Cinque passi per contrastare la violazione dell'email aziendale

Vantaggi principali

- Rilevamento e blocco delle varianti BEC indirizzando le molteplici tattiche utilizzate dai criminali informatici
- Visibilità sugli utenti più attaccati e sulle terze parti che presentano il maggior rischio d'attacco
- Ricezione di notifiche quando i fornitori con cui interagisci hanno account che potrebbero essere compromessi
- Formazione degli utenti all'identificazione e segnalazione delle frodi via email
- Accelerazione della risposta alle minacce e risparmio di tempo grazie all'automazione delle attività di correzione
- Miglioramento della sicurezza e dell'efficienza operativa grazie a una soluzione integrata end-to-end

La violazione dell'email aziendale (BEC, Business Email Compromise) contribuisce in modo significativo alle perdite finanziarie. Secondo l'Internet Crime Report dell'FBI, le perdite annuali causate dagli attacchi BEC hanno superato i 2,7 miliardi di dollari, ovvero 80 volte in più rispetto al ransomware[1].

Gli attacchi BEC spesso violano l'identità dei mittenti con email che cercano di far credere ai destinatari di interagire con una fonte affidabile. I criminali informatici sfruttano poi questa fiducia per indurre i destinatari a effettuare, ad esempio, un bonifico fraudolento. Difendersi da questi attacchi è difficile, perché non sfruttano payload dannosi per essere efficaci. Alcuni criminali informatici si spingono oltre, utilizzando account di fornitori legittimi ma compromessi per lanciare i loro attacchi BEC.

La protezione della tua azienda contro gli attacchi BEC richiede sia la tecnologia che la formazione. Hai bisogno di un approccio più globale per interrompere davvero la catena d'attacco di violazione tramite email. Proofpoint può aiutarti.

Proofpoint è il primo e unico fornitore a offrire una piattaforma completa e integrata di protezione contro le minacce che fornisce i seguenti vantaggi:

- Rilevamento e blocco delle minacce BEC prima che raggiungano le caselle email
- Formazione degli utenti all'identificazione e segnalazione delle frodi via email
- Visibilità sui rischi associati a fornitori e account di terze parti compromessi
- Automazione del rilevamento e della neutralizzazione delle minacce
- Protezione del tuo marchio dalle frodi via email

Questa scheda sulla soluzione descrive più in dettaglio il nostro approccio.

1 *Internet Crime Report*, FBI, 2022.

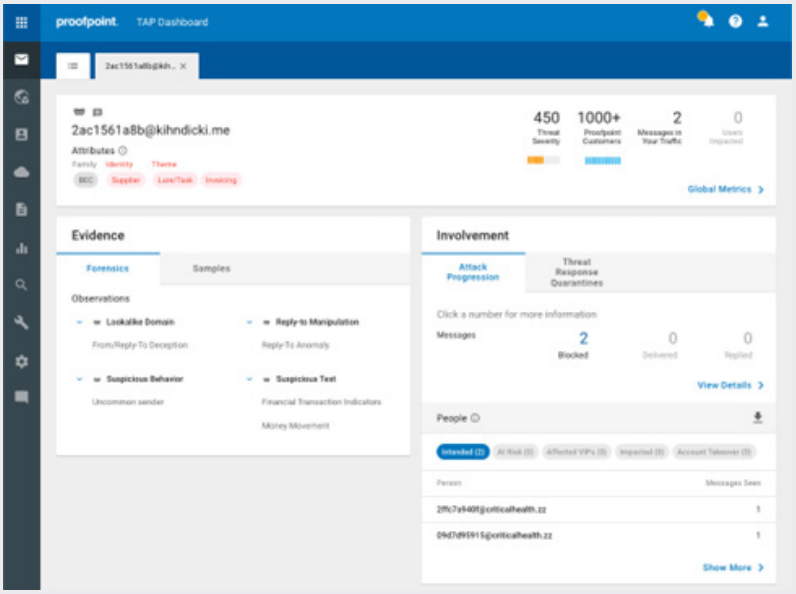

Figura 1. Proofpoint identifica gli utenti più colpiti dagli attacchi BEC e fornisce una visibilità granulare sui dettagli delle minacce BEC, compresi i temi, le tattiche utilizzate e altro ancora.

Rilevamento e blocco delle minacce fraudolente prima che si infiltrino nel tuo ambiente

La nostra piattaforma integrata sfrutta Proofpoint Advanced BEC Defense, alimentato da Supernova, il nostro più recente motore di rilevamento degli attacchi BEC basato sull'intelligenza artificiale (IA). Quest'avanzata tecnologia ha permesso di moltiplicare di 17 volte il numero di minacce identificate e di estendere la nostra capacità di rilevamento a un'ampia varietà di frodi tramite email.

Proofpoint Advanced BEC Defense conduce un'analisi approfondita su vari attributi dei messaggi, tra cui:

- Dati dell'intestazione del messaggio
- Indirizzo IP del mittente
- Relazione tra mittente e destinatario
- Reputazione del mittente

Proofpoint Advanced BEC Defense utilizza l'analisi semantica basata su moduli linguistici di grandi dimensioni per analizzare il corpo dei messaggi (sentimento e linguaggio), il che aiuta a stabilire se il messaggio rappresenta una minaccia BEC. Il motore di machine learning comportamentale tiene traccia delle attività per estrarre indicatori comportamentali, o firme delle minacce, al fine di comprendere i modelli da utilizzare per rilevare le anomalie in tempo reale.

Alcuni degli elementi tracciati includono:

- Se un mittente sta inviando un numero insolito di email
- Se le email provengono da un indirizzo IP insolito
- Se un mittente è mai stato visto dagli utenti dell'azienda

Questi segnali rafforzano lo stack di rilevamento e consentono di gestire nuovi casi d'uso. Di conseguenza, il motore di rilevamento è ora in grado di rilevare altre minacce avanzate veicolate tramite l'email, come ransomware, phishing delle credenziali d'accesso e account di terze parti compromessi.

Proofpoint Advanced BEC Defense rileva lo spoofing del nome visualizzato e i domini fotocopia. Blocca anche le frodi dei fornitori più sofisticate grazie a un'analisi dinamica dei messaggi che rileva le tattiche associate alle frodi della fatturazione dei fornitori. Utilizza il machine learning per adattarsi e apprendere in tempo reale e punta a un basso tasso di falsi positivi.

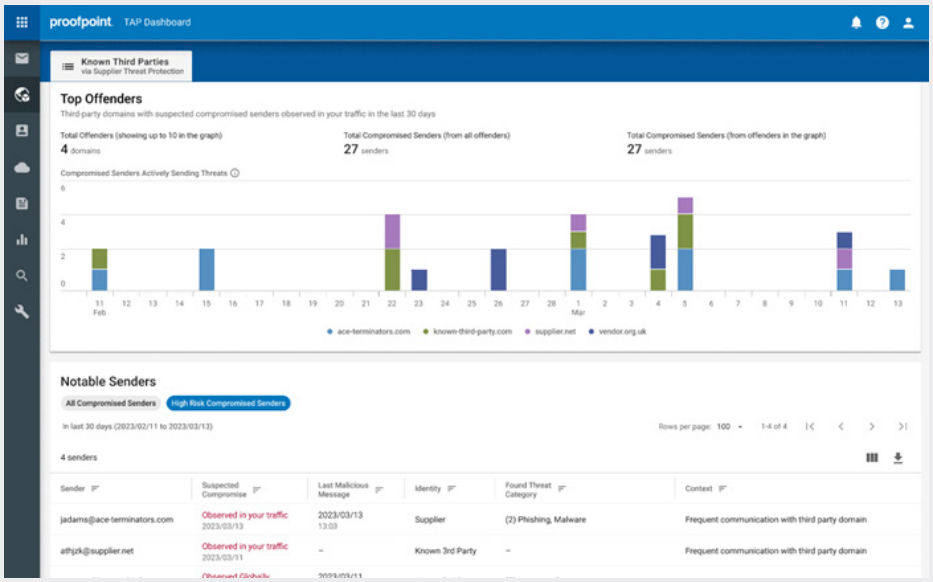

Figura 2. Il componente aggiuntivo Supplier Threat Protection rileva gli account di terze parti compromessi con cui la tua azienda interagisce.

Visibilità sui rischi di attacchi BEC

Per meglio comprendere, comunicare e mitigare i rischi di attacchi BEC a cui sei esposto, ti aiutiamo a rispondere alle seguenti domande che il tuo management potrebbe porti:

- A quali rischi di attacchi BEC siamo esposti?
- Quali sono gli utenti più colpiti?
- Quali delle nostre terze parti fidate hanno account potenzialmente compromessi?
- Come possiamo quantificare e ridurre i rischi?

Proofpoint è in grado di identificare gli utenti più attaccati e quelli che hanno più probabilità di lasciarsi trarre in inganno. Forniamo una visibilità granulare sui dettagli delle minacce BEC mostrandoti i temi di cui diffidare come le truffe con carte regalo, le frodi dei libri paga e le frodi legate alle fatture dei fornitori (consultare la Figura 1). Puoi quindi applicare controlli di sicurezza adattivi agli utenti presi di mira e comunicare meglio i rischi alla tua dirigenza.

Proofpoint estende la tua protezione fornendo visibilità e approfondimenti sui fornitori a rischio. Ti aiutiamo a gestire i rischi e le minacce per i fornitori grazie ai seguenti vantaggi:

- Identificazione proattiva degli account dei fornitori potenzialmente frodati e compromessi
- Vista delle minacce BEC incentrate sui fornitori e in base alle priorità
- Identificazione e prevenzione delle minacce provenienti dai domini dei fornitori e da domini fotocopia dannosi

Valutiamo il livello di rischio dei domini dei fornitori e lo classifichiamo come prioritario, notificandoti gli account potenzialmente compromessi. In questo modo i team della sicurezza possono concentrarsi sui fornitori che rappresentano il rischio più elevato per la tua azienda.

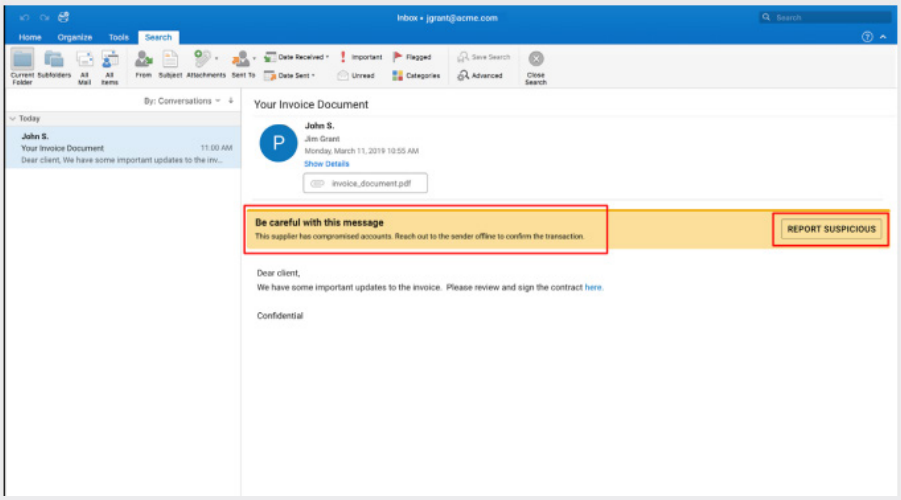

Figura 3. La visualizzazione di avvisi per le email sospette mette in guardia i tuoi utenti e permette loro di prendere decisioni più informate in merito alle email di cui non sono certi della legittimità.

Potenziamento della resilienza degli utenti agli attacchi BEC

Gli attacchi BEC prendono di mira le persone e le spingono a compiere azioni dannose inconsapevolmente. Poiché questi attacchi fraudolenti utilizzano il social engineering e il furto d'identità, i tuoi utenti sono spesso tua ultima linea di difesa. Questo è il motivo per cui per ridurre i rischi di attacchi BEC sono necessarie sia la tecnologia che la formazione.

Grazie al nostro tasto di segnalazione PhishAlarm, puoi mettere a disposizione dei tuoi utenti la conoscenza e gli strumenti adatti per identificare e segnalare le email fraudolente sospette. Inoltre, la visualizzazione di avvisi per le email sospette aiuta gli utenti a prendere decisioni più informate. Puoi anche formare gli utenti sulle ultime tattiche di attacco utilizzate negli attacchi BEC e assegnare una formazione mirata agli utenti più attaccati. In questo modo puoi rafforzare la loro resilienza agli attacchi BEC.

Automazione della risposta alle minacce

Molte aziende hanno problemi di carenza di personale nei loro team della sicurezza informatica. Perciò è difficile identificare, analizzare e neutralizzare le minacce BEC in tutta l'azienda. Noi portiamo l'automazione in prima linea nei processi di rilevamento e correzione delle minacce. Grazie a Proofpoint Threat Response Auto-Pull (TRAP) puoi mettere rapidamente in quarantena o eliminare qualsiasi email sospetta o indesiderata con un solo clic. L'automazione si estende ai messaggi inoltrati o ricevuti da altri utenti, nonché ai messaggi ricevuti da altri clienti Proofpoint. Ciò significa che tutti beneficiano delle informazioni aggiuntive raccolte.

Semplifichiamo anche la gestione delle caselle email di segnalazione degli abusi, Le email segnalate dagli utenti vengono analizzate automaticamente e quelle ritenute dannose possono essere messe in quarantena o eliminate. Ciò consente di accelerare la risposta alle minacce e ridurre i compiti manuali.

Protezione del tuo marchio dalle frodi via email

In caso di spoofing del marchio, i criminali informatici utilizzano il nome e il marchio della tua azienda per ingannare i tuoi clienti e partner commerciali e per sottrarre denaro. Proofpoint protegge il tuo marchio dallo spoofing negli attacchi BEC, impedendo l'invio di email fraudolente tramite i tuoi domini di fiducia. Autentichiamo tutte le email inviate da o verso la tua azienda. Semplificando l'implementazione dell'autenticazione DMARC grazie a un flusso di lavoro guidato e servizi gestiti, ti aiutiamo a proteggere i tuoi domini dallo spoofing e a bloccare tutti i tentativi di invio di email non autorizzate dai tuoi domini affidabili.

Inoltre, ti forniamo visibilità su tutte le email inviate attraverso il tuo dominio, incluse quelle inviate dai mittenti di terze parti affidabili. Identifichiamo i domini simili al tuo. Rileviamo dinamicamente i domini di nuova registrazione che abusano dell'identità del tuo marchio negli attacchi tramite email. Grazie al nostro servizio Virtual Takedown, puoi intervenire rapidamente per rimuovere questi siti.

Sintesi

Le frodi via email sono responsabili della maggior parte delle perdite finanziarie. A fronte del crescente livello di sofisticazione dei truffatori, gli schemi BEC si sono evoluti per includere frodi contro i fornitori complesse. Proofpoint è la prima e unica azienda a fornire una soluzione integrata, end-to-end, che protegge efficacemente contro queste minacce emergenti.

La nostra soluzione di protezione contro gli attacchi BEC offre i seguenti vantaggi:

- Rilevamento e blocco di diversi tipi di attacchi BEC
- Visibilità sulla superficie d'attacco umana e informazioni granulari sulle minacce BEC
- Identificazione dei fornitori che rappresentano un rischio e che potrebbero avere account compromessi.
- Rafforzamento della resilienza degli utenti agli attacchi BEC
- Automazione delle indagini e della risposta agli incidenti
- Protezione del tuo marchio dalle frodi via email

Proofpoint rende più veloce, più facile e più efficace contrastare gli attacchi BEC.

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**.