proofpoint.

LIBRO ELECTRÓNICO

5 ataques reales y cómo neutralizarlos

Vol. 1: ataques de ingeniería social

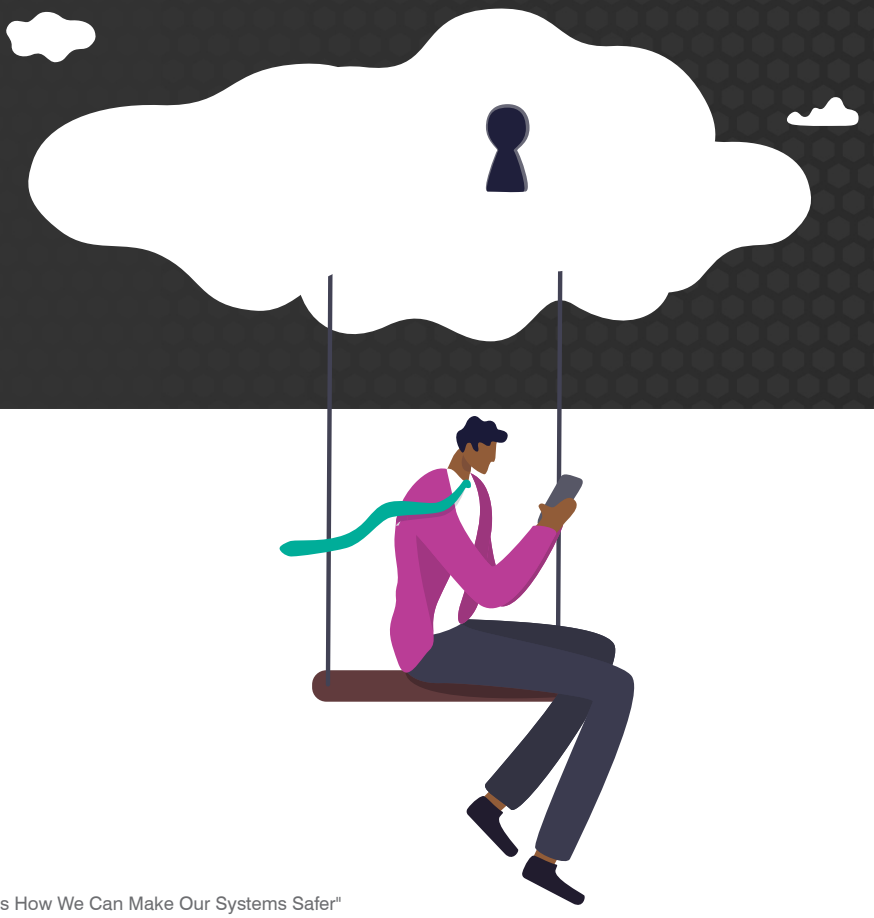
Introducción

Los ciberdelincuentes son ingeniosos y están muy motivados. ¿Por qué no iban a estarlo? Actúan en un sector de gran crecimiento en el que los riesgos son bajos y las recompensas tan grandes que se espera que la ciberdelincuencia cueste al mundo 23,8 billones de dólares al año en 2027[1].

Ante perspectivas tan lucrativas, la creatividad que muestran los ciberataques actuales parece infinita. Cada día surgen nuevas campañas de malware, ataques de phishing e ingeniosas tácticas de ingeniería social, mientras los equipos de seguridad juegan al gato y al ratón con los ciberdelincuentes para detenerlos. Aunque estas nuevas amenazas puedan parecer infinitamente variadas, tienen una serie de puntos en común: se distribuyen por correo electrónico y van dirigidas a las personas.

En esta serie de libros electrónicos, echamos un vistazo a algunos de los ataques por correo electrónico más insidiosos que circulan actualmente. Muchos de ellos han conseguido atravesar las defensas de varias herramientas de seguridad antes de ser detectados. Para ayudarle a entender por qué, analizaremos cada ataque paso a paso para mostrarle cómo se llevaron a cabo y cómo los ciberdelincuentes intentaron aprovechar las vulnerabilidades humanas. Y a continuación explicaremos cómo se neutralizaron.

Este volumen analiza los ataques mediante ingeniería social. En el volumen 2, se analizan ataques más técnicos.



1 Foro Económico Mundial. "2023 Was a Big Year for Cybercrime—Here's How We Can Make Our Systems Safer" (2023 fue un año excelente para los ciberdelincuentes: así podemos reforzar la seguridad de nuestros sistemas), enero de 2024.

Índice

SECCIÓN 1

Ataques BEC y a la cadena de suministro

En los ataques BEC, (Business Email Compromise), un ciberdelincuente se hace pasar por una persona o entidad en la que confía el destinatario, como un compañero, un proveedor o un partner. Muchos de los ataques BEC actuales son enormemente sofisticados, cuentan con una buena financiación y están cuidadosamente planificados y estudiados.

En los últimos años, estos ataques han sido una enorme fuente de beneficios para los ciberdelincuentes. Según el informe *Internet Crime Report 2023* del FBI, provocan a las empresas de EE. UU. unas pérdidas por valor de 17 000 millones de dólares. A nivel mundial, los ataques BEC han costado a las empresas la friolera de 50 000 millones de dólares[2]. En cambio, las víctimas del ransomware perdieron 1100 millones de dólares[3].

2 FBI. "Business Email Compromise: The $50 Billion Scam" (Business Email Compromise: el timo de los 50 000 millones de dólares), junio de 2023.

3 Wired. "Ransomware Payments Hit a Record $1.1 Billion in 2023" (Los pagos de ransomware alcanzan la cifra récord de 1100 millones de dólares en 2023), febrero de 2024.

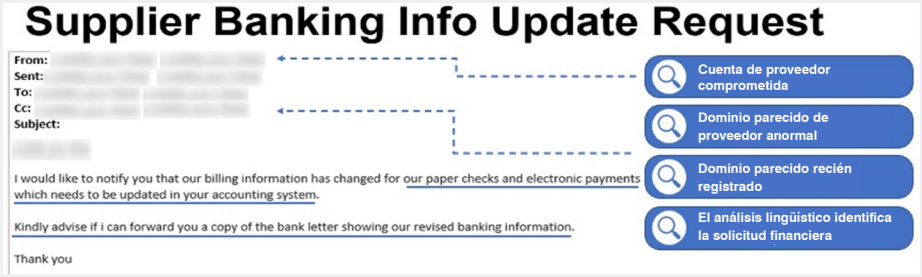
La situación

Proofpoint detectó este incidente BEC en un distribuidor mundial con más de 40 000 usuarios. La amenaza procedía de la cadena de suministro del grupo, y la herramienta de seguridad existente no la detectó. Este ejemplo es útil porque pone de relieve lo rápido que evoluciona el panorama de la ciberseguridad.

Desarrollo del ataque

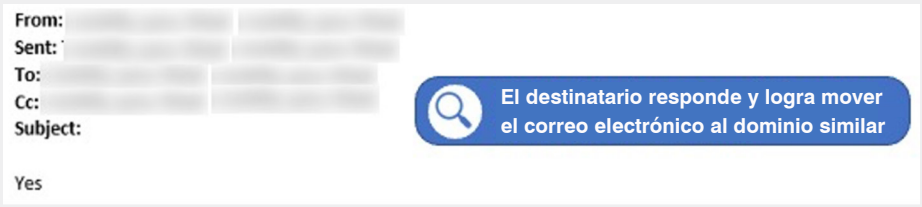
Veamos cómo se desarrolló el ataque:

1. **El mensaje engañoso.** El distribuidor mundial recibió un mensaje de correo electrónico de un remitente dentro de su cadena de suministro que solicitaba una actualización de su información de pago. Pero lo que parecía una solicitud rutinaria, era en cambio maliciosa, ya que la cuenta del remitente había sido comprometida.



Mensaje de correo electrónico inicial de un atacante, con observaciones del equipo de investigación forense de Proofpoint.

2. **El dominio similar malicioso.** El atacante intentaba redirigir los mensajes de correo electrónico de respuesta a un dominio similar recién registrado. Su objetivo era interceptar datos sensibles y desviar fondos.



La respuesta del cliente, que se envió a un lookalike domain (dominio similar).

Por qué estas amenazas son difíciles de detectar

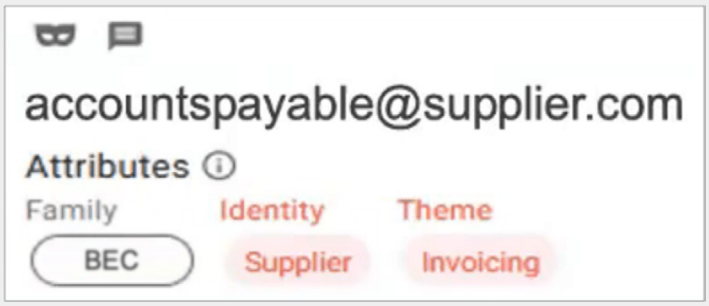
Los ataques BEC son muy difíciles de detectar porque no incluyen las habituales payloads (URL o adjuntos de correo maliciosos) que permitan su análisis. En lugar de eso, los ciberdelincuente recurren a la suplantación de la identidad u otras técnicas de ingeniería social para engañar a las personas.

La herramienta de seguridad del distribuidor no detectó la amenaza por diversas razones. Para empezar, daba demasiada importancia a la antigüedad del dominio como factor de detección. Además, no fue capaz de identificar los dominios similares. Y por último, no analizó la dirección de respuesta, lo que le habría permitido detectar la redirección a un nuevo dominio.

Cómo detectó Proofpoint el ataque

Para identificar muchas amenazas, como los ataques BEC y el phishing de credenciales, es fundamental combinar la antigüedad del dominio con otros indicadores de intención maliciosa. Esa es la razón por la que Proofpoint utiliza un enfoque multicapa. Nuestro motor de comportamiento utiliza inteligencia artificial (IA), aprendizaje automático y análisis del comportamiento para identificar los principales indicadores de compromiso. En concreto, identifica patrones de correo electrónico sospechosos.

En este ejemplo, Proofpoint identificó términos que indicaban que el mensaje contenía una solicitud de naturaleza financiera. Aunque la solicitud no parecía inusual por sí sola, cuando se combinaba con el cambio de la dirección de respuesta, resultaba sospechosa. Además, el dominio se registró el mismo día en que se envió el correo electrónico.



El panel de Proofpoint Targeted Attack Protection (TAP) clasifica cada amenaza. En este ejemplo, muestra que identificamos la amenaza como un ataque BEC, que procedía de un proveedor y que estaba relacionada con la facturación.

SECCIÓN 2

Phishing de firma electrónica

El phishing de firma electrónica es una amenaza que incita al destinatario a divulgar sus credenciales u otra información personal mediante un mensaje que solicita su firma. El mensaje puede incluir un archivo adjunto con un contrato o una factura que hay que firmar.

En 2023, en un solo mes, Proofpoint detectó más de 75 000 amenazas diferentes como esta.

La situación

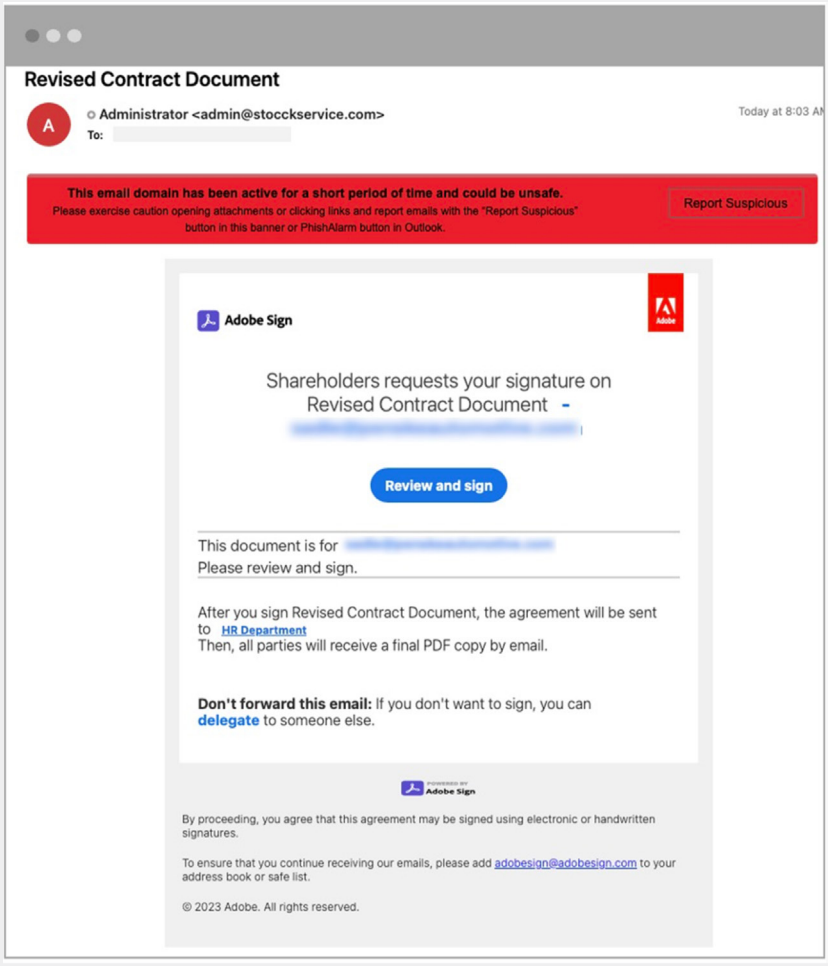
Proofpoint detectó una amenaza de recopilación de credenciales alojada en la aplicación SaaS Amazon Web Services (AWS) Amplify. Nuestro cliente, una empresa automovilística con 2000 empleados, utilizaba la aplicación.

Un ciberdelincuente había creado un señuelo de phishing que parecía un enlace a un documento sensible, concretamente un contrato actualizado que había que ver y refrendar. El objetivo era un empleado que trabajaba con contratos y tenía otras responsabilidades fiduciarias, que a menudo se comunica con miembros del consejo de administración, clientes y proveedores en el desempeño de su trabajo. Por ello, no era raro que recibiera este tipo de solicitudes.

Desarrollo del ataque

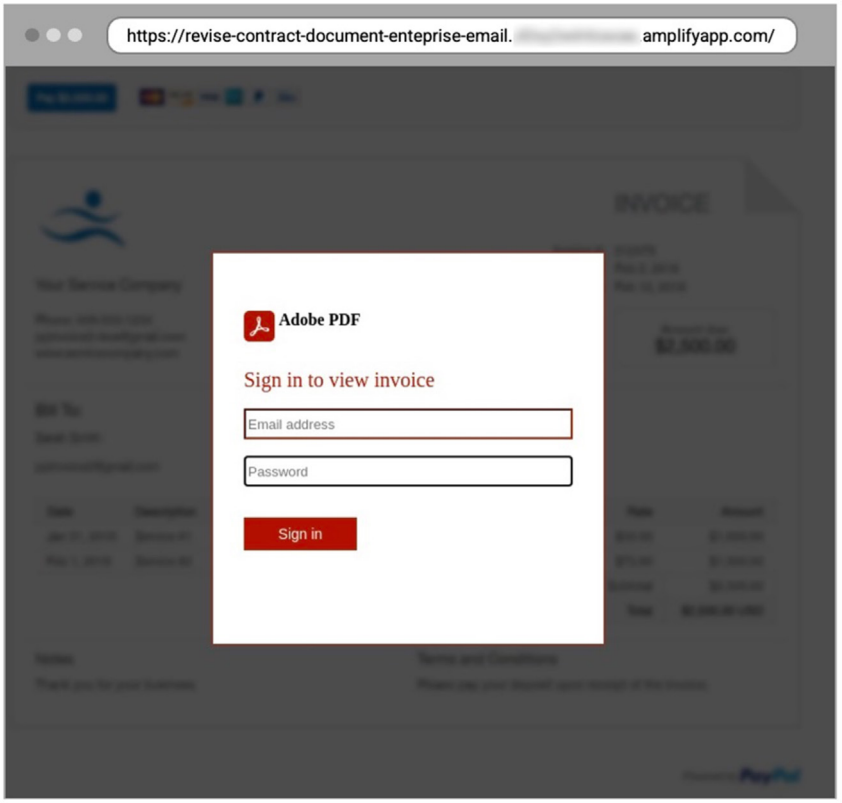
Veamos cómo se desarrolló el ataque:

1. **El mensaje engañoso.** Nuestro cliente recibió un mensaje de correo electrónico invitando al empleado a ver y firmar un contrato actualizado.



El mensaje malicioso.

2. **La URL maliciosa.** Si el empleado hubiera hecho clic en la URL maliciosa, habría visto una pantalla de inicio de sesión diseñada para parecerse a otras pantallas de inicio de sesión legítimas. El objetivo del ciberdelincuente era incitar al empleado a divulgar sus credenciales.



Página de inicio de sesión falsa alojada en amplifyapp.com.

Por qué estas amenazas son difíciles de detectar

Aplicaciones como AWS Amplify y otros servicios SaaS como DocuSign, Adobe Sign y OpenSpan Sign suelen utilizarse en estos ataques. Ofrecen a los ciberdelincuentes una forma sencilla de distribuir contenidos maliciosos que parecen legítimos.

En este caso, el dominio de la URL tenía más de cinco años. La dirección IP pertenecía a Amazon, lo que probablemente daría lugar a un veredicto de legitimidad. La mayoría de las soluciones de protección del correo electrónico son capaces de detectar un ataque de phishing de credenciales estándar. Sin embargo, el dominio de confianza del proveedor SaaS complica la tarea para la mayoría de los motores de detección. Concretamente, 19 proveedores de soluciones de protección del correo electrónico, muchos de los cuales afirman utilizar tecnologías de inteligencia artificial y aprendizaje automático avanzadas para bloquear estos ataques, no interceptaron esta amenaza.

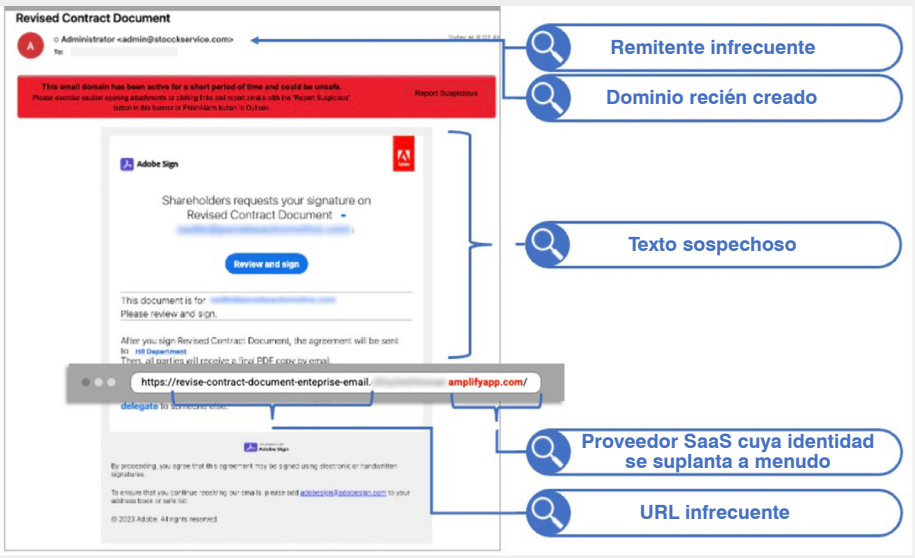
Cómo detectó Proofpoint el ataque

El motor de IA basada en el comportamiento de Proofpoint utiliza indicios a nivel de mensajes para detectar y bloquear una amplia variedad de amenazas. Esto significa que podemos detectar amenazas de phishing desconocidas hasta ahora en una fase más temprana de la cadena de ataque y bloquearlas antes de que se distribuyan.

Proofpoint realizó una análisis multicapa en profundidad del perfil del usuario e identificó una combinación remitente/destinatario basada en patrones de comunicación anteriores. Descubrimos que el remitente rara vez se comunicaba con el destinatario o con cualquier otro empleado de la empresa automovilística.

Gracias a la IA basada en el comportamiento y al aprendizaje automático, Proofpoint llevó a cabo un análisis en profundidad de la URL, con objeto de evaluar la pertinencia de la URL en función de puntos de datos históricos y de otra actividad anómala. Tras examinar el comportamiento de envío de toda la empresa, se estableció que la URL nunca había sido utilizada por el destinatario ni por ningún otro empleado de la empresa.

Proofpoint detectó además el uso de un dominio de proveedor SaaS legítimo y conocido. En otras empresas a las que proporcionamos protección, hemos observado que los ciberdelincuentes explotan este mismo dominio para distribuir contenido malicioso.



Resumen de las observaciones de Proofpoint en relación con el mensaje de correo electrónico de firma electrónica que dio lugar a su alerta.

SECCIÓN 3

Amenazas TOAD

Las tácticas de ingeniería social siguen evolucionando a medida que los ciberdelincuentes buscan formas nuevas y creativas de obtener acceso inicial a sistemas sensibles. Los ataques por teléfono (TOAD) son prueba de ello. Los atacantes envían mensajes de correo electrónico a los destinatarios e intentan persuadirles para que llamen a un falso centro de llamadas.

En general, los usuarios no están protegidos contra las llamadas telefónicas maliciosas. Por eso es tan importante bloquear estos mensajes de correo electrónico. Estos ataques son muy difíciles de detectar, ya que a menudo no contienen URL ni archivos adjuntos.

En 2023, en un solo mes, Proofpoint detectó más de 19 000 amenazas TOAD que habían pasado desapercibidas a 14 herramientas de protección del correo electrónico distintas.

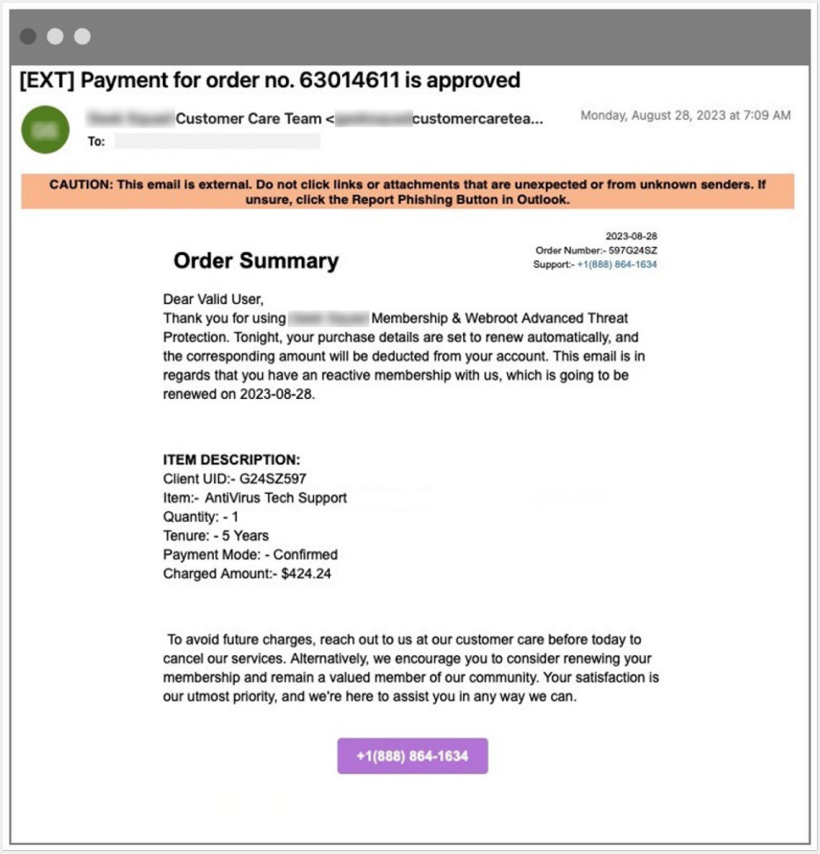
La situación

Proofpoint detectó una amenaza TOAD en una empresa de fabricación con más de 45 000 empleados. Un ciberdelincuente que decía trabajar para una conocida empresa de software antivirus envió un mensaje fraudulento a uno de sus empleados. En lugar de añadir URL o archivos adjuntos a su mensaje, el ciberdelincuente incluyó un número de teléfono.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

1. **El mensaje engañoso.** Un mensaje de correo electrónico pretendía confirmar una próxima compra de una conocida empresa tecnológica.



[EXT] Payment for order no. 63014611 is approved

[redacted] Customer Care Team <[redacted]customercaretea... Monday, August 28, 2023 at 7:09 AM

To: [redacted]

CAUTION: This email is external. Do not click links or attachments that are unexpected or from unknown senders. If unsure, click the Report Phishing Button in Outlook.

Order Summary

2023-08-28
Order Number:- 597G24SZ
Support:- +1(888) 864-1634

Dear Valid User,
Thank you for using [redacted] Membership & Webroot Advanced Threat Protection. Tonight, your purchase details are set to renew automatically, and the corresponding amount will be deducted from your account. This email is in regards that you have an reactive membership with us, which is going to be renewed on 2023-08-28.

ITEM DESCRIPTION:
Client UID:- G24SZ597
Item:- AntiVirus Tech Support
Quantity: - 1
Tenure: - 5 Years
Payment Mode: - Confirmed
Charged Amount:- $424.24

To avoid future charges, reach out to us at our customer care before today to cancel our services. Alternatively, we encourage you to consider renewing your membership and remain a valued member of our community. Your satisfaction is our utmost priority, and we're here to assist you in any way we can.

+1(888) 864-1634

Mensaje de correo electrónico malicioso inicial enviado a la bandeja de entrada del destinatario.

2. **Secuencia de ataque TOAD.** Si el empleado hubiera llamado a este número, el ciberdelincuente podría haberle animado a hacer clic en una URL maliciosa en su ordenador, para desencadenar una serie de ataques, como el acceso remoto, el robo de datos confidenciales o la infección por ransomware.

Esquema general de la secuencia de ataque TOAD típico.

Por qué estas amenazas son difíciles de detectar

Las amenazas TOAD pueden ser difíciles de detectar, ya que rara vez contienen payloads maliciosas. Es más, los ciberdelincuentes suelen utilizar dominios conocidos pertenecientes a Google, a Microsoft o a otros servicios de correo electrónico legítimos.

Como esta amenaza TOAD se envió desde un dominio propiedad de Google, el mensaje superó autenticaciones de correo electrónico como SPF (Sender Policy Framework) y DMARC. El mensaje tampoco contenía ninguna paylaod maliciosa, lo que podría explicar por qué la herramienta de seguridad de la empresa fabricante no interceptó la amenaza.

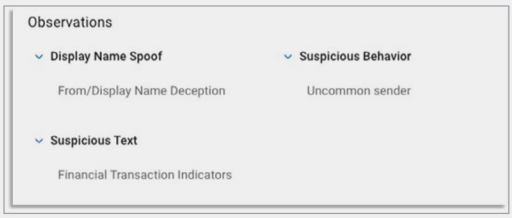
Cómo detectó Proofpoint el ataque

Proofpoint utiliza tecnologías de inteligencia artificial y aprendizaje automático avanzadas para analizar y combinar los distintos indicadores de comportamiento para detectar amenazas TOAD. Este enfoque es más fiable que el simple seguimiento y mantenimiento de una base de datos de números de teléfono maliciosos previamente identificados durante los ataques TOAD.

Cuando el motor de IA basada en el comportamiento de Proofpoint analizó este mensaje, identificó términos relativos a una transacción financiera y a la necesidad de actuar de manera urgente, dos indicadores de un mensaje potencialmente malicioso. Además, las amenazas TOAD incluyen siempre un número de teléfono e instan al destinatario a llamar rápidamente. Esa es la razón por la que Proofpoint analiza los mensajes para detectar números de teléfono.

Realizamos un análisis multicapa, que también determinó que el destinatario nunca había recibido un correo electrónico de este remitente, basándonos en patrones de comunicación anteriores. De hecho, ninguno de los empleados de la empresa había recibido nunca un correo electrónico de este remitente.

Durante los ataques TOAD, los ciberdelincuentes suelen enviar mensajes que parecen proceder de una marca legítima en un intento de establecer una relación implícita de confianza. Nuestro análisis también detectó esta táctica.



Resumen de las observaciones de Proofpoint que dieron lugar al veredicto.

SECCIÓN 4

Redirección de pagos

La redirección de pagos es una forma de ataque BEC. Los principales objetivos de estos ataques son el personal que tramita las solicitudes relacionadas con las nóminas. En general, un ciberdelincuente se hace pasar por un empleado que necesita actualizar la información de la cuenta en la que se abona su salario. La nueva información corresponde en realidad a una cuenta perteneciente al ciberdelincuente. Una vez realizado el cambio, los fondos perdidos no podrán ser recuperados por la empresa.

La redirección de pagos no es una forma nueva de ataque BEC, pero su frecuencia es cada vez mayor. Proofpoint sigue observando cómo este tipo de amenaza atraviesa las defensas de otras herramientas de protección del correo electrónico. En nuestras recientes evaluaciones de amenazas, descubrimos que más de 400 de estos ataques habían pasado desapercibidos para otras 12 herramientas de protección del correo electrónico.

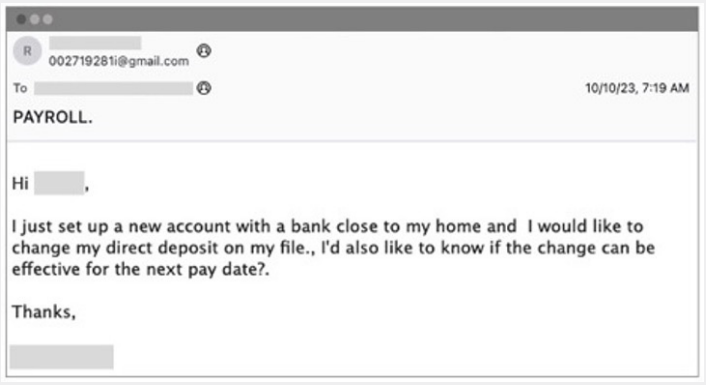
La situación

Proofpoint detectó una de estas amenazas en una empresa del sector de la energía y los servicios públicos con 300 empleados. En este caso, un ciberdelincuente se hizo pasar por un empleado normal y envió un correo electrónico al director de recursos humanos (RR. HH.) de la empresa. No solo la herramienta de protección del correo electrónico de la empresa distribuyó el mensaje, sino que su herramienta de corrección posterior a la entrega basada en la API tampoco lo detectó ni eliminó.

Desarrollo del ataque

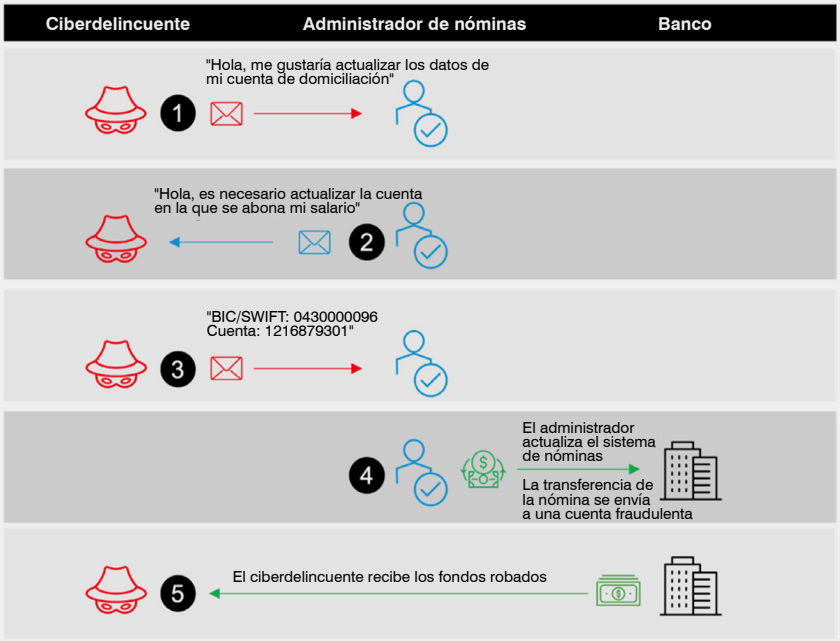
Veamos cómo se desarrolló el ataque:

1. **El mensaje engañoso.** El ciberdelincuente envió una solicitud al departamento de RR. HH. en la que pedía la actualización de la cuenta de domiciliación de "su" sueldo. Este mensaje fue enviado desde una cuenta que se parecía a la cuenta de correo electrónico personal de un empleado legítimo.



Mensaje de correo electrónico malicioso original enviado a la bandeja de entrada del destinatario.

2. **Secuencia de ataque de redirección de nóminas.** Si el destinatario hubiera respondido al mensaje, el objetivo del ciberdelincuente habría sido persuadirle para que transfiriera fondos a otra cuenta bancaria que no pertenecía al empleado víctima de la suplantación de identidad.



Secuencia de ataque típica de un ataque de redirección de pagos.

Por qué estas amenazas son difíciles de detectar

Estas amenazas no suelen utilizar payloads maliciosas, como adjuntos o URL. También suelen enviarse desde servicios de mensajería personal como Google, Yahoo e iCloud, y se dirigen contra usuarios específicos.

Además, las herramientas de protección del correo electrónico basadas en API que buscan amenazas después de la entrega son las que tienen más probabilidades de pasar por alto este tipo de amenazas. Esto explica en parte su funcionamiento. Para que estas herramientas sean eficaces, los equipos de TI y de seguridad tienen que rellenarlas manualmente con un diccionario de los posibles nombres mostrados (display names) de todos los empleados, una tarea que requiere mucho tiempo y que es difícil de aplicar a gran escala.

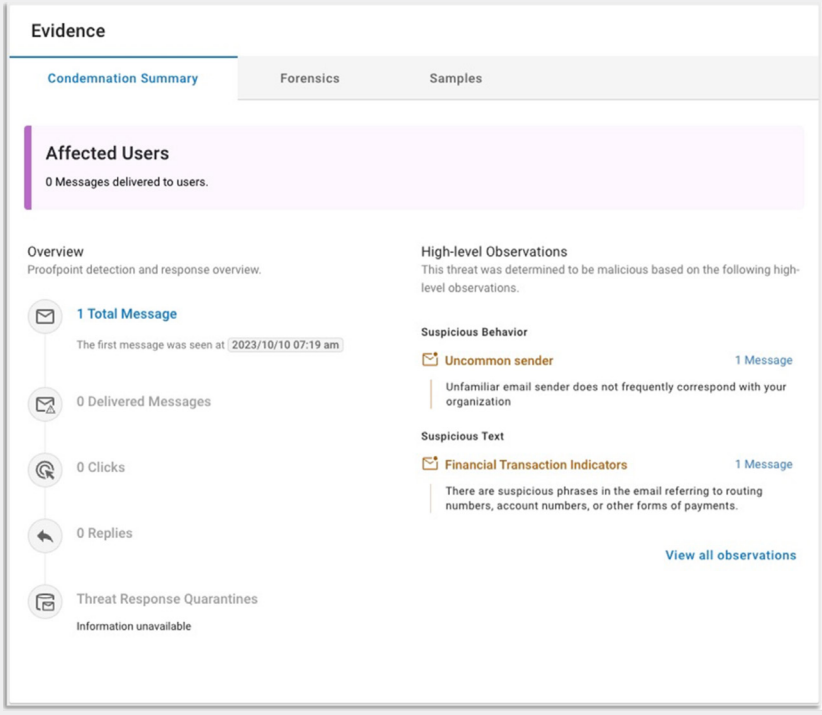
Para evitarlo, muchas empresas optan por activar la prevención de la suplantación de nombres mostrados sólo para sus altos ejecutivos. Sin embargo, los ciberdelincuentes que están detrás de la redirección de pagos no se limitan a hacerse pasar por altos ejecutivos, sino que su objetivo es cualquier empleado con acceso a los fondos de la empresa. En nuestro ejemplo anterior, un ciberdelincuente se aprovechó precisamente de esa debilidad.

Cómo detectó Proofpoint el ataque

Para comprender el verdadero propósito de un mensaje de correo electrónico, una herramienta de protección del correo electrónico necesita interpretar el tono y la intención del mensaje. Para ello, Proofpoint utiliza varias señales de detección, motores de análisis e IA basada en el comportamiento. Nuestros motores de detección optimizados con IA y aprendizaje automático se entrenan continuamente con millones de mensajes de correo electrónico diarios procedentes de nuestro ecosistema global de inteligencia de amenazas.

Una de las señales que utilizamos para detectar mensajes de correo electrónico maliciosos es el análisis de las comunicaciones entre un remitente y un destinatario, y la frecuencia de sus mensajes. En el ejemplo anterior, era extraño que el director de RR. HH. recibiera correos electrónicos de este empleado concreto desde su dirección personal.

La mayoría de las herramientas de protección del correo electrónico utilizan indicios diseñados para identificar remitentes inusuales. Por lo tanto, generan un elevado número de falsos positivos. Nuestra estrategia es diferente. Combinamos varios indicios para no depender demasiado de uno o dos. Combinando el indicio empleado para identificar remitentes inusuales con un análisis del lenguaje utilizado el cuerpo del mensaje, Proofpoint extrae el tono y la intención de un mensaje.



Resumen de la amenaza neutralizada por Proofpoint que destaca los indicios que nos llevaron a condenar esta amenaza.

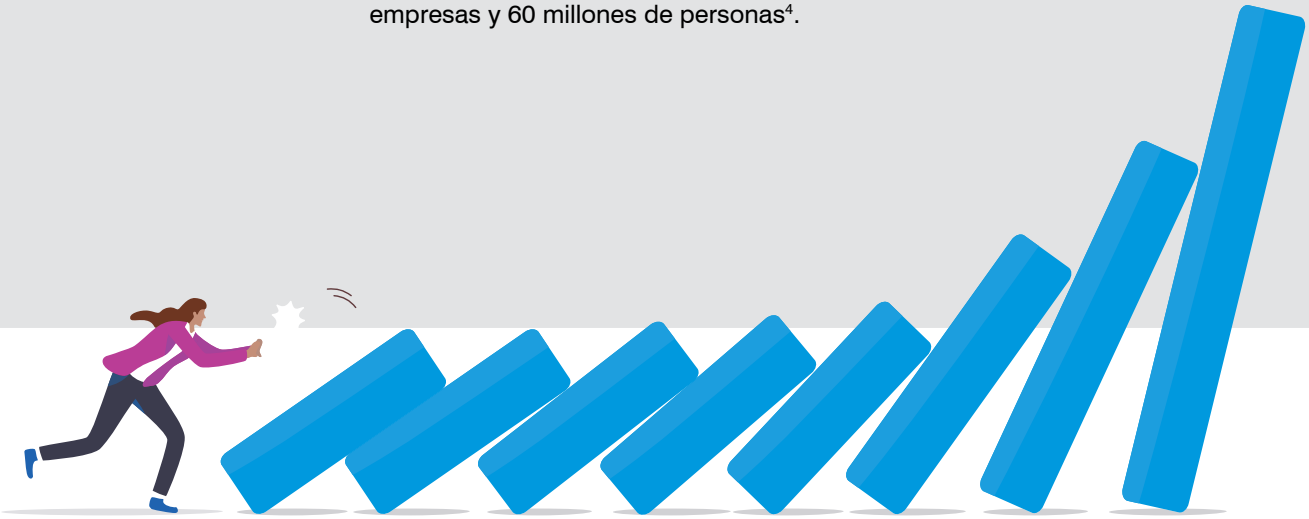
SECCIÓN 5

Compromiso de la cadena de suministro

Los compromisos de la cadena de suministro son otra forma de ataque BEC en alza. En estos ataques, un ciberdelincuente ataca a una empresa comprometiendo la seguridad de sus proveedores y otros terceros de su cadena de suministro. Los atacantes saben que las empresas con cadenas de suministro maduras suelen tener ciberdefensas más sólidas, lo que las convierte en objetivos difíciles.

Así, en lugar de lanzar un ataque directo, el ciberdelincuente se infiltra en una de las entidades de confianza de la empresa y se hace pasar por ella. El secuestro de hilos, o secuestro de conversaciones, es una técnica muy utilizada, en la que los ciberdelincuentes atacan cuentas de correo electrónico específicas y las comprometen para espiar las conversaciones. Llegado el momento, los ciberdelincuentes se meten en la conversación. A veces incluso se atreven a iniciar una nueva conversación.

Estos ataques son cada día más populares y sofisticados. El compromiso de la cadena de suministro más importante ocurrido en 2023 costó a las empresas afectadas más de 9900 millones de dólares. Se vieron afectadas más de mil empresas y 60 millones de personas[4].



4 TechCrunch. "MOVEit, the Biggest Hack of the Year, by the Numbers" (MOVEit, el mayor pirateo del año, en cifras), agosto de 2023.

La situación

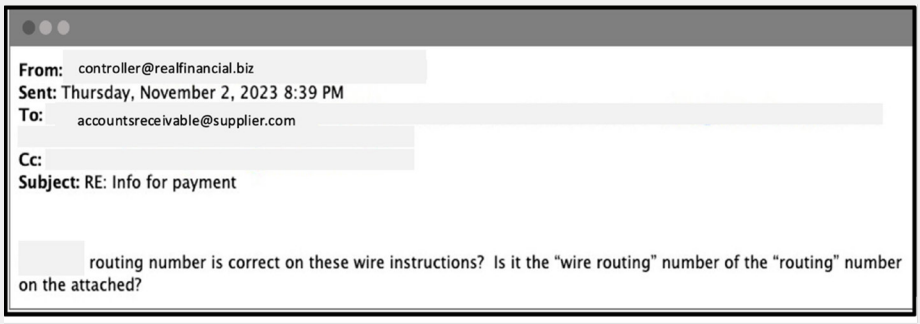
Proofpoint detectó un mensaje fraudulento que parecía haber sido enviado por un empleado del departamento de cuentas a cobrar de una pequeña empresa de servicios financieros con sede en Florida. Sin embargo, en realidad se trataba de un ciberdelincuente que se hacía pasar por otra persona. Su objetivo era lanzar un ataque a la cadena de suministro contra un importante bufete de abogados de Boston.

En un correo electrónico enviado al interventor del bufete, el ciberdelincuente solicitaba que los pagos se efectuaran a una cuenta nueva.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

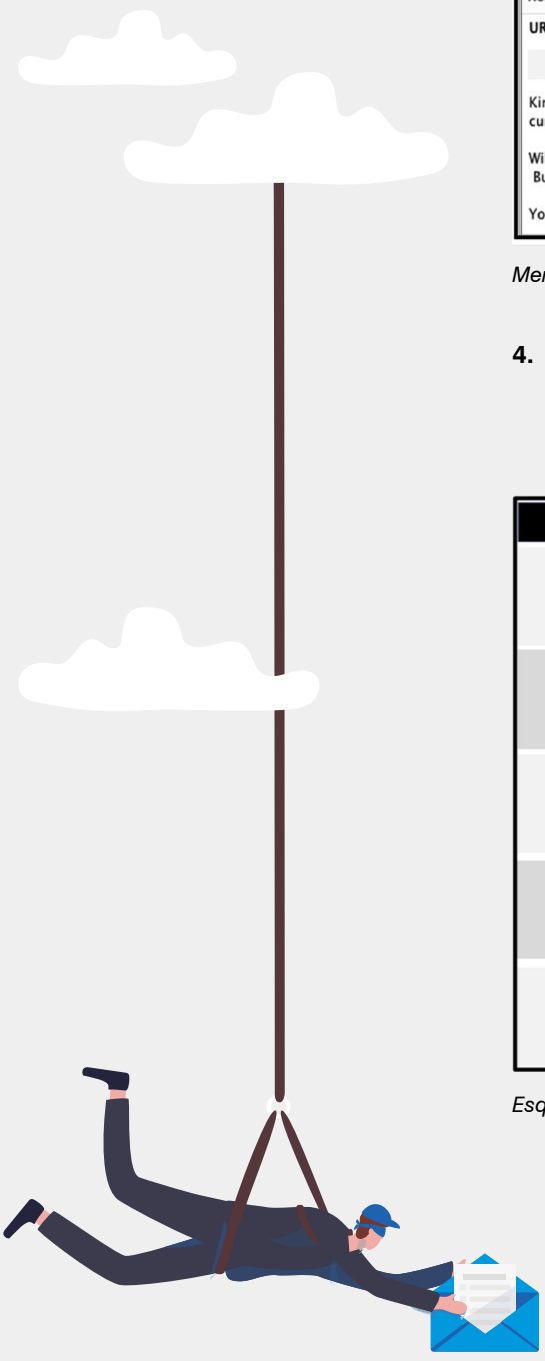
1. **Mensaje legítimo del cliente.** El cliente envió un mensaje de correo electrónico al proveedor para confirmar la exactitud de los datos bancarios para los pagos.



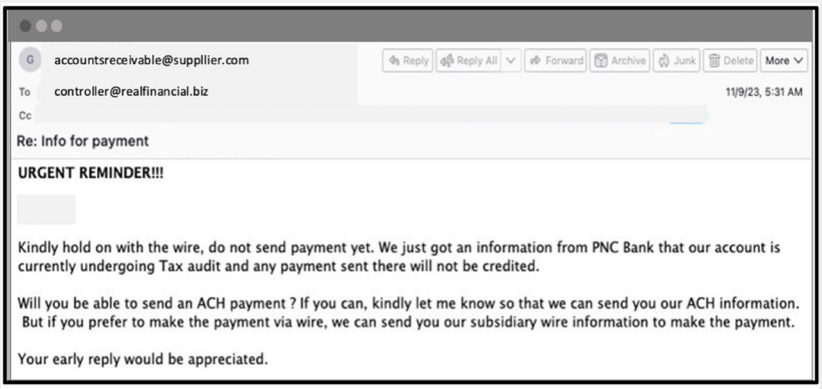
Mensaje legítimo del cliente confirmando los datos bancarios para los pagos.

2. **Mensaje legítimo del proveedor.** El proveedor respondió a la solicitud de confirmación de los datos bancarios para los pagos.

Mensaje legítimo del proveedor en respuesta a la solicitud de confirmación de los datos bancarios para los pagos.

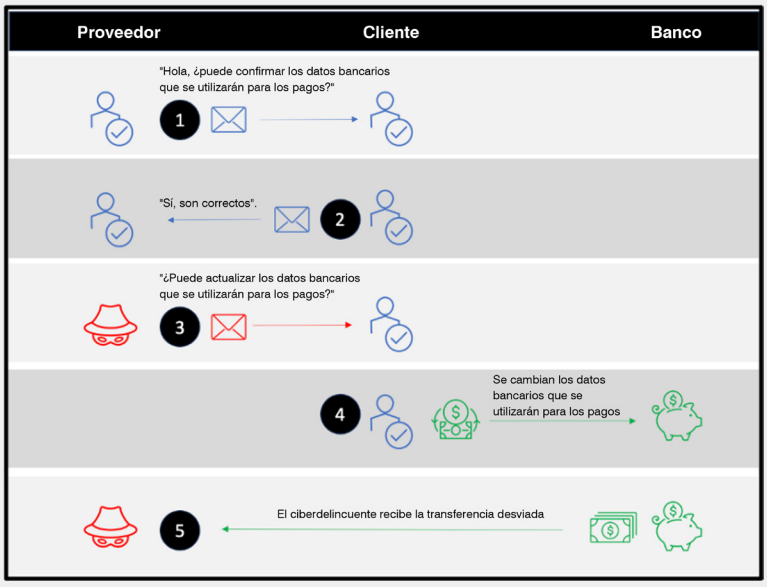


3. **Mensaje fraudulento del ciberdelincuente.** El ciberdelincuente entró en acción enviando un correo electrónico al cliente desde otra cuenta que parecía exactamente igual a la del proveedor. La realidad es que este correo electrónico fue enviado desde un dominio parecido (lookalike domain), que incluía una letra de más en la dirección del remitente. Para dar apariencia de legitimidad a su mensaje, el ciberdelincuente copió y pegó toda la conversación debajo del cuerpo del mensaje.



Mensaje fraudulento del ciberdelincuente.

4. **Secuencia de ataque de compromiso de la cadena de suministro.** El ciberdelincuente pidió que los pagos se efectuaran a otra cuenta a través de una cámara de compensación automatizada. El ciberdelincuente era el titular de esa nueva cuenta.



Esquema general de la secuencia de ataque.

Por qué estas amenazas son difíciles de detectar

Los ataques de compromiso de la cadena de suministro rara vez incluyen payloads maliciosas. Esta es una de las razones por las que son difíciles de detectar y neutralizar. El ciberdelincuente utiliza la ingeniería social para convencer al destinatario de que le ayude a lograr su objetivo.

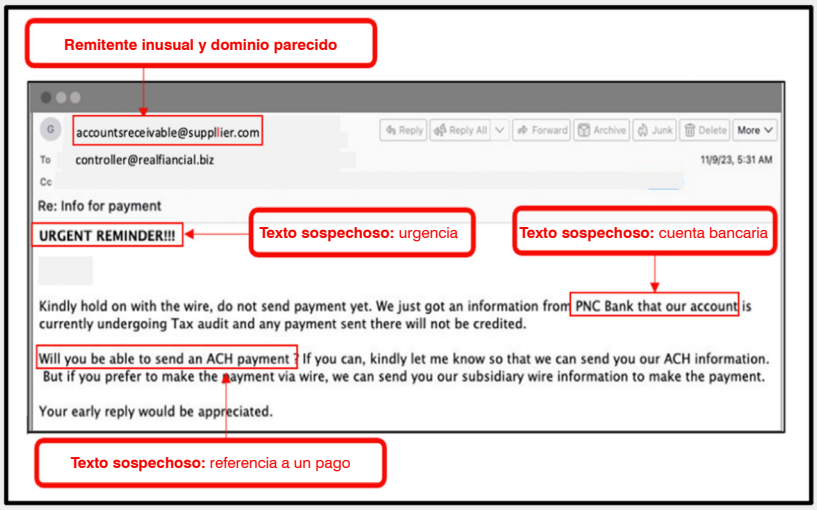
En este escenario, un proveedor pidió a un prestador de servicios que cambiara los datos bancarios que se utilizarían para los pagos. Una solicitud de este tipo no es inusual. Por eso, las herramientas de protección del correo electrónico basadas en API tienen dificultades para detectar estos ataques. Las herramientas basadas en API se basan en indicios para identificar a los remitentes inusuales, por lo que generan un elevado número de falsos positivos y alertas. Este enfoque limitado que utiliza IA basada en el comportamiento ayuda a entender por qué muchas empresas se quejan de la gran cantidad de información estéril que generan estos indicios.

Para detectar este tipo de mensajes maliciosos, una herramienta de protección del correo electrónico necesita interpretar el tono contextual y la intención de un mensaje. Ésta es la única forma de determinar el verdadero propósito de un mensaje antes de que llegue a la bandeja de entrada de un usuario.

Cómo detectó Proofpoint el ataque

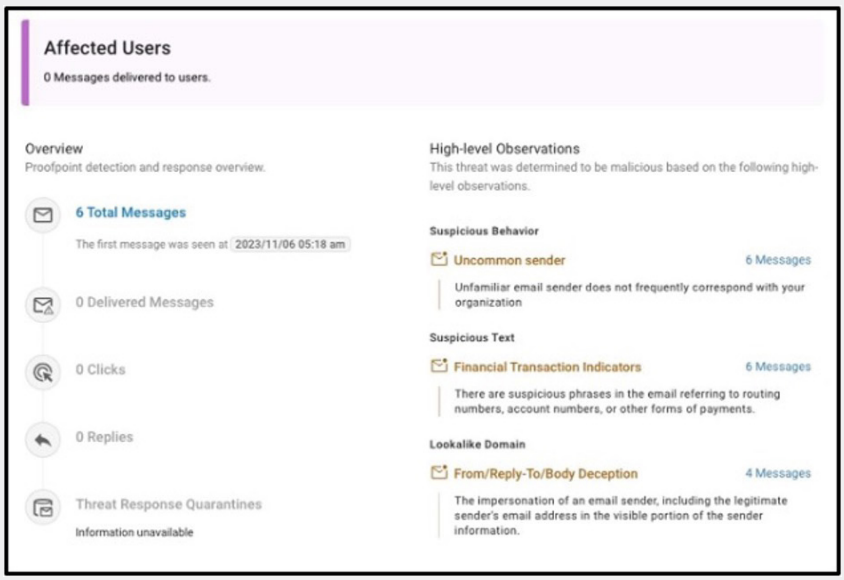
Proofpoint combina la inteligencia sobre amenazas con la IA basada en el comportamiento y el aprendizaje automático para determinar si los mensajes de correo electrónico son legítimos o maliciosos. Entrenamos constantemente nuestros motores de detección con millones de correos electrónicos al día procedentes de nuestro ecosistema global de inteligencia de amenazas. Esto nos permite detectar y bloquear este tipo de mensajes con un mayor nivel de confianza.

Para reducir la información espuria, combinamos varios indicios en lugar de basarnos en uno o dos, que pueden generar un elevado número de falsos positivos. Estos indicios incluyen el análisis de las comunicaciones entre remitentes y destinatarios y la frecuencia de estos mensajes. También analizamos el lenguaje utilizado en el cuerpo del mensaje para extraer el tono e interpretar la intención, y buscamos dominios parecidos y urgencia de pagos.



Varios indicios de detección identificados en un mensaje de correo electrónico de un proveedor fraudulento.

Analizando el contenido y la intención del correo electrónico y el lenguaje utilizado, Proofpoint determinó que el mensaje de nuestro ejemplo era una solicitud financiera fraudulenta. Esta campaña consistía en unos pocos mensajes en los que se suplantaba la identidad de una persona y se dirigía a un solo cliente. Ningún otro cliente de Proofpoint había sido víctima de este ataque antes.

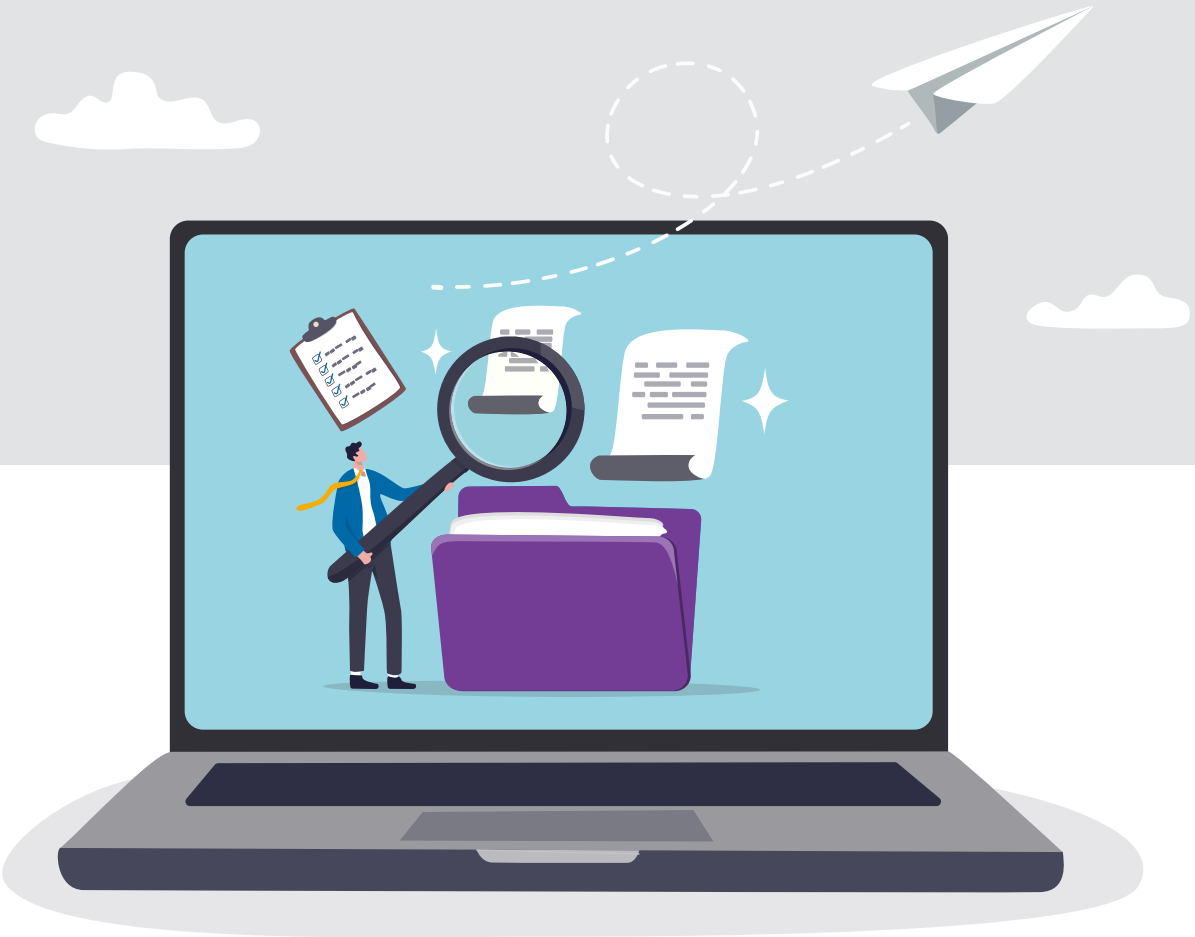


Resumen de la amenaza neutralizada que muestra los indicios que llevaron a Proofpoint a bloquear esta amenaza.

SECCIÓN 6

Conclusión

Todas estas estafas solo sirven para poner de relieve la necesidad crítica de contar con medidas de ciberseguridad sólidas y multicapa.



Para ir un paso por delante del siempre cambiante panorama de las amenazas, necesita adoptar un enfoque integral para proteger a sus empleados de las amenazas a las que se enfrentan:

- **Detecte las amenazas antes de la entrega.** La única forma de proteger a usuarios es bloquear los mensajes maliciosos antes de que se entreguen. Un estudio de Proofpoint revela que 1 de cada 7 usuarios hizo clic en un mensaje de correo electrónico en menos de un minuto. Busque una herramienta que combine algoritmos de aprendizaje automático e inteligencia avanzada de amenazas para identificarlas y bloquearlas.
- **Eduque a sus usuarios.** Sus empleados, contratistas y partners constituyen su primera línea de defensa. Asegúrese de que reciben formación para concienciar en materia de seguridad para todo tipo de ataques. Recuérdeles que denuncien rápidamente todo comportamiento inusual.
- **Lleve a cabo auditorías de seguridad regulares.** Las auditorías pueden ayudarle a identificar posibles vulnerabilidades en su entorno. Al hacerlo, asegúrese de buscar irregularidades en sus configuraciones y registros de acceso.
- **Configure su sistema para detectar errores de configuración.** Además de comprobar si hay errores de configuración, no olvide activar la corrección automática. Esto le permitirá detectar cambios no autorizados y corregirlos rápidamente, evitando que los ciberdelincuentes se establezcan de forma duradera en su empresa.
- **Elabore un plan de respuesta a incidentes.** Identifique varios escenarios de ataque. A continuación, determina cómo investigará y corregirá los incidentes. Asegúrese de comprobar la eficacia real de su plan realizando ejercicios de simulación con regularidad.

Pasos siguientes

Ahora más que nunca, es importante proteger a su organización de las crecientes amenazas por correo electrónico. Debe adoptar un enfoque proactivo para proteger su empresa, empleados y clientes de ataques avanzados como el ransomware, las estafas BEC y el phishing de credenciales.

La evaluación rápida de riesgos del correo electrónico de Proofpoint le proporciona una visibilidad y una perspectiva completas de la vulnerabilidad a ataques. Le ayuda a identificar a las personas objetivo de amenazas por correo electrónico dentro de su empresa.

No espere a que sea demasiado tarde para poner a prueba la seguridad de su correo electrónico. Póngase en contacto con Proofpoint para programar una **evaluación gratuita de riesgos asociados al correo electrónico**.

MÁS INFORMACIÓN

Para obtener más información, visite **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 85 % 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**.

proofpoint.

0503-006-06-01 07/24