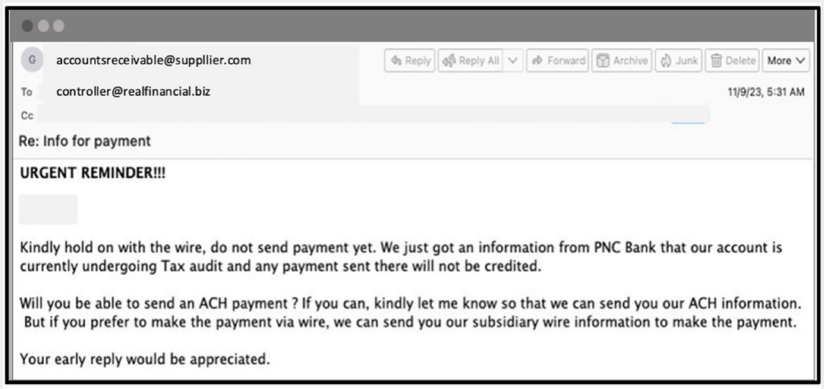
2. **Email legittima del fornitore.** Il fornitore ha risposto alla domanda di conferma delle coordinate bancarie da utilizzare per i pagamenti.



Email legittima del fornitore in risposta alla richiesta di conferma delle coordinate bancarie da utilizzare per i pagamenti

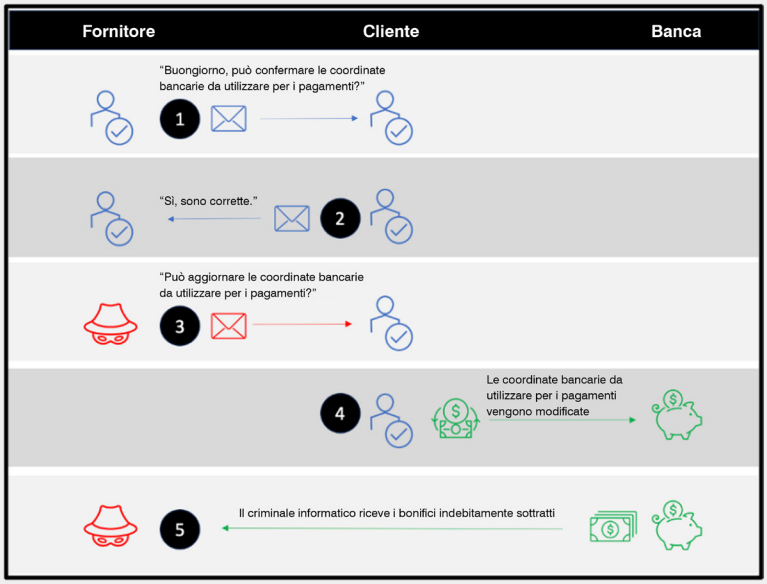


3. **Email fraudolenta del criminale informatico.** Il criminale informatico si è inserito nel flusso inviando un'email al cliente da un account diverso che appariva molto simile a quello del fornitore. In realtà, l'email era stata inviata da un dominio fotocopia, che includeva una lettera aggiuntiva nell'indirizzo del mittente. Per far sembrare l'email legittima, il criminale informatico ha copiato l'intera conversazione email sotto il corpo del messaggio.



Email fraudolenta del criminale informatico

4. **La sequenza dell'attacco di violazione della supply chain.** Il criminale informatico ha richiesto che i pagamenti a mezzo bonifico bancario fossero effettuati su un altro contro attraverso un portale di pagamento automatizzato. Il criminale informatico era l'intestatario di quel nuovo conto.



Panoramica della sequenza d'attacco

Perché queste minacce sono difficili da rilevare

Gli attacchi di violazione della supply chain raramente includono payload dannosi, uno dei motivi per cui sono difficili da individuare e neutralizzare. Il criminale informatico ha utilizzato il social engineering per convincere il destinatario ad aiutarlo nel raggiungere il suo obiettivo.

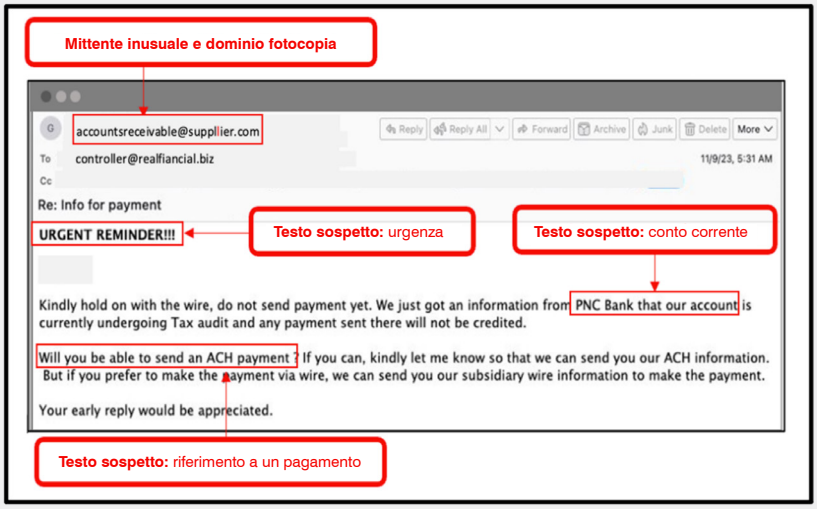
In questo scenario, un fornitore ha richiesto a un'azienda di modificare le coordinate bancarie da utilizzare per i pagamenti. Una tale richiesta non è infrequente: per questo motivo, gli strumenti di sicurezza dell'email basati sulle API faticano a rilevare tali attacchi. Gli strumenti basati sulle API si basano su segnali che permettono di identificare i mittenti inusuali e generano molti falsi positivi e avvisi. Questo approccio limitato basato sull'IA comportamentale aiuta a spiegare perché molte aziende si lamentano delle numerose informazioni inutili generate da questi segnali.

Per rilevare questi tipi di messaggi dannosi, uno strumento di sicurezza dell'email deve interpretare il tono contestuale nonché l'intento di un messaggio. È l'unico modo per stabilire il vero obiettivo di un messaggio prima che venga recapitato nella casella email di un utente.

Come Proofpoint ha rilevato l'attacco

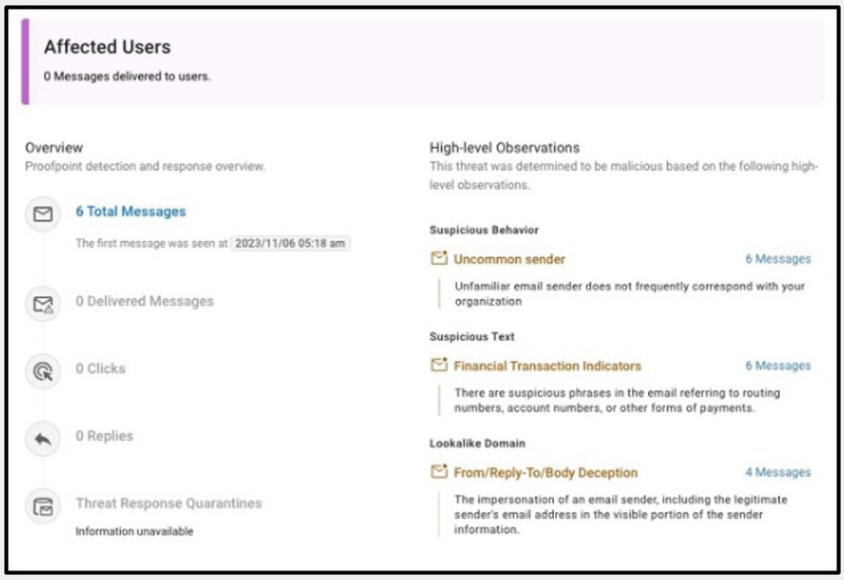
Proofpoint combina le informazioni di threat intelligence con l'IA comportamentale e il machine learning per stabilire se le email sono legittime o dannose. Addestriamo costantemente i nostri motori di rilevamento con milioni di email al giorno provenienti dal nostro ecosistema mondiale di threat intelligence. In questo modo possiamo rilevare e bloccare questi tipi di messaggio con un livello di fiducia più elevato.

Per ridurre le informazioni inutili, combiniamo diversi segnali invece di affidarci solo a uno o due segnali, che potrebbe generare un numero elevato di falsi positivi. Un segnale è l'analisi delle comunicazioni tra i mittenti e i destinatari nonché la frequenza di questi messaggi. Analizziamo anche il linguaggio utilizzato nel corpo del messaggio per capire il tono e interpretarne l'intento. Verifichiamo anche la presenza di domini fotocopia e richieste urgenti di pagamento.



Diversi segnali di rilevamento identificati nell'email di un fornitore fraudolento

Analizzando il contenuto e l'intento dell'email nonché il linguaggio utilizzato, Proofpoint ha stabilito che il messaggio del nostro esempio era una richiesta finanziaria fraudolenta. Questa campagna presentava solo pochi messaggi che rubavano l'identità di una persona e prendeva di mira solo un cliente. Nessun altro cliente Proofpoint era ancora stato colpito da questo attacco.

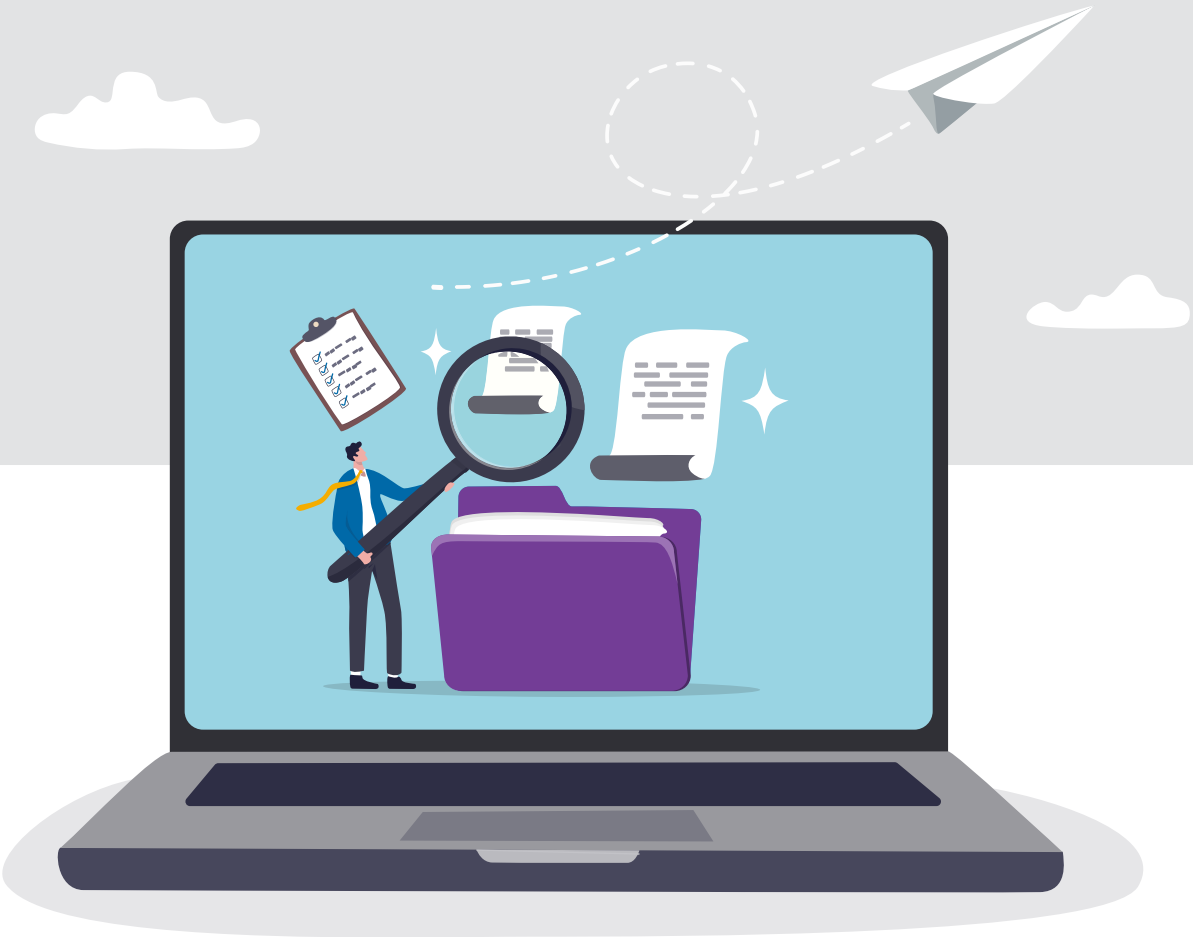


Sintesi della minaccia neutralizzata che evidenzia i segnali che hanno portato Proofpoint a bloccare questa minaccia

SEZIONE 6

Conclusioni

Tutte queste truffe non fanno che sottolineare la necessità di adottare solide misure di sicurezza informatica a più livelli.



Per rimanere un passo avanti sulle minacce in costante evoluzione, devi adottare un approccio completo alla protezione contro le minacce che prendono di mira i tuoi collaboratori:

- **Rileva le minacce prima della consegna.** Il solo mezzo di proteggere gli utenti è di bloccare i messaggi dannosi prima della loro consegna. In base alle ricerche condotte da Proofpoint, un utente su sette fa clic su un'email entro un minuto. Scegli uno strumento che combina algoritmi di machine learning e una threat intelligence avanzata per identificare e bloccare le minacce avanzate.
- **Forma i tuoi utenti.** I tuoi collaboratori, collaboratori interinali e i tuoi partner sono la tua prima linea di difesa. Assicurati che ricevano formazione di sensibilizzazione alla sicurezza informatica per tutti i tipi di attacchi. Ricorda loro di segnalare rapidamente tutti i comportamenti insoliti.
- **Esegui regolarmente verifiche di sicurezza.** Le verifiche possono aiutarti a identificare le potenziali vulnerabilità nel tuo ambiente. Come parte del lavoro, assicurati di cercare le irregolarità nelle tue configurazioni e nei log d'accesso.
- **Imposta il tuo sistema per monitorare gli errori di configurazione.** Oltre a ricercare gli errori di configurazione, non dimenticarti di attivare la correzione automatica. Potrai così rilevare le modifiche non autorizzate e correggerle prontamente, impedendo ai criminali informatici di stabilire persistenza nella tua azienda.
- **Crea un piano di risposta agli incidenti.** Identifica diversi scenari d'attacco. Quindi, stabilisci come analizzerai e correggerai gli incidenti. Assicurati di testare la reale efficacia del tuo piano eseguendo regolarmente esercizi di simulazione.

Passi successivi

Oggi più che mail è importante proteggere la tua azienda dalle minacce email in aumento. Devi adottare un approccio reattivo per proteggere la tua azienda, i tuoi collaboratori e i tuoi clienti da attacchi avanzati come ransomware, minacce BEC e phishing delle credenziali di accesso.

La valutazione rapida dei rischi legati all'email di Proofpoint ti fornisce visibilità e informazioni complete sulla tua vulnerabilità agli attacchi. Ti aiuta a identificare le persone prese di mira da minacce email nella tua azienda.

Non aspettare che sia troppo tardi per testare la sicurezza della tua email. Contatta Proofpoint per una **valutazione gratuita dei rischi legati all'email**.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **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 l'85% 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**.

proofpoint.

0503-006-05-01 07/24