proofpoint.

LIBRO ELECTRÓNICO

Manual sobre las estafas Business Email Compromise (BEC)

Plan de seis pasos para detener la redirección de pagos, el fraude de facturas de proveedores y los timos de las tarjetas regalo

proofpoint.com/es

La amenaza actual más costosa para la ciberseguridad no tiene fácil solución

El Informe sobre delitos en Internet de 2020 del Internet Crime Complaint Center (IC3) del FBI afirma que, el año pasado, la "explosión de delitos en Internet" generó pérdidas por unos 1800 millones de dólares entre las víctimas de fraude por correo electrónico.

El departamento financiero de una empresa de repuestos perteneciente a uno de los mayores fabricantes de automóviles del mundo recibe un mensaje de correo electrónico en el que alguien le solicita una transferencia de 37 millones de dólares. Aunque cualquiera la consideraría una cifra elevada, para esta multinacional se trata de una transacción comercial habitual. Sin embargo, esta vez la solicitud no procede de un proveedor, de un socio comercial ni de un directivo, sino de un atacante que finge ser otra persona: estamos ante uno de los mayores ejemplos registrados de estafa de tipo Business Email Compromise (BEC), un fraude que compromete el correo electrónico corporativo.[1]

En Arizona, un empresario envía un mensaje de correo electrónico a una compañera para informarle de que la empresa va a trabajar con un nuevo proveedor, RS Enterprise. El empresario está demasiado ocupado viajando y no puede ordenar el pago de 157 000 dólares prometido al proveedor, así que facilita a su colega todos los datos necesarios para que ella transfiera el dinero. Más de 350 personas recibieron en Arizona mensajes con instrucciones similares, mensajes que parecían proceder de un proveedor u otro socio comercial conocido. Pero, según el FBI (Federal Bureau of Investigation), en realidad los remitentes eran ciberdelincuentes y llegaron a recaudar más de 30 millones de dólares.[2]

Un hombre envía a otro un mensaje de correo electrónico lamentándose de que debe confinarse porque presenta síntomas de COVID-19.
Está angustiado porque, con las prisas por ponerse en cuarentena, olvidó llevar consigo el móvil y otros objetos básicos, así que le pide al destinatario que compre tarjetas regalo de iTunes o Walmart por valor de 250 dólares. También le pide que le envíe una foto de las tarjetas y sus respectivos códigos

1 Nicole Lindsey (*CPO Magazine*). "Toyota Subsidiary Loses $37 Million Due to BEC" (Filial de Toyota pierde 37 millones de dólares en un ataque BEC). Septiembre de 2019.

2 Susan Campbell (*azfamily.com*). "Arizona workers lost $30 million to work email scams, FBI says" (Según el FBI, varios trabajadores de Arizona perdieron 30 millones de dólares en timos de correo electrónico corporativo). Abril de 2021.

para poder comprar con ellas todo lo necesario durante el confinamiento.[3]

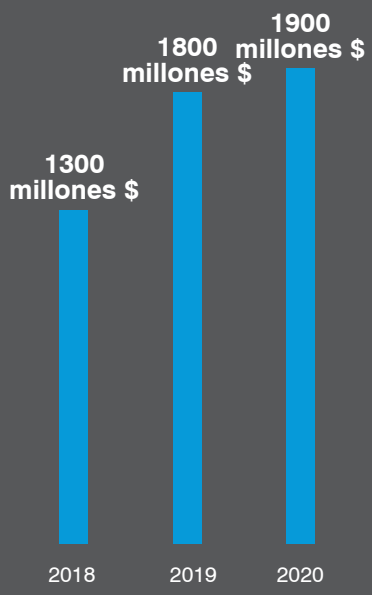
Una cara tendencia

Todas estas historias son ejemplos recientes de ataques con estafas BEC. Y son solo tres de los miles que desde principios de 2020 se han lanzado contra usuarios y empresas de Estados Unidos. De hecho, 2020 fue un año especialmente productivo para los ciberdelincuentes, que explotaron plenamente los trastornos de la pandemia y la creciente dependencia de la tecnología experimentada durante la crisis.

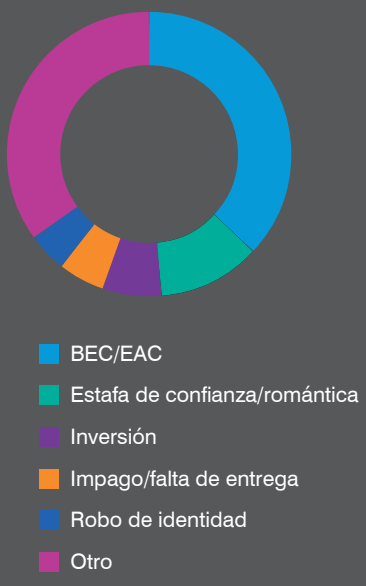
Entre estas actividades maliciosas destacan los ataques BEC, que han demostrado ser los que mayor coste tienen para las víctimas. El Informe sobre delitos en Internet de 2020 del Internet Crime Complaint Center (IC3) del FBI afirma que, el año pasado, la "explosión de delitos en Internet" generó pérdidas por unos 1800 millones de dólares entre las víctimas de fraude por correo electrónico.[4] Según el informe, esta cifra representa casi la mitad (44 %) de todas las pérdidas de empresas y particulares debidas a ciberdelitos denunciados el pasado año y también es 64 veces mayor que las pérdidas económicas atribuidas a la ola de campañas de ransomware que lanzaron los ciberdelincuentes en 2020.[5] El importe de las pérdidas económicas es incluso más impresionante si tenemos en cuenta que únicamente 19 369 del récord de 791 790 quejas que recibió el IC3 en 2020 de víctimas de la ciberdelincuencia estaban relacionadas con timos por correo electrónico. Es solo el 2,4 % de todas las quejas.

Lo bueno es que estas amenazas se pueden manejar con la perspectiva, la estrategia y las medidas adecuadas. En este libro electrónico se explica cómo funcionan los ataques BEC, qué formas adoptan y cómo puede evitar convertirse en la próxima víctima que salte a los titulares.

Pérdidas por BEC denunciadas



Desglose del total de pérdidas denunciadas por ciberdelincuencia



Fuente: FBI

3 Lance Whitney (*TechRepublic*). "Scammers exploit coronavirus for Business Email Compromise campaigns" (Los estafadores explotan el coronavirus en campañas de Business Email Compromise). Abril de 2020.

4 FBI. "2020 Internet Crime Report" (Informe sobre delitos en Internet de 2020). Marzo de 2021.

5 Sara Pan (*Proofpoint*). “FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020” (El informe de delitos de Internet del FBI revela que el fraude por correo electrónico es la amenaza que ocasionó las mayores pérdidas financieras en 2020). Marzo de 2021.

Índice

¿Por qué tienen tanto éxito los ataques BEC?

En pocas palabras: son difíciles de detectar y enormemente persuasivos.

Las estafas BEC se basan en gran medida en técnicas de ingeniería social para engañar a las víctimas y abusar de su confianza. Es decir, normalmente los mensajes no incluyen malware ni URL maliciosas que las defensas de ciberseguridad habituales, como herramientas tradicionales, productos autónomos y defensas nativas de las plataformas cloud, puedan bloquear o al menos detectar y analizar.

Además, los ataques BEC tienden a estar muy dirigidos. Es posible que en un ataque se envíen únicamente unos cuantos mensajes a un pequeño grupo de usuarios. El reducido volumen de mensajes ayuda a los atacantes a pasar desapercibidos ante numerosas herramientas de seguridad.

Estrategias de engaño: técnicas de suplantación de identidad

Los ciberdelincuentes también utilizan diferentes técnicas para configurar y ejecutar ataques BEC. Por ejemplo, en estos ataques son fundamentales las tácticas de suplantación de identidad, porque el atacante necesita que el destinatario considere legítimas las instrucciones del mensaje.

Los estafadores suelen investigar a las empresas para identificar a sus víctimas —proceso que consiste en determinar, normalmente mediante recursos públicos como LinkedIn, qué personas de la organización tienen acceso a datos, sistemas y activos de interés— y averiguar con quién trabajan y en quién confían. A continuación, lo más probable es que empleen una o varias de las estrategias siguientes para iniciar su ataque de estafa BEC (en realidad, la mayoría de estos ataques utilizan varias tácticas de impostura).

Falsificación del "display name" (nombre mostrado)

En el campo "De" de sus mensajes de correo electrónico, los ciberdelincuentes utilizan el nombre de ejecutivos, abogados, socios comerciales, proveedores o cualquier otra persona o entidad en la que pueda confiar un usuario. Normalmente, este campo es el identificador de correo más fácil de manipular para los estafadores. La mayoría de los ataques BEC usan la falsificación del nombre de "display-name", junto a otros métodos de suplantación de identidad, como la suplantación de dominios (véase más abajo).

"Domain spoofing" (suplantación de dominios)

En este tipo de phishing, los atacantes secuestran la marca de una empresa con el fin de robar dinero o datos a través de un ataque BEC. Utilizan una copia exacta del dominio de confianza de la empresa para enviar sus mensajes fraudulentos. Los ciberdelincuentes pueden llegar a crear un sitio web falso en una dirección web simulada que imita la marca de la organización para que los usuarios crean que interaccionan con una entidad legítima.

"Lookalike domains" (dominios parecidos)

Otra técnica de suplantación que utilizan los atacantes consiste en registrar un dominio que se parece tanto al dominio de confianza de la víctima que le induce a confusión. Por ejemplo, un ciberdelincuente que pretende engañar a los usuarios que trabajan en "granempresa.com" o hacen negocios con ella puede registrar un dominio llamado "gran.empresa.com" o "grannempresa.com" y enviar mensajes fraudulentos utilizando este dominio similar. El dominio falso es tan parecido al verdadero que pocos usuarios se dan cuenta de la diferencia hasta que es demasiado tarde.

Compromiso y usurpación de cuentas

Es la técnica de suplantación de identidad por excelencia. Cuando los atacantes comprometen la cuenta de un remitente de confianza, tienen acceso al historial de correo electrónico de esa persona, sus contactos y su calendario. En otras palabras, tienen toda la información y los accesos que necesitan para suplantar al titular de esa cuenta. En cierto sentido, no solo fingen ser el usuario: a todos los efectos son el usuario mismo.

La invasión de los ladrones de cuerpos: cómo se comprometen las cuentas

Phishing de credenciales

Esta estrategia de ataque ha existido durante décadas y está diseñada para inducir a los usuarios a divulgar las credenciales de cuentas confidenciales. Por ejemplo, el usuario seleccionado puede recibir un mensaje que parezca proceder del departamento informático de la empresa —quizá incluso indique "Servicio técnico" en el campo "De"— pidiéndole que haga clic en un enlace para validar su información de acceso a una aplicación corporativa.

Ataques de contraseña por fuerza bruta

Esta otra estrategia para hacerse con la cuenta de un usuario también lleva mucho tiempo en circulación. Básicamente, los ciberdelincuentes intentan adivinar la información de acceso de un usuario hasta que consiguen "forzar" su entrada en la cuenta. Es agresiva, pero a menudo rápida y eficaz, porque mucha gente aún utiliza combinaciones de nombre de usuario y contraseña fáciles de descifrar. Por lo tanto, sigue siendo un método de preferencia para muchos estafadores.

Tokens para aplicaciones OAuth cloud

Las aplicaciones de autenticación abierta (OAuth) se integran en servicios cloud y pueden estar suministradas por un proveedor diferente al del servicio. Estas aplicaciones añaden funciones empresariales y mejoran la interfaz de usuario de servicios cloud como Microsoft 365 y Google Workspace. La mayoría de las aplicaciones OAuth necesitan autorización para acceder y gestionar datos e información del usuario y para registrarse en otras aplicaciones cloud en su nombre.

Dada la amplitud de los permisos que pueden obtener, las aplicaciones OAuth son un vector y una superficie de ataque crecientes. Los ciberdelincuentes utilizan add-ons de terceros y técnicas de ingeniería social para convencer a los usuarios de que les concedan acceso a las aplicaciones cloud de su empresa mediante autenticación basada en token. Y una vez que se autoriza un token OAuth, el acceso se mantiene hasta que se revoca de forma manual.

Malware

Algunos atacantes emplean malware para obtener la información que necesitan y usurpar la cuenta de un usuario. Los tipos de malware que suelen utilizarse en la usurpación de cuentas incluyen:

- Registradores de pulsaciones, que captan lo que escribe un usuario, incluidas las credenciales de acceso
- Ladrones de información o "info stealers", que, como indica su nombre, roban datos tales como información de contacto y contraseñas de navegadores

La pérdida en dólares asociada al desvío de nóminas se disparó hasta el 815 % entre el 1 de enero de 2018 y el 30 de junio de 2019.[6]

—FBI

Tres tipos de ataques BEC

Cuando el atacante cuenta con toda la información necesaria para lanzar un ataque BEC, normalmente lleva a cabo uno de los siguientes tipos de ataque:

Desvío del pago de nóminas u otros pagos

Con este método de ataque, los ciberdelincuentes literalmente solicitan el envío de dinero.

En el **desvío de nóminas**, el atacante, ya sea suplantando a un empleado o utilizando su cuenta comprometida para hacerse pasar por él, pretende redirigir a su cuenta el pago legítimo de la nómina que se realiza en la cuentas bancaria del empleado.

En la **redirección de pagos**, el ciberdelincuente finge ser un remitente externo, por ejemplo un proveedor, y solicita a los representantes de la empresa que ingresen el pago de una factura en una cuenta bancaria diferente a la habitual (es decir, la suya).

6 FBI. "Business Email Compromise: The $26 Billion Scam" (Ataques BEC: el fraude que cuesta 26 000 millones de dólares). Septiembre de 2019.

Los ataques de desvío de nóminas y redirección de pagos pueden tener un propósito claro, pero no son tan sencillos de llevar a cabo para los perpetradores. Para empezar, exigen recopilar gran cantidad de información desde el principio. El ataque debe identificar correctamente a la persona del departamento de Recursos Humanos (RR. HH.) o de Nóminas de la empresa, información que puede reunirse mediante recursos públicamente disponibles, como LinkedIn, el sitio web de la empresa y bases de datos comerciales.

Y después queda otro paso difícil. Para parecer legítima y no levantar sospechas en la víctima, la solicitud de desvío de nóminas y pagos también debe mostrar una familiaridad verosímil con el proceso de abono de retribuciones o facturas de la empresa.

Cómo funcionan los ataques de desvío de nóminas y redirección de pagos

1. El atacante contacta con RR. HH. o Nóminas

Un atacante que se hace pasar por un empleado se pone en contacto por correo electrónico con el departamento de RR. HH. o Nóminas de la empresa y solicita actualizar su información de ingreso en cuenta. (El número de cuenta y el código ABA nuevos pertenecen al atacante, no al empleado al que suplanta).

2. RR. HH. o Nóminas cambia la cuenta

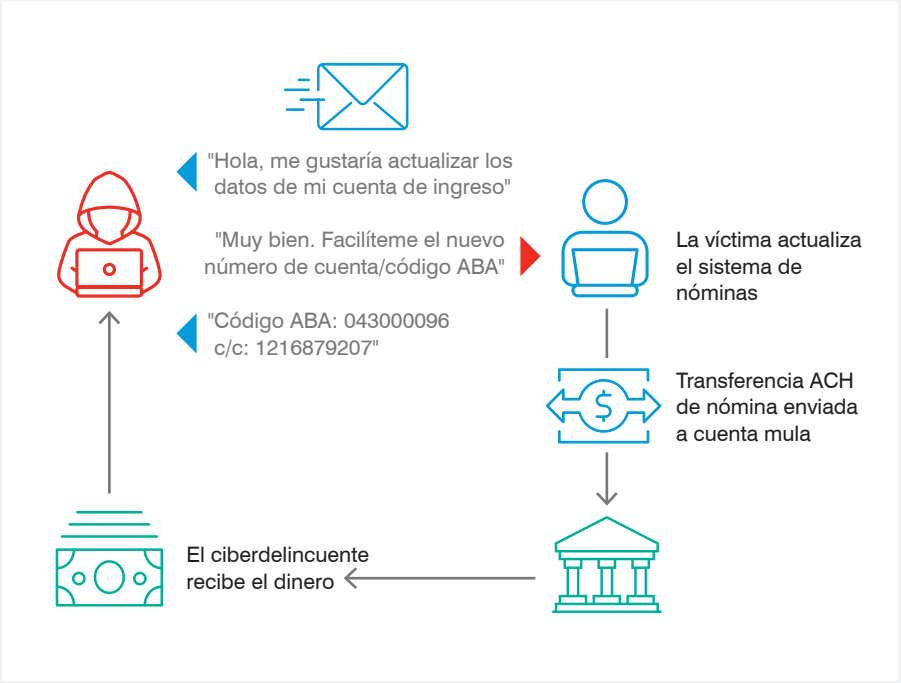
El departamento de RR. HH. o de Nóminas, creyendo que la solicitud es legítima, modifica los datos de la cuenta.

3. Se ingresa la nómina

La siguiente nómina del empleado se envía a la cuenta del atacante.

4. El atacante retira el dinero

El atacante retira el dinero y cierra la cuenta antes de que el empleado se dé cuenta de que no ha recibido la nómina.



Timos con tarjetas regalo

Imagine que recibe un mensaje de correo electrónico de su superior pidiéndole que compre unas cuantas tarjetas regalo de un conocido minorista. Le explica que tiene pensado distribuirlas entre los miembros del equipo como recompensa por el enorme esfuerzo realizado en el último proyecto. Y, como todos teletrabajan, le pide también que le envíe los códigos de las tarjetas para facilitarles su uso a los destinatarios.

¿Cuestionaría esta petición o la tramitaría sin pensarlo dos veces? En este último caso, sin duda no sería el único y, por desgracia, se convertiría en víctima de una estafa.

Según la Comisión Federal de Comercio (FTC), desde 2018 los consumidores dicen haber gastado casi 245 millones de dólares en tarjetas regalo utilizadas para pagar a los ciberdelincuentes en una gran variedad de estafas.[7] Y, según la Better Business Bureau (BBB), en más de un tercio (35 %) de los fraudes por impostura empresarial —donde se encuentran los ataques BEC—, los estafadores solicitan tarjetas regalo a sus víctimas.[8]

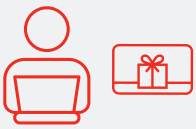
Pero ¿para qué quieren los atacantes que las víctimas les envíen tarjetas regalo? Porque tienen una rentabilidad rápida y fácil. No conllevan complicadas instrucciones de transferencia bancaria, lo que evita la suspicacia natural de las víctimas y los habituales controles fiscales de las empresas.

Además, las tarjetas regalo son una herramienta ideal para blanquear dinero. Los estafadores pueden utilizarlas para comprar y revender mercancía o simplemente para vender los códigos con descuento en Internet. Y una vez canjeadas las tarjetas, el dinero no puede recuperarse.

Cómo funcionan los ataques de tarjetas regalo

1. El ciberdelincuente suplanta a un empleado/amigo/CEO

Un ciberdelincuente suplanta a una figura de confianza en la empresa, como el CEO, y envía un mensaje de correo electrónico a su objetivo, como el asistente de dirección, solicitando la compra de tarjetas regalo. El atacante puede darle a entender que las tarjetas son obsequios para empleados, clientes o proveedores. También indica a la víctima que le envíe los números de las tarjetas y los códigos necesarios para canjearlas.



2. La víctima adquiere las tarjetas regalo y envía la información correspondiente

La víctima tramita la solicitud.

3. El ciberdelincuente recibe el dinero

El atacante canjea las tarjetas por dinero o por mercancía que después revende. O es posible que venda los códigos directamente en el mercado negro.

7 FTC. "FTC Data Show Gift Cards Remain Scammers' Favorite Payment Method" (Los datos de la FTC indican que las tarjetas regalo siguen siendo el método de pago favorito de los estafadores). Diciembre de 2010.

8 Better Business Bureau. "BBB Investigation on gift card payment scams: Why do scammers love gift cards?" (Investigación de BBB sobre los timos de pago de tarjetas regalo: ¿por qué les gustan tanto a los estafadores?). Marzo de 2021.

Fraude de facturas de proveedores

En un estudio de siete días llevado a cabo a principios de 2021, el 98 % de las empresas recibieron ataques con suplantación de identidad o vulneración de la seguridad de un proveedor.

Como su nombre indica, el fraude mediante facturas de proveedores es un ataque en el que un ciberdelincuente finge ser un proveedor, un distribuidor u otro socio comercial para conseguir que la empresa abone una factura falsa. La táctica del estafador suele incluir la suplantación de la dirección de correo electrónico legítima del proveedor o la usurpación de la cuenta de correo de uno de sus empleados.

La estafa de facturas de proveedores está en auge entre los tipos de ataques BEC, ya que cada vez más atacantes utilizan la cadena de suministro y el ecosistema de los partners como vector de amenaza para lanzar ataques indirectos contra empresas. Tenga en cuenta lo siguiente:

- En un estudio de siete días llevado a cabo a principios de 2021, el 98 % de las empresas recibieron ataques mediante suplantación de identidad o vulneración de la seguridad de un proveedor[9]
- Uno de cada cuatro mensajes de phishing procede de proveedores suplantados y comprometidos.[10]

Los ciberdelincuentes se hacen pasar por suministradores minoristas de material de oficina, agencias de diseño web, firmas de marketing, servicios de limpieza y catering, servicios de control de plagas... la lista es larga. Y a menudo la suplantación les funciona durante mucho tiempo porque numerosas empresas, especialmente las más grandes, carecen de visibilidad de su cadena de suministro. No saben cuántos proveedores tienen ni cuáles pueden suponer un riesgo.

Grandes ganancias potenciales

El fraude de facturas de proveedores normalmente genera las pérdidas económicas más cuantiosas de los ataques BEC, ya que pueden comportar pagos considerables entre empresas.[11] Estas estafas suelen ser enormemente eficaces porque se "cuelan" en los procesos rutinarios de la empresa y utilizan cuentas corporativas legítimas de los proveedores u otros socios comerciales en los que confía la víctima. Al ser legítimas, estas cuentas comprometidas eluden la detección de muchos controles de seguridad.

Algunos ciberdelincuentes de extremada audacia e ingenio se hacen pasar incluso por proveedores que ni siquiera existen… y aun así tienen éxito. Por ejemplo, entre 2013 y 2015, un estafador y una serie de cómplices defraudaron más de 100 millones de dólares a Google y Facebook con una compleja estafa de facturas de proveedores. Crearon en Letonia una empresa falsa utilizando el nombre de una firma real afincada en Taiwán con la que hacían negocios ambas tecnológicas. Sin embargo, al final Google y Facebook tuvieron suerte: los delincuentes fueron apresados y al parecer las empresas pudieron recuperar todo o la mayor parte del dinero.[12]

9 Sara Pan (*Proofpoint*). "98% of Organizations Received Email Threats from Suppliers: What You Should Know" (El 98 % de las organizaciones recibieron amenazas por correo electrónico a través de los proveedores: lo que debe saber). Febrero de 2021.

10 *Ibid.*

11 Sara Pan (*Proofpoint*). "FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020" (El informe de delitos de Internet del FBI revela que el fraude por correo electrónico es la amenaza que ocasionó las mayores pérdidas financieras en 2020). Marzo de 2021.

12 Vanessa Roma (*NPR*). "Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of $100 Million" (Un hombre se declara culpable de un ataque de phishing que defraudó 100 millones de dólares a Facebook y Google). Marzo de 2019.

De: Chris@proveedor (cuenta de proveedor comprometida)
Para: Jason (víctima)

External Message
Thanks Connie~

Dear Jason,

Hope you are well.
The following invoices are due or will be due in Apr. And now we haven't received the payment from you side.
Could you please help to arrange the payment in Apr? Thank you.

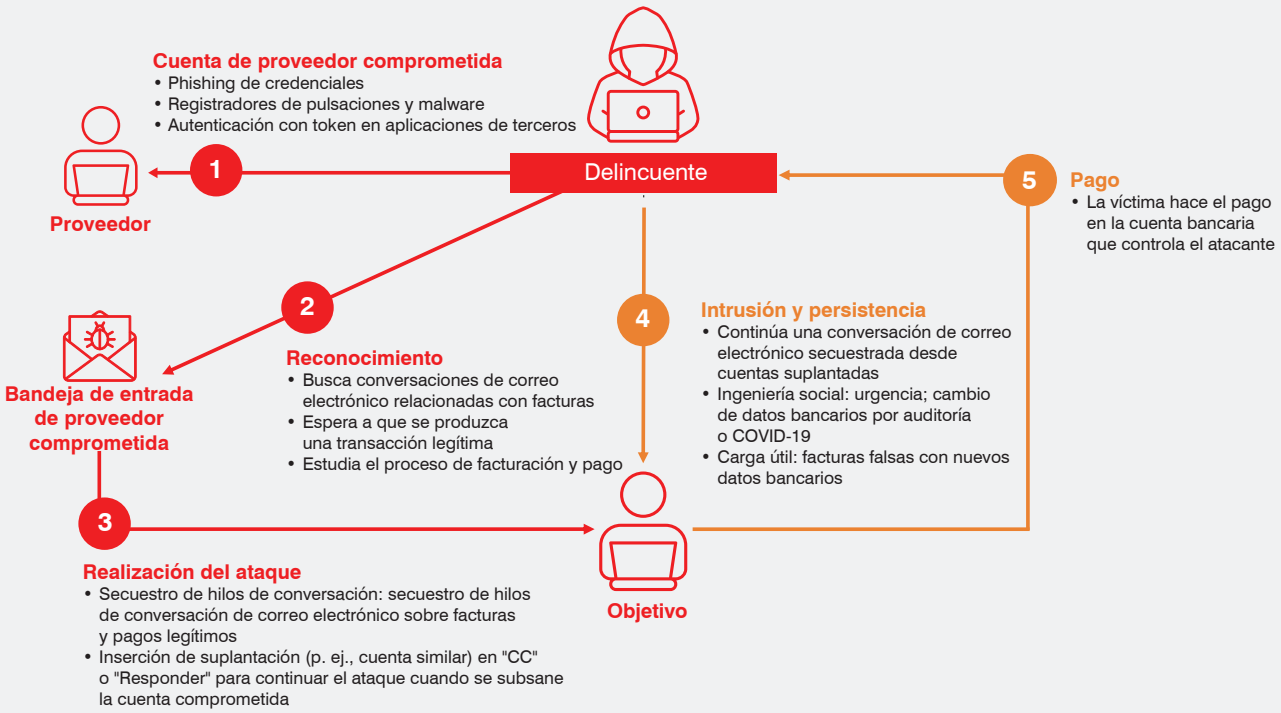
Total amount: USD 2,791,867.92

Class	Number	Amount(USD)	Days Late	Transaction Date	Due Date
Invoice	[redacted]	179,976.49	43	12-26-2019	03-10-2020
Invoice	[redacted]	15,328.07	34	01-04-2020	03-19-2020
Invoice	[redacted]	36,128.50	31	01-07-2020	03-22-2020
Invoice	[redacted]	29,744.80	31	01-07-2020	03-22-2020
Invoice	[redacted]	62,243.65	29	01-09-2020	03-24-2020
Invoice	[redacted]	9,306.72	28	01-10-2020	03-25-2020
Invoice	[redacted]	8,846.00	28	01-10-2020	03-25-2020
Invoice	[redacted]	1,873.20	28	01-10-2020	03-25-2020
Invoice	[redacted]	3,439.44	27	01-11-2020	03-26-2020
Invoice	[redacted]	54,257.82	27	01-11-2020	03-26-2020
Invoice	[redacted]	1,267.58	24	01-14-2020	03-29-2020
Invoice	[redacted]	11,290.40	22	01-16-2020	03-31-2020

Ejemplo de mensaje de correo electrónico enviado como parte de una tentativa de fraude de facturas de proveedores.

Los ciberdelincuentes que recurren al fraude de facturas de proveedores pueden utilizar tanto la suplantación como las cuentas comprometidas para robar credenciales de los usuarios, distribuir malware y, por supuesto, enviar facturas falsas. Por eso, aunque lo que pretenden con estos timos es lucrarse, si tienen tiempo y oportunidad también aprovechan para poner los cimientos de otros ataques.

Cómo funciona el fraude de facturas de proveedores



1. El ciberdelincuente usurpa una cuenta de correo electrónico

Normalmente, el fraude de facturas de proveedores empieza cuando el ciberdelincuente usurpa la cuenta de correo electrónico de un empleado de un proveedor de confianza o crea una cuenta tan parecida que induce a confundirla con ella.

2. El atacante busca mensajes relacionados con facturas

A continuación, el atacante analiza la lista de contactos de la cuenta comprometida del proveedor y busca mensajes relacionados con facturas en la bandeja de entrada del usuario.

3. El atacante se "cuela" en una transacción legítima

Tras informarse sobre los procesos de facturación y pago de la organización, el atacante espera la oportunidad de "colarse" en una transacción legítima.

4. El atacante responde dentro de una conversación existente

En este momento, el atacante suele cambiar a una cuenta similar del dominio y responde en un hilo de conversación existente para mantener acceso a la conversación legítima incluso en el caso de que la empresa atacada recupere el control de la cuenta.

5. El atacante envía una factura falsificada

Cuando el proveedor envía una factura a la organización, el atacante interviene y envía una factura falsa en su lugar. Esta factura incluye los datos de pago de una cuenta que controla el atacante y posiblemente una solicitud para que la organización modifique los datos de pago que figuran actualmente en su expediente.

6. La organización hace el ingreso en la cuenta del atacante

La organización paga la factura e ingresa el importe en la cuenta del atacante. Cuando el proveedor real se da cuenta de que no le han pagado, el atacante ya ha retirado el dinero y ha cerrado la cuenta.

Seis pasos para proteger su empresa de los ataques BEC

En los ataques de fraude por correo electrónico, los ciberdelincuentes utilizan múltiples tácticas y combinaciones de suplantación y compromiso de cuentas. Y cada ataque es diferente. No obstante, un factor fundamental común a todos ellos es que necesitan que la víctima no se dé cuenta de que abusan de su confianza.

Por sí sola, ninguna línea de defensa logra prevenir con eficacia estos ataques complejos, sofisticados y sigilosos. Por eso hace falta una estrategia multicapa, totalmente integrada y centrada en las personas.

Estas son las seis estrategias principales para crear este tipo de defensa:

1. Visibilice los riesgos de ataques BEC a sus usuarios

Lógicamente, un enfoque centrado en las personas empieza por las personas. Cada persona es única. También lo es su valor para los ciberdelincuentes y, por lo tanto, el riesgo que suponen para la empresa. El perfil general de riesgo de un usuario está formado por una combinación infinita de tres factores: vulnerabilidad, ataques y privilegios.

Para determinar el perfil de riesgo de los usuarios de su empresa, debe evaluar:

- **Sus hábitos y puntos débiles digitales (vulnerabilidades).** Hágase preguntas como: ¿Cuál es la función de los usuarios? ¿Qué están autorizados a hacer? ¿Cómo trabajan? ¿En qué hacen clic? ¿Cómo acceden a los recursos de la empresa? ¿A qué tipos de aplicaciones y datos tienen acceso?
- **Los tipos de amenazas a los que pueden enfrentarse (ataques).** ¿Es probable que el usuario se enfrente a ataques altamente dirigidos, como los BEC, y por lo tanto necesite una protección más avanzada y formación en materia de seguridad? ¿O es más fácil que reciba ciberamenazas ordinarias de bajo perfil que pueden contenerse con defensas estándar y formación básica en ciberseguridad?
- **Su nivel de acceso (privilegios).** Los privilegios determinan todo aquello potencialmente valioso a lo que tiene acceso un usuario, como datos, autoridad financiera y relaciones estratégicas. Su cargo en la empresa —por ejemplo, en el departamento financiero o en la dirección— es otro factor que cuenta a la hora de determinar y calificar sus privilegios. Pero no es el único y, con frecuencia, ni siquiera es el más importante.

Unos niveles de riesgo elevados de cualquiera de estas tres categorías constituyen un motivo de preocupación y, en la mayoría de los casos, requieren niveles adicionales de seguridad. Cuando dos o más factores presentan un riesgo elevado, es señal de un problema de seguridad más urgente.

A continuación se incluyen cuatro categorías de usuarios que ponen de manifiesto cómo las combinaciones de vulnerabilidades, ataques y privilegios afectan a su nivel de riesgo general:

- **Objetivos latentes**: son los usuarios con privilegios elevados que también son más vulnerables a los timos de phishing.
- **Objetivos fáciles**: estos usuarios reciben numerosos ataques y son vulnerables a las amenazas.

EVALUACIÓN DEL RIESGO DEL USUARIO

Al igual que las personas son únicas, también lo es el valor de cada una para los ciberdelincuentes, así como el riesgo para los empresarios.

Todas tienen sus propias **vulnerabilidades**, hábitos digitales y puntos débiles. Los atacantes les **atacan** de diversas formas y con distinta intensidad. Además, tienen distintos niveles de **privilegios** de acceso a los datos, sistemas y recursos.

Estos tres factores interrelacionados determinan su riesgo global.

- **Objetivos importantes:** estos usuarios con altos privilegios son un objetivo frecuente y se enfrentan a un aluvión constante de ataques que, si tienen éxito, pueden ocasionar graves daños a la organización.
- **Objetivos inminentes**: esta cuarta categoría contiene a los usuarios que la organización debe tratar como prioridad de seguridad urgente. Registran un nivel elevado en los tres factores de riesgo: vulnerabilidad, ataques y privilegios. En otras palabras, son vulnerables a las herramientas y las tácticas de los ciberdelincuentes, están en el punto de mira de los atacantes y tienen acceso a datos, sistemas y otros recursos que causarían un daño duradero si un ataque prosperase.

2. Incremente la visibilidad de los proveedores

Debe saber quiénes son sus proveedores, qué dominios utilizan para enviar mensajes de correo electrónico a sus usuarios y con qué personas de esas empresas interaccionan normalmente sus empleados.

Identificar a las personas de la empresa que son más vulnerables, reciben más ataques y tienen más privilegios es un paso fundamental para prevenir ataques BEC. Pero la cadena de suministro y el ecosistema de partners son vectores de amenazas importantes para los ciberdelincuentes, que los utilizan para lanzar ataques indirectos contra sus objetivos. Por eso debe asegurarse de tener una buena visibilidad de la cadena de suministro de su empresa y conocer los riesgos que suponen los interlocutores externos.

Debe saber quiénes son sus proveedores, qué dominios utilizan para enviar mensajes de correo electrónico a sus usuarios y con qué personas de esas empresas interaccionan normalmente sus empleados. También, en la medida de lo posible, debe averiguar quiénes son los proveedores de sus proveedores. Tómese tiempo para crear un catálogo de proveedores tan detallado como sea necesario para poder obtener visibilidad de los riesgos que comportan.

Para facilitar este proceso, busque una solución que pueda ayudarle a automatizar las tareas de:

- Identificar quiénes son sus proveedores y los dominios que utilizan para enviar mensajes de correo electrónico a los usuarios de su empresa
- Buscar dominios parecidos a los de los proveedores
- Ver las amenazas procedentes de los dominios de los proveedores, como suplantación, malware, phishing y spam
- Validar los registros DMARC de los proveedores y bloquear ataques que intenten suplantar sus dominios

3. Detecte y bloquee las amenazas BEC antes de que se infiltren en su entorno

Esta tercera recomendación puede parecer evidente, pero recuerde que no todas las ciberdefensas son eficaces para detectar y bloquear las tácticas de suplantación.

Los ataques BEC no son como otras ciberamenazas. Por eso, para detenerlas hacen falta soluciones y estrategias avanzadas de análisis dinámico y alerta permanente ante posibles amenazas. La detección basada en reglas estáticas no basta para identificar y detener ataques BEC, ya que no pueden mantener el ritmo de evolución de sus técnicas y tácticas.

Dónde buscar signos de BEC

- Datos del encabezado del mensaje
- Dirección IP del remitente
- Relación entre el remitente y el destinatario
- Reputación del remitente
- Grado de confianza, tono y lenguaje

El fraude de facturas de proveedores —que normalmente implica el uso de la cuenta legítima pero comprometida de un proveedor— puede ser aún más peliagudo. Las defensas de su empresa tienen que ser capaces de bloquear incluso los más sofisticados ataques de fraude de proveedores. Elija una solución que analice dinámicamente los mensajes en busca de diversas tácticas asociadas con este tipo de fraude.

Tácticas de fraude de facturas de proveedores

- Cambios de la dirección de respuesta
- Uso de direcciones IP maliciosas
- Uso de dominios de proveedores cuya identidad ha sido usurpada
- Palabras o frases empleadas habitualmente en ataques de fraude de proveedores

Aprendizaje automático

Las herramientas de aprendizaje automático se pueden adaptar para las últimas amenazas BEC sin necesidad del constante ajuste manual que precisan las herramientas tradicionales para afrontarlas.

Las herramientas de aprendizaje automático se pueden adaptar para las últimas amenazas BEC sin necesidad del constante ajuste manual que precisan las herramientas tradicionales para afrontarlas. El aprendizaje automático más eficaz puede reaccionar con rapidez a la evolución de las tácticas de los atacantes bloqueando los mensajes peligrosos y autorizando la entrega de los inofensivos.

Pero no se equivoque: aislado, el aprendizaje automático no es un remedio mágico. Su eficacia depende de la profundidad y la amplitud del conjunto de datos con el que se entrenan los modelos y de la experiencia en amenazas de las personas que los perfeccionan. Los modelos entrenados con datos erróneos o incompletos y sin el contexto de las amenazas generan un elevado índice de falsos positivos, lo que se traduce en más trabajo para los equipos de seguridad y mensajería y en una peor experiencia para el usuario.

4. Haga más resilientes a sus usuarios

Los ataques BEC se basan en ingeniería social, no en exploits técnicos, y solo funcionan si los usuarios caen en la trampa. Por eso, los usuarios bien formados son la última —y más fuerte— línea de defensa de su empresa.

Todos sus empleados deben conocer las amenazas de impostores. Sin embargo, como estos ataques están dirigidos a personas específicas, debe concentrar la formación sobre seguridad en los empleados de departamentos como Contabilidad y Finanzas, Recursos Humanos y Suministros, para que conozcan y estén alerta a las tácticas de engaño habituales. Además, haga hincapié en:

- Impartir formación adecuada a los cargos importantes de la empresa, como el CEO y el CFO.
- Incluir a cualquier otro empleado que suponga un riesgo elevado por ser más vulnerable, recibir más ataques o tener más privilegios.
- Considere la posibilidad de formar también en materia de seguridad a contratistas y trabajadores autónomos que tengan acceso a los sistemas corporativos. Estos trabajadores suelen formar parte del panorama laboral actual, especialmente en los entornos modernos cada vez más distribuidos y remotos, pero a menudo se pasan por alto desde el punto de vista de la seguridad.
- Aborde el riesgo de fraude de facturas de proveedores con los usuarios que más probabilidades tengan de afrontar este tipo de ataques BEC.

La formación de concienciación en materia de seguridad y ataques sobre fraudes BEC no debe consistir en un curso puntual ni en ejercicios esporádicos, ya que estos ataques, como la mayoría de las ciberamenazas, son constantes y están en permanente evolución.

Si contrata la ayuda de un tercero con experiencia en cursos de este tipo, contará con impartir la formación adecuada a las personas apropiadas, por ejemplo, realizando simulaciones de phishing basadas en ataques BEC reales que preparen a los usuarios para las amenazas que tienen más probabilidades de recibir.

Otra sugerencia para combatir los ataques BEC es alentar a los usuarios a denunciar los mensajes sospechosos... y ponérselo fácil. Cuando un usuario denuncia un mensaje, también es preciso que los equipos de seguridad reaccionen con agilidad y determinen rápidamente si el mensaje conlleva una amenaza o no. Si tardan en responder (o no responden), puede que en el futuro los usuarios se sientan menos inclinados a denunciar mensajes sospechosos y tengan menos cuidado a la hora de abrir o contestar mensajes de riesgo.

5. Automatice la respuesta y la corrección de incidentes

Al automatizar los aspectos principales del análisis del correo electrónico y la respuesta, los equipos de seguridad pueden establecer mejor las prioridades en su trabajo y reaccionar con más rapidez a las amenazas y los mensajes de correo electrónico que denuncien los usuarios.

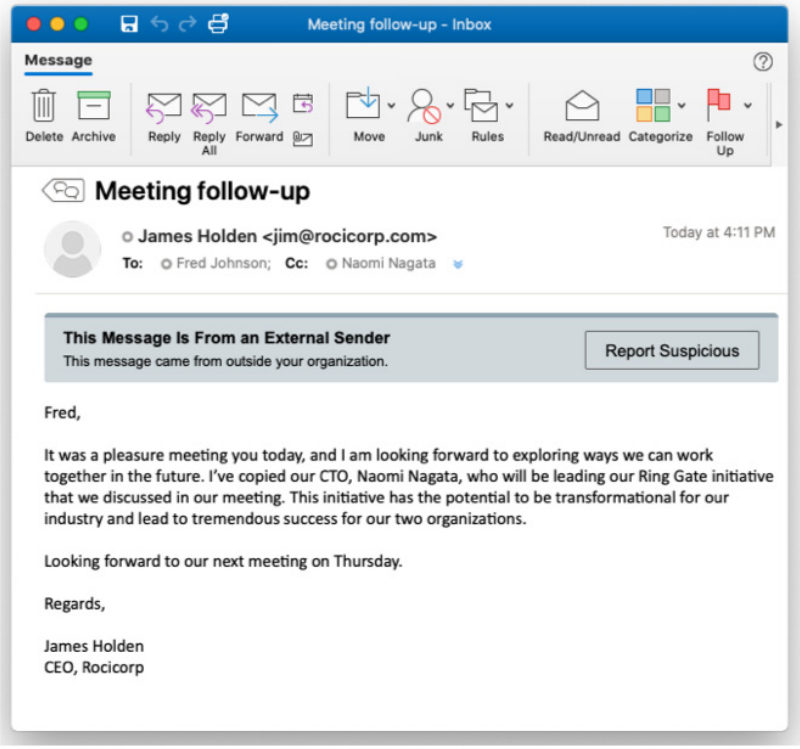
La mayoría de las organizaciones se enfrentan a un problema de escasez de personal de seguridad de TI. Los equipos de seguridad están desbordados por la necesidad de administrar un gran número de proveedores y productos de seguridad que rara vez son compatibles. Como consecuencia, se complica la detección, la investigación y la neutralización de las amenazas BEC en toda la empresa. Y cuanto más largos sean los procesos, más tiempo estará expuesta la empresa.

Al automatizar los aspectos principales del análisis del correo electrónico y la respuesta, los equipos de seguridad pueden establecer mejor las prioridades en su trabajo y reaccionar con más rapidez a las amenazas y los mensajes de correo electrónico que denuncien los usuarios. Los equipos de seguridad también deben transmitir a los usuarios preocupados que, si es necesario, pueden ayudarles a acceder a la información de un mensaje marcado como sospechoso durante su análisis.

Etiquetar automáticamente los mensajes externos para informar a los destinatarios de su origen también puede contribuir a que los usuarios examinen el mensaje más de cerca para asegurarse de que es legítimo y que no procede de un impostor.

Si resulta que un mensaje es malicioso, puede ponerse en cuarentena automáticamente junto con todas sus copias, incluidos los reenvíos a otros usuarios. No es necesario administrar o investigar manualmente cada incidente, lo que permite ahorrar tiempo y esfuerzo a su equipo.

Para terminar, los usuarios reciben un mensaje personalizado en el que se les informa de que el mensaje era malicioso. Este enfoque refuerza los comportamientos positivos y los anima a denunciar mensajes similares en el futuro.



6. Protéjase de los ataques dirigidos a sus clientes y su marca

Busque una solución que proteja su marca y la reputación de su empresa evitando que se envíen mensajes fraudulentos a través de sus dominios de confianza.

En el caso de la falsificación 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.

Es posible que la falsificación de la marca no ocasione pérdidas económicas directas a su compañía, pero puede dañar su reputación, erosionar la confianza de los clientes y provocar un daño duradero a su negocio.

Busque una solución que proteja su marca y la reputación de su empresa evitando que se envíen mensajes fraudulentos a través de sus dominios de confianza. La solución debe verificar que todos los mensajes recibidos y enviados desde su organización cumplen los controles DMARC (Domain-based Message Authentication, Reporting and Conformance) estándar del sector.

También debe señalar todos los mensajes de correo electrónico enviados a través de su dominio, incluidos los de remitentes externos de confianza.

Incluso bloqueando su dominio, los dominios parecidos pueden ser un problema, ya que favorecen que los clientes se dejen engañar por mensajes BEC que simulan proceder de su empresa. Busque dominios recién registrados que suplanten a su empresa en ataques por correo electrónico o sitios web de phishing antes de que pasen de la inactividad al estado activo con carga maliciosa. Ocurre lo mismo con los ciberdelincuentes que usurpan su marca en otros canales digitales, como dominios web, redes sociales y redes oscuras fraudulentas.

Conclusión: la importancia de una defensa unificada y basada en las personas

Para crear una estrategia multicapa, totalmente integrada y centrada en las personas que proteja a su empresa del riesgo de ataques de fraude BEC, debe abandonar la mentalidad de "seguridad compartimentada". Aun teniendo productos sueltos que aborden todos los frentes de ataque, estos deben colaborar estrechamente entre sí de modo que cada elemento refuerce a los demás.

Con una solución de seguridad del correo electrónico unificada o integrada, podrá simplificar sus operaciones de seguridad y hacer mejor uso de sus recursos de TI, reducirá los costes y las tareas manuales y, sobre todo, será mucho más eficaz a la hora de proteger su organización del panorama actual de amenazas BEC en constante evolución.

Conozca las soluciones de Proofpoint para proteger su empresa frente a ataques BEC en:

proofpoint.com/us/solutions/bec-and-eac-protection.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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 encuentran más de la mitad del Fortune 1000, 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.

0503-004-01-01 06/21