Cinco medidas para luchar contra las estafas Business Email Compromise (BEC)

Ventajas principales

- Detección y neutralización de variantes BEC gracias a la cobertura de múltiples tácticas usadas por los cibercriminales.
- Visibilidad de los usuarios más atacados y qué colaboradores externos presentan el mayor riesgo de ataque.
- Notificaciones cuando los proveedores con los que interactúa tengan cuentas potencialmente comprometidas.
- Formación de los usuarios para que identifiquen y denuncien las estafas por correo electrónico.
- Aceleración de la respuesta a amenazas y ahorro de tiempo gracias a la automatización de la corrección.
- Mejora de la seguridad y de la eficacia operativa con una solución integrada completa.

Las estafas Business Email Compromise (BEC) contribuyen enormemente a las pérdidas financieras de las empresas. Según el informe Internet Crime Report del FBI, las pérdidas anuales atribuibles a las estafas BEC superan los 2700 millones de dólares, es decir, 80 veces más que las que provoca el ransomware[1].

Los ataques BEC suelen suplantar a remitentes con mensajes de correo electrónico que hacer creer a los destinatarios que están interactuando con una fuente de confianza. A partir de ahí, los atacantes utilizan esta confianza para conseguir que los destinatarios realicen, por ejemplo, una transferencia bancaria fraudulenta u otro desembolso económico. La protección frente a esos ataques es complicada, ya que su eficacia no depende de payloads maliciosas. Pero algunos atacantes van todavía más allá y utilizan cuentas de proveedores legítimas pero comprometidas para lanzar sus ataques BEC.

La protección de su organización frente a los ataques BEC requiere una combinación de tecnología y formación. Necesita un enfoque más holístico para romper de verdad la cadena de ataque de compromiso del correo electrónico. Pero Proofpoint puede ayudarle.

Proofpoint es el primer y único proveedor en proporcionar una plataforma completa e integrada de protección frente a amenazas capaz de:

- Detectar y neutralizar las amenazas BEC antes de que lleguen a los buzones de correo.
- Formar a los usuarios para que detecten y denuncien las estafas BEC.
- Ofrecer visibilidad de los riesgos asociados a los proveedores y las cuentas de terceros comprometidas.
- Automatizar la detección y respuesta a amenazas.
- Proteger su marca cuando se producen estafas por correo electrónico.

Este resumen de la solución describe nuestro enfoque de manera más detallada.

1 *Internet Crime Report* (Informe sobre la ciberdelincuencia), FBI, 2022.

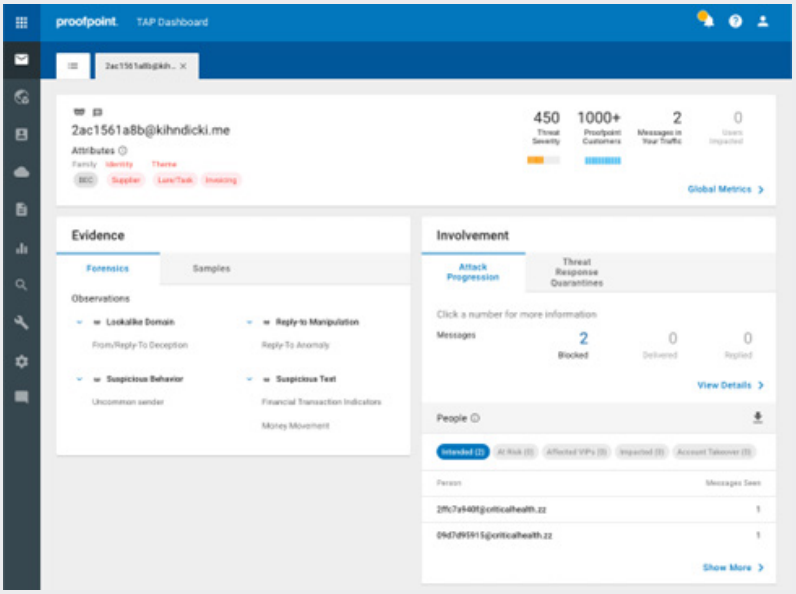

Figura 1: Proofpoint identifica los usuarios más atacados por los ataques BEC y proporciona visibilidad pormenorizada de las amenazas BEC, incluidos los temas y tácticas utilizadas.

Detecte y bloquee las amenazas de impostores antes de que se infiltren en su entorno

Nuestra plataforma integrada utiliza Advanced BEC Defense, que está impulsada por nuestro motor de detección basado en inteligencia artificial (IA), Supernova. Esta tecnología de vanguardia ha conseguido que se detecten 17 veces más amenazas, ampliando nuestra detección a una gran variedad de ataques de fraude por correo electrónico.

Advanced BEC Defense realiza análisis en profundidad de varios atributos de los mensajes, concretamente:

- Datos del encabezado del mensaje
- Dirección IP del remitente
- Relación entre el remitente y el destinatario
- Reputación del remitente

La solución utiliza el análisis semántico basado en grandes modelos de lenguaje para analizar los cuerpos de los mensajes en cuanto a lenguaje empleado y estilo, con el fin de determinar si un mensaje es una amenaza BEC. El motor de comportamiento basado en aprendizaje automático analiza la actividad para extraer indicios de comportamiento, o firmas de amenazas, con el fin de comprender patrones que luego utilizará para detectar anomalías en tiempo real.

Los elementos que analiza son los siguientes:

- Si el remitente está enviando un número anormal de mensajes de correo electrónico.
- Si los mensajes proceden de una dirección IP habitual.
- Si un remitente ha sido visto alguna vez por los usuarios de la empresa.

Estos indicios fortalecen la pila de detección y permiten nuevos casos de uso. Como resultado, el motor de detección detecta ahora otras amenazas avanzadas por correo electrónico, como el ransomware, el phishing de credenciales y las cuentas de terceros comprometidas.

Advanced BEC Defense detecta la falsificación del "display name" (nombre mostrado) el uso de "lookalike domains" (dominios parecidos). Incluso bloquea los fraudes de proveedores más sofisticados por medio del análisis dinámico de los mensajes, capaz de identificar las tácticas asociadas al fraude de facturas de proveedores. Utiliza aprendizaje automático para ajustarse y mejorar en tiempo real y su objetivo es reducir las tasas de falsos positivos.

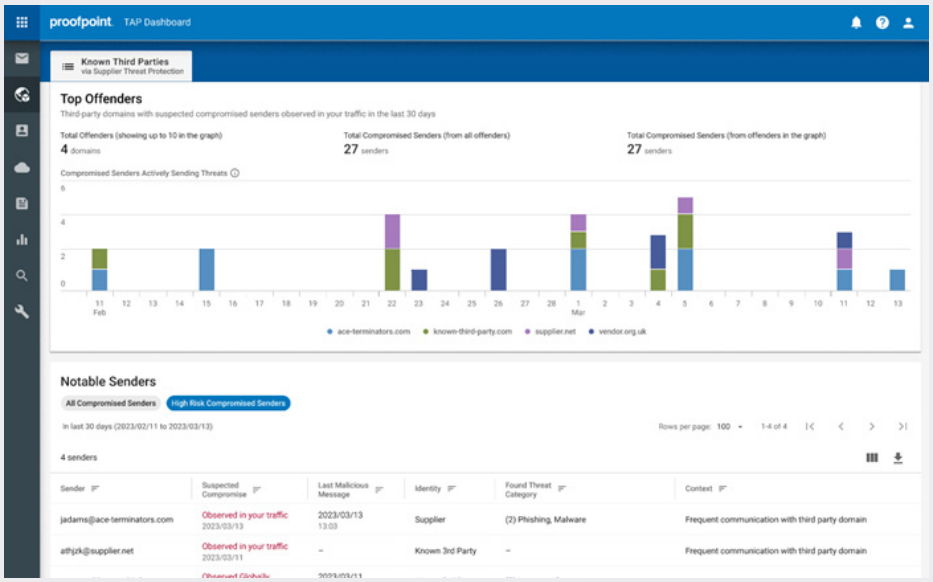

Figura 2: El add-on Supplier Threat Protection detecta las cuentas de terceros comprometidas con las que interactúa su organización.

Consiga visibilidad de los riesgos de ataques BEC

Para comprender, comunicar y reducir mejor los riesgos de ataques BEC, le ayudamos a responder a las siguientes preguntas que puede realizar su equipo directivo:

- ¿Cuáles son los riesgos de ataques BEC a los que nos exponemos?
- ¿Cuáles son los usuarios más atacados?
- ¿Cuáles de nuestros colaboradores externos de confianza tienen cuentas potencialmente comprometidas?
- ¿Cómo podemos cuantificar y mitigar los riesgos?

Proofpoint puede indicarle cuáles son sus usuarios más atacados y quiénes son más susceptibles de caer en las amenazas de impostores. Le ofrecemos una visibilidad pormenorizada de los detalles de las amenazas BEC, indicándole los temas a los que debe prestar atención, como las tarjetas regalo, la redirección de nóminas, el fraude de facturas de proveedores, etc. (véase la Figura 1). Entonces puede aplicar controles de seguridad adaptables a determinados usuarios y comunicar mejor los riesgos a su equipo directivo.

Proofpoint amplía su protección ofreciendo visibilidad e información sobre los proveedores de riesgo. Le ayudamos a gestionar los riesgos y amenazas asociadas a los proveedores gracia a que le permitimos:

- Identificar de manera proactiva las cuentas de proveedores que podrían haber sido suplantadas o comprometidas.
- Ofrecer una vista priorizada y centrada en los proveedores de las amenazas BEC.
- Identificar y prevenir amenazas de dominios de proveedores, así como lookalikes (dominios parecidos) maliciosos de esos dominios.

Evaluamos y priorizamos el nivel de riesgo de estos dominios de proveedores y le notificamos las cuentas potencialmente comprometidas. Esto permite a sus equipos de seguridad centrarse en los proveedores que suponen un mayor riesgo para su organización.

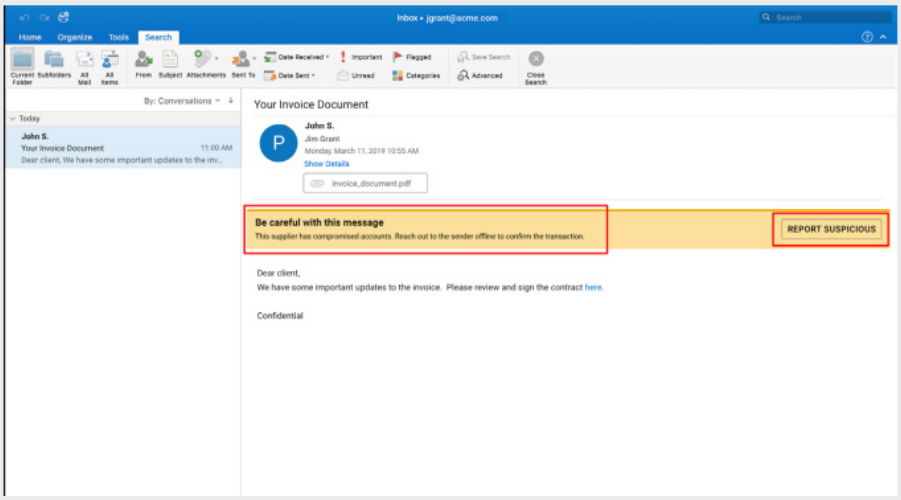

Figura 3: Las etiquetas de advertencia de correo electrónico alertan a los usuarios y les ayudan a tomar decisiones más informadas respecto a los mensajes sobre los que tienen dudas.

Mejore la resiliencia de los usuarios frente a los ataques BEC

Los ataques BEC se dirigen a personas, y su éxito depende de que lleven a cabo acciones maliciosas sin saberlo. Puesto que los ataques de impostores recurren a la ingeniería social y a la usurpación de la identidad, los usuarios constituyen a menudo su última línea de defensa. Por este motivo, la mitigación de los riesgos de ataques BEC requiere tanto tecnología como formación.

Gracias a nuestro botón de denuncias Proofpoint PhishAlarm, pone a disposición de los sus usuarios los conocimientos y herramientas adecuados para identificar e informar sobre correos electrónicos de impostores sospechosos. Nuestras etiquetas de advertencias de correo electrónico también alertan a los usuarios sobre el correo electrónico incierto para que puedan tomar decisiones más informadas. Puede formar a los usuarios sobre las últimas tácticas de ataque utilizadas en los ataques BEC recientes y asignar formación dirigida a sus usuarios más atacados. Esto les garantiza una mayor resiliencia frente a ataques BEC.

Automatice la respuesta a amenazas

Muchas organizaciones se enfrentan a la escasez de personal en sus departamentos de seguridad de TI. Detectar, investigar y mitigar las amenazas BEC en toda una organización es una tarea complicada. Llevamos la automatización a la primera línea de los procesos de detección y corrección de amenazas. Gracias a nuestra funcionalidad Threat Response Auto-Pull (TRAP), puede poner rápidamente en cuarentena o eliminar cualquier mensaje de correo electrónico sospechoso o no deseado con un solo clic. La automatización se extiende a los mensajes reenviados o recibidos por otros usuarios, así como a los mensajes recibidos por otros clientes de Proofpoint. Esto significa que todos se benefician de la inteligencia adicional.

Además, simplificamos la administración del buzón de correo malicioso. Los mensajes de correo electrónico denunciados por los usuarios se analizan automáticamente, y los que se consideran maliciosos pueden ponerse en cuarentena o corregirse. Esto le permite acelerar la respuesta a las amenazas y reducir el trabajo manual.

Proteja su marca cuando se producen estafas por correo electrónico

En el caso de la suplantación de la marca, los ciberdelincuentes engañan a sus clientes y a sus partners comerciales utilizando el nombre y la marca de su empresa para timarles. Protegemos su marca frente a compromisos cuando se producen estafas BEC impidiendo el envío de mensajes fraudulentos a través de sus dominios de confianza. Autenticamos todos los mensajes que entran y salen de su organización. Y, gracias a la simplificación de la implementación DMARC con un flujo de trabajo guiado y servicios gestionados, le ayudamos a prevenir eficazmente la suplantación de dominios y bloquear todos los intentos de enviar mensajes no autorizados a través de sus dominios de confianza.

Además, proporcionamos visibilidad de todos los mensajes de correo electrónico enviados a través de su dominio, incluidos los de remitentes externos de confianza. Identificamos los dominios parecidos al suyo. Detectamos dinámicamente nuevos dominios registrados que se hacen pasar por su marca en ataques por correo electrónico de phishing. Y nuestro servicio Virtual Takedown le permite tomar rápidamente las medidas oportunas.

Resumen

Las estafas por correo electrónico generan las mayores pérdidas económicas. El mayor nivel sofisticación de los estafadores se ha traducido en ataques BEC que incluyen ahora complejos fraudes de proveedores. Proofpoint es el primer y único proveedor que proporciona una solución global e integral para proteger de forma eficaz contra estas amenazas emergentes.

Nuestra solución contra ataques BEC:

- Detecta y bloquea tipos diferentes de ataques BEC.
- Proporciona visibilidad de la superficie de ataque humana y detalles pormenorizados de las amenazas BEC.
- Identifica los proveedores que presentan un riesgo y pueden tener cuentas comprometidas.
- Forma a sus usuarios para que sean más resilientes a las estafas BEC.
- Automatiza la investigación y respuesta a incidentes.
- Protege su marca cuando se producen estafas por correo electrónico.

Proofpoint le permite protegerse de forma más rápida, fácil y eficaz frente a los ataques BEC.

MÁS INFORMACIÓN

Para obtener más información, visite **www.proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.