LIBRO ELECTRÓNICO

La nube en el punto de mira

Explotación de vulnerabilidades de Microsoft 365: cómo los ciberdelincuentes aprovechan el uso compartido de archivos, la identidad y la cadena de suministro

proofpoint.

Introducción

En la era digital, Microsoft 365 es una herramienta fundamental para llevar a cabo el trabajo. Desafortunadamente, su popularidad lo ha convertido en objetivo principal para los ciberdelincuentes. Y aunque Microsoft 365 incluye una serie de funciones nativas para detener los ciberataques, estas herramientas simplemente no son suficientes para hacer frente a los ataques sofisticados actuales.

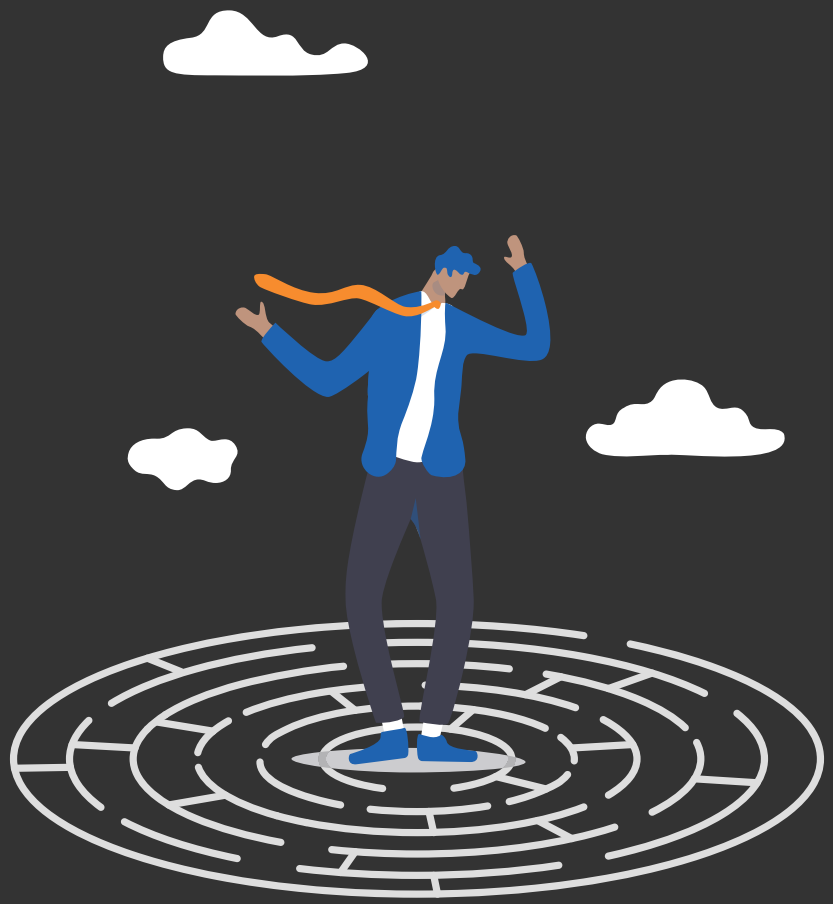
Cada año, los ataques contra Microsoft 365 centrados en las personas cuestan a las organizaciones millones de dólares y generan frustración tanto en los equipos de seguridad como en los usuarios. La situación ha alcanzado tal nivel que expertos del sector como Gartner coinciden en que las herramientas integradas en la nube deben complementarse con soluciones de terceros[1].

La razón por la que las herramientas integradas ya no son suficientes es bien sencilla: los ciberdelincuentes se han convertido en expertos a la hora de atacar a las personas. Y esto los hace cada vez más difíciles de detener.

El compromiso de usuarios suele ser el primer paso en una serie de eventos de mayor envergadura que ocurren cuando una organización sufre una vulneración de la seguridad. Conocida como la "cadena de ciberataques", estos eventos comienzan con el compromiso del usuario y avanzan hacia el abuso de privilegios, robo de datos y mucho más.

Etapas de la cadena de ciberataque.

1 Gartner. Market Guide for Email Security" (Market Guide para la seguridad del correo electrónico), febrero de 2023.



Este libro electrónico analiza cinco tipos de ataques centrados en las personas que ofrecen a los ciberdelincuentes una puerta de entrada y, en última instancia, ponen a las organizaciones en riesgo de sufrir consecuencias más graves. Estos ataques son muy difíciles de detectar solamente con las funciones que incluye Microsoft 365.

1. Ataques Business Email Compromise (BEC)
2. Ataques por teléfono o TOAD
3. Cargas maliciosas en archivos compartidos
4. Usurpación de cuentas
5. Cuentas de proveedores comprometidas

Cada sección incluye varios ejemplos que ponen de manifiesta lo variados e ingeniosos pueden ser estos ataques. También muestran cómo casi cualquier persona que utiliza Microsoft 365, sin seguridad adicional, puede convertirse en víctima de un atacante experimentado.

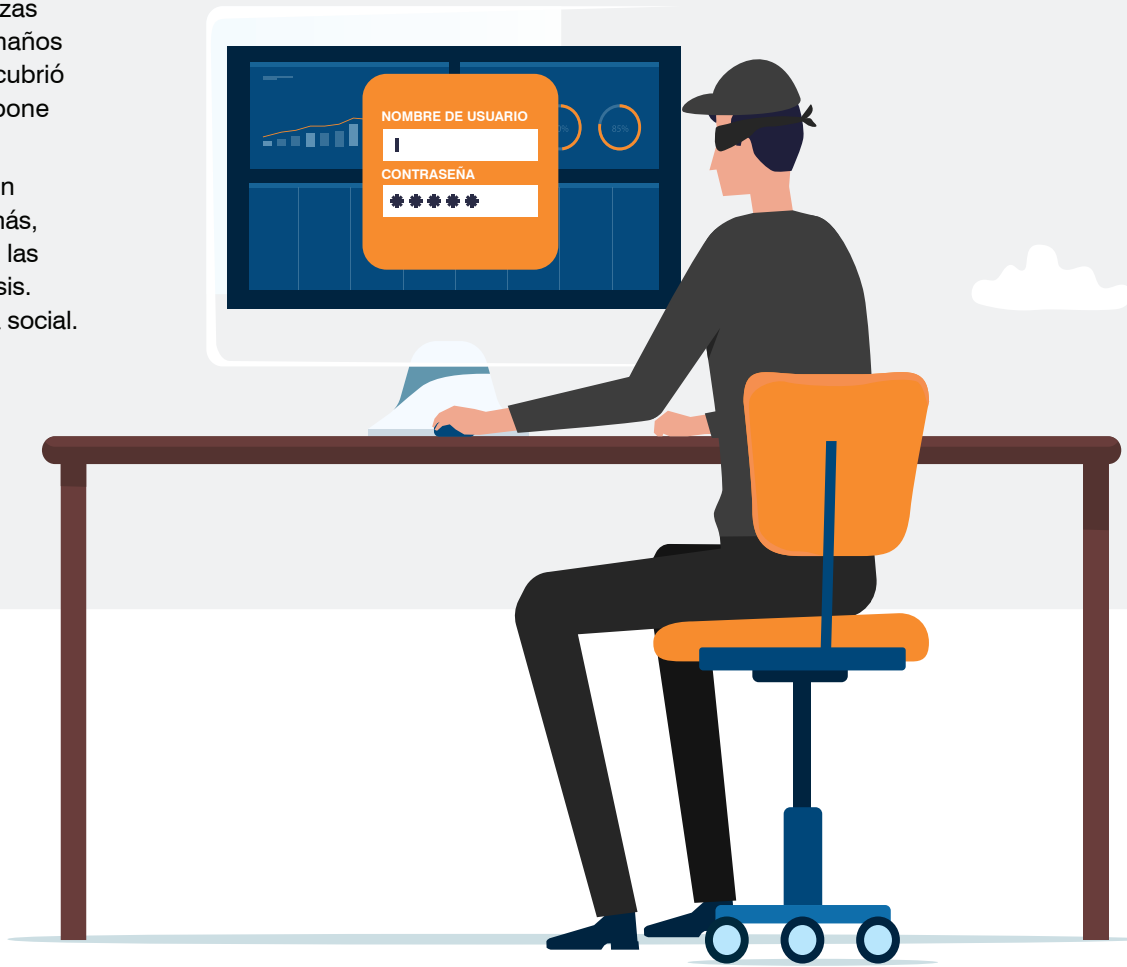
Todos estos ejemplos son amenazas del mundo real observadas por Proofpoint en evaluaciones de riesgo que hemos realizado para organizaciones.

SECCIÓN 1

BUSINESS EMAIL COMPROMISE

Los ataques Business Email Compromise (BEC) representan una de las amenazas más dañinas desde el punto de vista financiero para empresas de todos los tamaños y sectores. Las pérdidas siguen aumentando año tras año. En 2022, el FBI descubrió que las empresas perdieron 2700 millones de dólares por estafas BEC. Eso supone 300 millones de dólares más que en 2021.

Muchos de los ataques BEC actuales son enormemente sofisticados, cuentan con una buena financiación y están cuidadosamente planificados y estudiados. Además, son muy difíciles de detectar. Esto se debe a que los ciberdelincuentes no envían las cargas útiles habituales, como URL maliciosas o archivos adjuntos, para su análisis. En su lugar, recurren a la suplantación de identidad y otras técnicas de ingeniería social.



2 FBI. "2022 Internet Crime Report" (Informe sobre delitos en Internet de 2021), 2023.

Entorno:
Microsoft 365

Categoría de amenaza:
ingeniería social

Tipo de ataque:
desvío de nóminas

Objetivo:
administrador
de prestaciones

Ataque de desvío de nóminas

Los ataques de desvío de nóminas son ataques de fraude por correo electrónico normalmente dirigidos contra empleados de servicios financieros y fiscales, nóminas y recursos humanos. En estos ataques, los ciberdelincuentes buscan ganarse la confianza de los empleados con el fin de cambiar los detalles de pago y robar las nóminas de los empleados. Utilizan tácticas de ingeniería social, por lo que pueden ser extremadamente difíciles de detectar. Los desvíos de nóminas se consideran un riesgo moderado para empresas y organizaciones.

Ejemplo de ataque de desvío de nóminas.

En este ataque, un estafador envió un mensaje de correo electrónico a un administrador de beneficios desde una cuenta de Gmail haciéndose pasar por un empleado que solicitaba un cambio en la domiciliación de su nómina a una nueva cuenta bancaria. En esta ocasión, el estafador y la víctima incluso llegaron a intercambiar varios mensajes. En evaluaciones y pruebas de concepto (POC) realizadas por Proofpoint, los controles de seguridad de correo electrónico nativos de Microsoft fueron incapaces de detener este tipo de ataques.

Entorno:
Microsoft 365

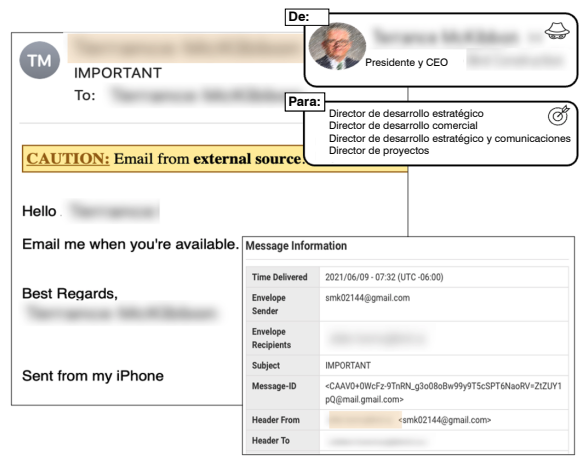
Categoría de amenaza:
ingeniería social

Tipo de ataque:
suplantación

Objetivo:
directivos, desarrollo estratégico y comercial

Ataque de suplantación de directivos

Cuando un ciberdelincuente consigue hacerse pasar por un empleado, el perjuicio económico para la empresa puede ser serio. Sin embargo, cuando se hacen pasar por altos ejecutivos, las pérdidas pueden ser mucho más graves. En los últimos años, este tipo de ataques ha aumentado drásticamente. Desde marzo de 2020, Proofpoint ha registrado más de 7000 suplantaciones de CEO en estafas por correo electrónico. Más de la mitad de los clientes de Proofpoint han sufrido al menos un intento de estafa a través de la cuenta de correo electrónico comprometida de un alto ejecutivo.



Ejemplo de ataque de suplantación de directivos.

Aquí, un atacante envió mensajes de correo electrónico a empleados desde una cuenta de Gmail, haciéndose pasar por un CEO que necesitaba que tomaran medidas adicionales. Si hubieran respondido, el estafador podría haber obtenido fácilmente datos o recompensas económicas. En las evaluaciones y pruebas de concepto realizadas por Proofpoint, los controles de seguridad de correo electrónico nativos de Microsoft no pudieron detener este tipo de ataques.

Entorno:
Microsoft 365

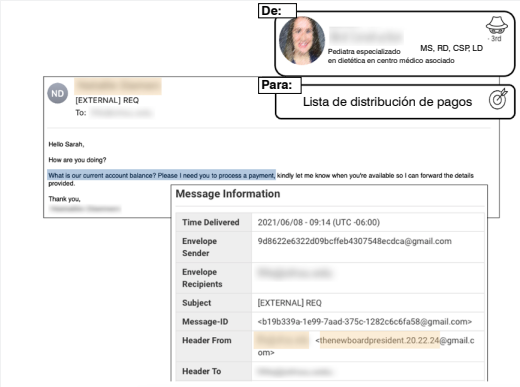
Categoría de amenaza:
ingeniería social

Tipo de ataque:
fraude de facturas

Objetivo:
departamento financiero

Ataque a través de facturas de proveedores

Las estafas que se dirigen a consumidores, como el fraude con tarjetas de regalo, caracterizan la gran cantidad de ataques BEC. Sin embargo, los estafas BEC de estilo B2B que se dirigen a proveedores son muy específicas, por lo que, aunque pueden ser menos frecuentes, las pérdidas financieras de estos ataques pueden ser bastante importantes. Proofpoint ha detenido múltiples intentos de facturación a proveedores donde cada incidente podría haber costado millones de dólares. En estos ataques, los ciberdelincuentes envían facturas falsas o información de redirección nueva para que los pagos se envíen a una cuenta bancaria controlada por ellos.



Ejemplo de fraude de facturación a proveedores.

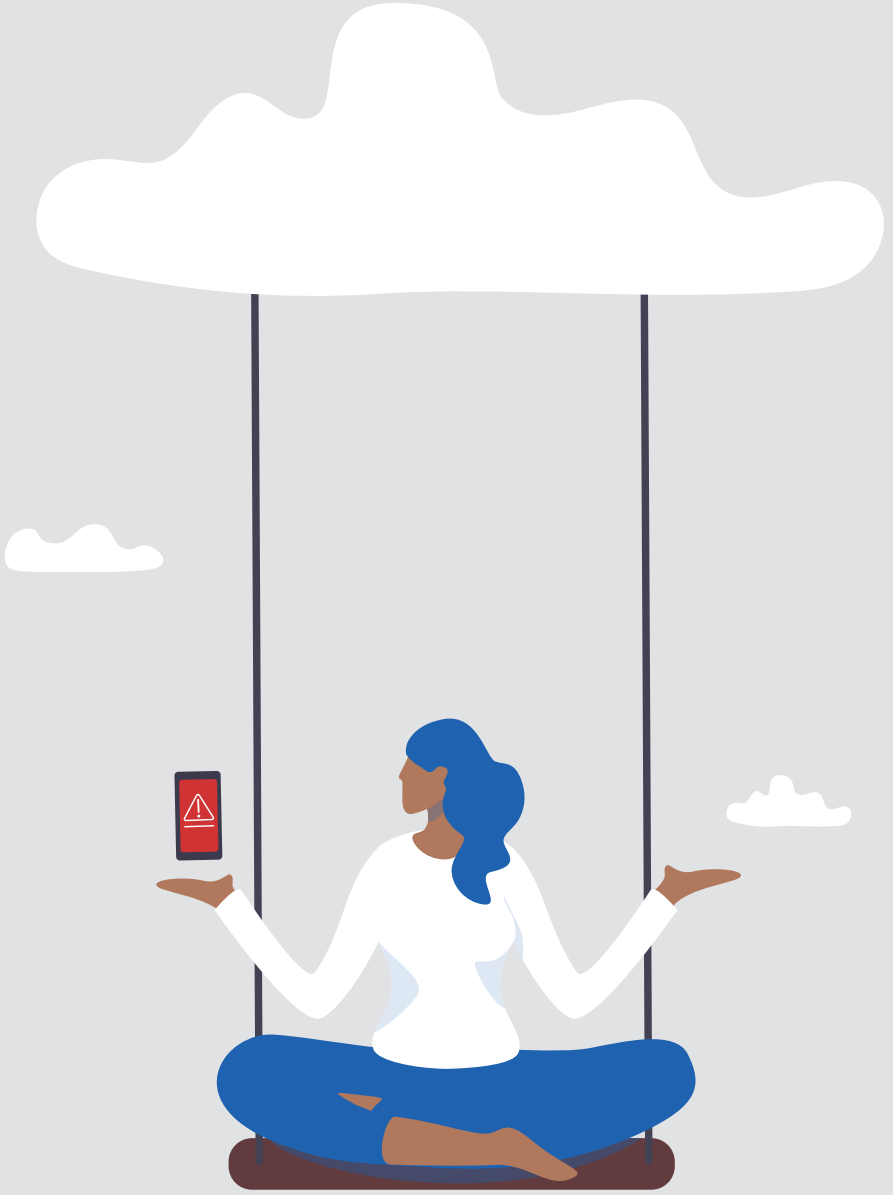
En este caso, el atacante se hizo pasar por un exempleado que ahora trabaja en una organización asociada que necesitaba que se procesara su pago. Este mensaje, enviado al departamento financiero desde una cuenta de Gmail, superó los controles de seguridad de correo electrónico nativos de Microsoft.

A menudo, los ciberdelincuentes utilizan Gmail u otros servicios de correo electrónico gratuitos cuando intentan este tipo de fraude. Esto se debe a que les ayuda a eludir las comprobaciones de autenticación de correo electrónico, como Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM). Los atacantes también pueden enviar URL o archivos adjuntos maliciosos para ayudarles a obtener acceso a información financiera u otros datos de alto valor.

SECCIÓN 2

ATAQUES POR TELÉFONO O TOAD

En un ataque por teléfono (TOAD), un objetivo recibe un mensaje que generalmente contiene una factura o una alerta falsa. El mensaje también incluye un número de servicio al cliente al que pueden llamar para hacer preguntas o corregir un error. Si la víctima llama al número, se encuentra al ciberdelincuente al otro lado de la línea. En su punto máximo, Proofpoint observó que se enviaron más de 13 millones de mensajes TOAD al mes en 2022. Esta cifra ha estado aumentando constantemente desde que apareció esta técnica por primera vez en 2021[3].



Entorno:
Microsoft 365

Categoría de amenaza:
ingeniería social

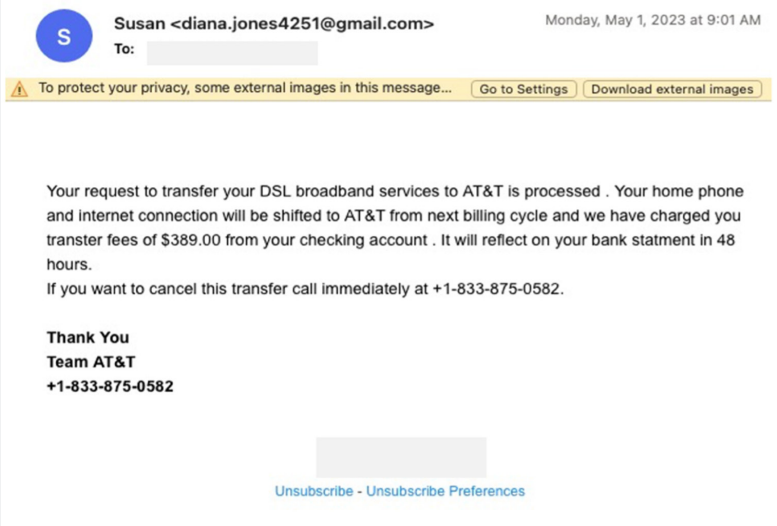
Tipo de ataque:
TOAD

Objetivo:
usuario de Microsoft 365

Amenazas TOAD

El fraude por correo electrónico respaldado por agentes de servicio al cliente de centros de llamadas es prolífico y lucrativo. En muchos casos, las víctimas pierden decenas de miles de dólares robados directamente de sus cuentas bancarias. Entre 2021 y 2022, se informó de que 68,4 millones de estadounidenses perdieron 39 500 millones de dólares en ataques de fraude telefónico[4].

Hay dos tipos de actividad de amenazas de centros de llamadas que Proofpoint observa regularmente. Uno utiliza software de asistencia remota gratuito y legítimo para robar dinero. El segundo utiliza malware disfrazado como un documento para comprometer un equipo y puede llevar a la instalación de malware adicional.



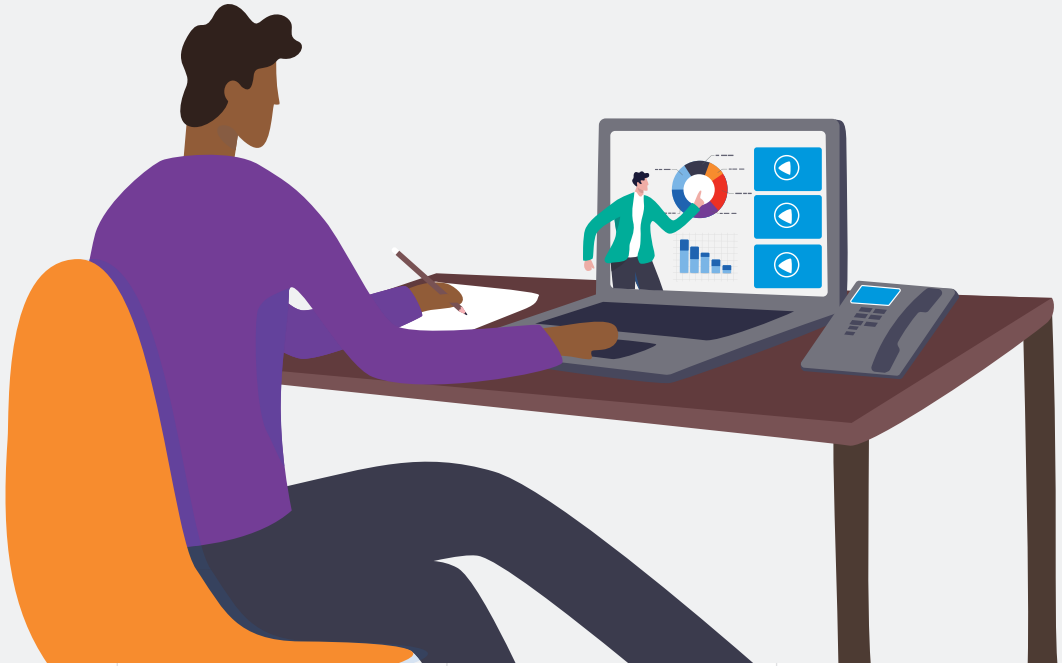
Ejemplo de ataque TOAD.

4 Truecaller. U.S. Spam & Scam Report (Informe sobre spam y estafas en EE. UU.). 2022.

En un ataque típico de centro de llamadas, un usuario recibe un mensaje que debe ser atendido con urgencia, como el mensajes de correo electrónico anterior. A menudo, el mensaje incluye algún tipo de recibo por una compra grande y parece enviado por una empresa legítima. Se instruye al destinatario que llame a un número en el correo electrónico para cancelar la transacción o disputar su compra.

Si el usuario llama al número de teléfono del mensaje, un representante de servicio al cliente guiará verbalmente al usuario para que visite un sitio web o una tienda de aplicaciones móviles. Los investigadores de Proofpoint han visto una variedad de pasos siguientes, que incluyen guiar a las víctimas para descargar malware, transferir dinero o habilitar el acceso remoto.

Microsoft no detecta estos mensajes porque no incluyen cargas útiles (payloads) o URL maliciosas.



SECCIÓN 3

CARGAS MALICIOSAS EN ARCHIVOS COMPARTIDOS

Los ataques mediante cargas maliciosas en archivos compartidos son uno de los tipos más comunes de ataques basados en URL. Los datos internos de amenazas de Proofpoint muestran que las URL representan tres cuartos del conjunto de ciberamenazas. Además, las URL de uso compartido de archivos se utilizan en más del 50 % de estos ataques.

Dado que los usuarios confían de forma inherente y utilizan servicios como Microsoft OneDrive y Microsoft SharePoint, los ciberdelincuentes suelen utilizar estos enlaces. Microsoft se encuentra en una posición única en lo que respecta a estos ataques, ya que no solo alberga inadvertidamente estos archivos maliciosos, sino que también les permite pasar a través de sus soluciones de seguridad de correo electrónico.

En 2021, descubrimos que más de 45 millones de amenazas basadas en URL enviadas a nuestros clientes incluían contenido malicioso alojado por Microsoft.

Entorno:
Microsoft 365

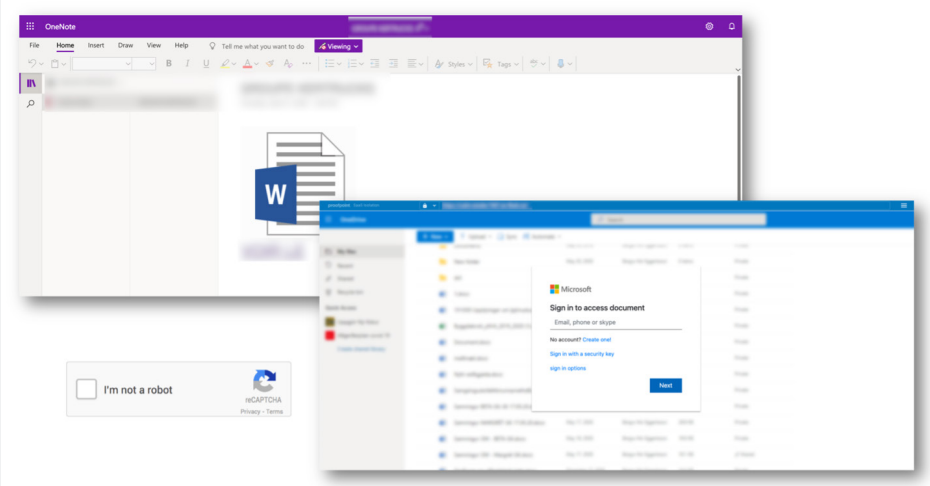
Categoría de amenaza:
uso compartido de archivos basada en URL

Tipo de ataque:
phishing de credenciales

Objetivo:
buzón de correo compartido

Phishing de credenciales de OneNote

Los ciberdelincuentes han aumentado su uso de CAPTCHA 50 veces año tras año, según los datos de Proofpoint[5]. En estos ataques, los actores maliciosos intentan robar las credenciales de usuario enviándoles enlaces a documentos falsos. Cuando los usuarios hacen clic en estos enlaces, se les muestra un CAPTCHA. Después de marcar la casilla CAPTCHA, se les dirige a una página falsa de Microsoft donde se les pide que introduzcan sus credenciales.



Un ejemplo de una página de Microsoft OneNote con un enlace a un falso documento de Word.

5 Proofpoint. Informe El factor humano. 2022.

En este ejemplo, un atacante se hizo pasar por un proveedor externo que estaba enviando una solicitud de trabajo al buzón compartido de una empresa de telecomunicaciones. El objetivo del atacante era que los usuarios del buzón entregaran sus credenciales al enviarles un enlace a un falso documento de Word que les presentaba un CAPTCHA. Enviado a través de OneDrive, el enlace a la página maliciosa eludió los controles de seguridad nativos de Microsoft.

Es sorprendente que incluso después de ser denunciada por Proofpoint, la página de OneDrive seguía activa un mes después. Este es solo uno de los millones de páginas de uso compartido de archivos abusadas que suplantan la marca Microsoft cada mes.

Entorno:
Microsoft 365

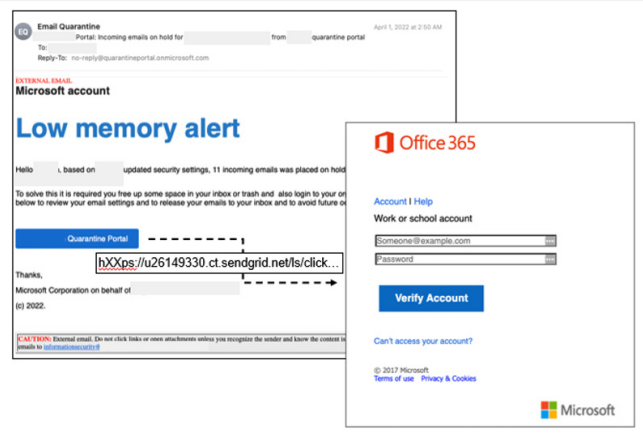
Categoría de amenaza:
abuso de servicios de nube legítimos

Tipo de ataque:
phishing de credenciales

Objetivo:
usuario de Microsoft 365

Phishing de credenciales para el abuso de servicios de nube legítimos

El robo de credenciales de Microsoft 365 es una táctica habitual que los ciberdelincuentes utilizan para intentar comprometer cuentas de los usuarios. Dentro de la cuenta de su víctima, los atacantes pueden obtener detalles que les permiten enviar mensajes muy convincentes. Como resultado, son capaces de robar datos valiosos y desviar fondos.



Un ejemplo de robo de credenciales que imita la marca Microsoft, alojado en un sitio de servicios en la nube legítimo.

En este ejemplo, el atacante utilizó SendGrid como host y envió su mensaje desde un dominio falsificado de Microsoft (onmicrosoft.com) para que pareciera legítimo. En la parte inferior del mensaje, incluso dieron la impresión de que Microsoft Corporation era un signatario en nombre de la organización.

Lo que destaca aquí es que cuando los ciberdelincuentes utilizan servicios en la nube legítimos, sus ataques a menudo pasan desapercibidos para Microsoft. La razón por lo consiguen se debe a la forma en que Microsoft gestiona los enlaces. Microsoft Safe Links no cuenta con análisis en entorno aislado (sandbox) predictivo en el momento en que los usuarios hacen clic. En su lugar, se basa en la reputación, lo que significa que es incapaz de detectar amenazas desconocidas que provienen de servicios legítimos en la nube y de intercambio de archivos.

SECCIÓN 4

USURPACIÓN DE CUENTAS

La usurpación de cuentas es una táctica utilizada habitualmente por los ciberdelincuentes. En estos ataques, un ciberdelincuente roba las credenciales de usuario para poder asumir la identidad corporativa de esa persona. Un solo conjunto de credenciales es muy valioso para los atacantes, ya que puede utilizarse para acceder al correo electrónico, al almacenamiento de documentos y a otros servicios de inicio de sesión único. Con ese nivel de acceso, los efectos de un ataque que tenga éxito pueden ser graves. En 2021[6], las organizaciones perdieron una media de 6,2 millones de dólares anuales debido a las intrusiones en cuentas de la nube. Y estos ataques van en aumento. En 2022, Verizon descubrió que el robo de credenciales tuvo lugar en el 76 % de los ataques de ingeniería social[7].

6 Ponemon Institute. Informe de Ponemon: "Cost of Cloud Compromise and Shadow IT" Coste del compromiso de cuentas cloud y las shadow IT), 2021.
7 Verizon. "Data BreachInvestigation Report" (Informe sobre las investigaciones de fugas de datos), 2023.

Entorno:
Microsoft 365

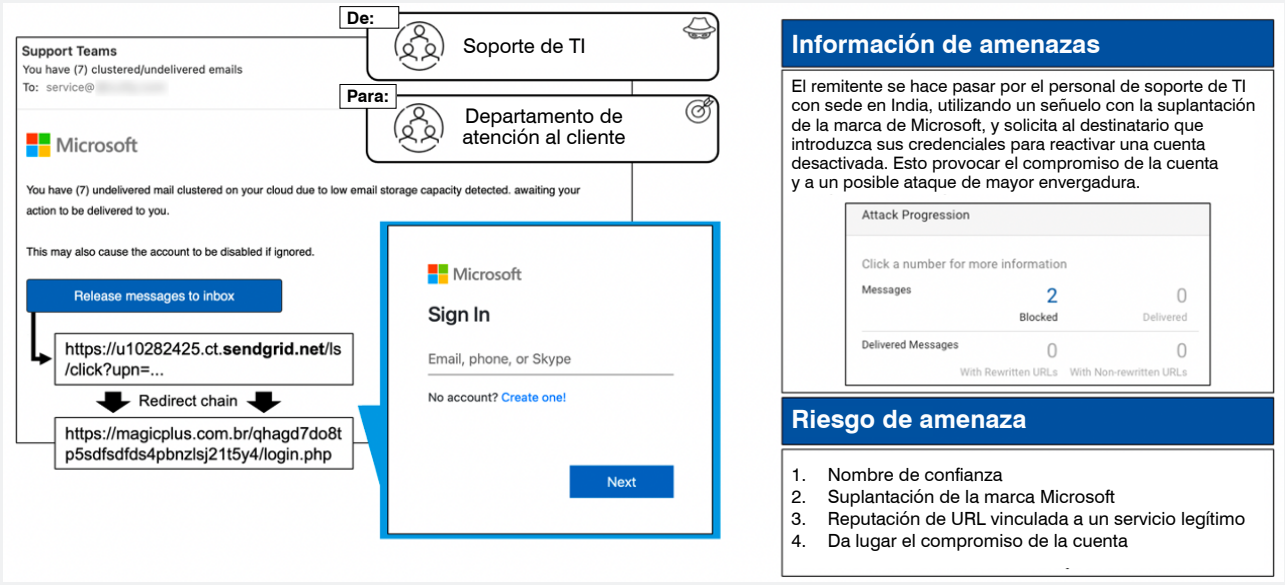
Categoría de amenaza:
basada en URL

Tipo de ataque:
robo de credenciales

Objetivo:
departamento de atención al cliente

Ataque de recopilación de credenciales contra Microsoft 365

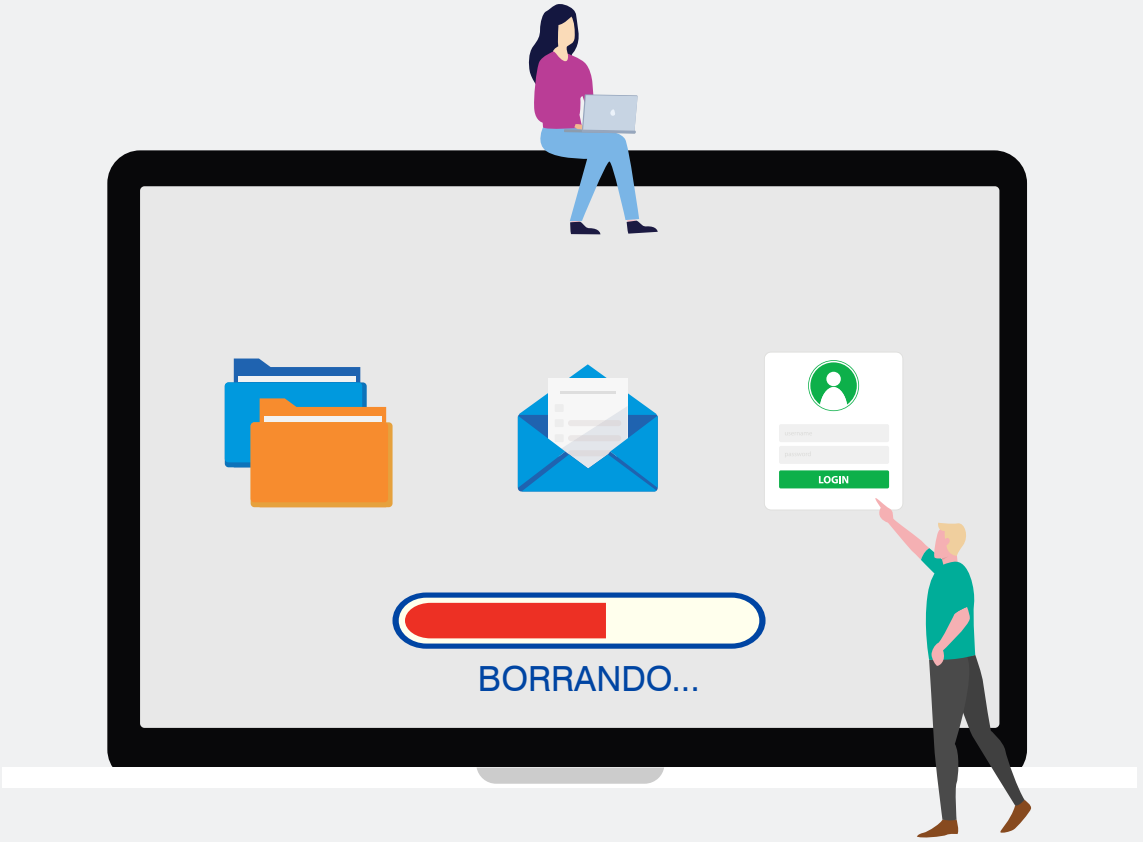
Muchos de los ataques de credenciales utilizan la misma táctica: imitan a Microsoft para superar las defensas perimetrales nativas de Microsoft. Abusar de la familiaridad y la confianza en las principales marcas es una de las formas más simples de ingeniería social. Microsoft es el favorito indiscutible cuando se trata de abuso de marcas. La investigación de Proofpoint muestra que Microsoft ocupó cuatro de las cinco primeras posiciones de las marcas más abusadas en todas las amenazas en 2022[8].



Un ejemplo de un intento de robo de credenciales.

8 Proofpoint. Informe El factor humano. 2023.

Este intento de robar credenciales eludió los controles de seguridad del correo electrónico nativos de Microsoft. El atacante envió un mensaje a un empleado del centro de atención al cliente haciéndose pasar por un miembro del personal de soporte de TI. Para parecer legítimo, el mensaje del atacante incluía un nombre reconocible y la marca de Microsoft. Proofpoint observa a menudo a ciberdelincuentes que utilizan una URL legítima (en este caso, sendgrid.net) para eludir las defensas de análisis de URL de Microsoft.



Entorno:
Microsoft 365

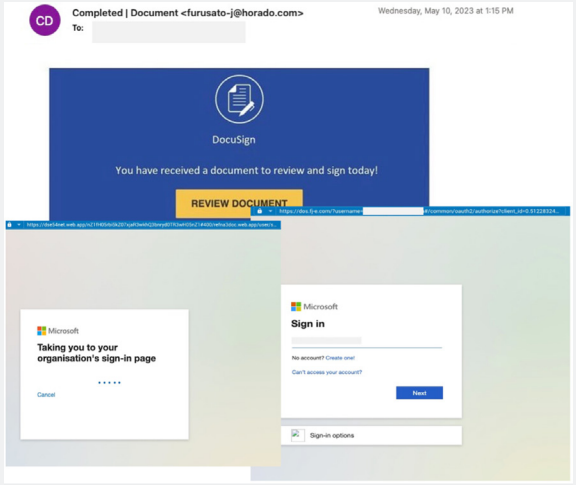
Categoría de amenaza:
recopilación de credenciales de MFA

Tipo de ataque:
phishing de credenciales

Objetivo:
usuario de Microsoft 365

Phishing habilitado para MFA

La autenticación multifactor (MFA) ya no puede considerarse como una garantía para detener la suplantación de cuentas. Los atacantes son cada vez más hábiles para eludirla. En su punto álgido, la investigación de Proofpoint encontró que las técnicas de elusión de la autenticación multifactor generaron más de un millón de mensajes al mes en 2022[9].



Ejemplo de phishing habilitado con MFA con una URL que redirige a una página de inicio de sesión de Microsoft falsa.

Este ataque eludió los controles de seguridad nativos de Microsoft al parecerse a una página de DocuSign con un enlace para la firma del usuario. En lugar de llevar al usuario a DocuSign, la URL redirige a una página de inicio de sesión falsa de Microsoft.

Para llevar a cabo este ataque, el atacante utilizó EvilProxy, que es un marco de phishing que utiliza un proxy inverso para personalizar las páginas de destino para cada destinatario y recopilar credenciales, eludiendo la protección de MFA. Este kit es relativamente nuevo y está disponible para la venta en foros de exploits. Una vez que se recopilan las credenciales MFA, proporciona acceso persistente a una cuenta incluso con un restablecimiento de contraseña.

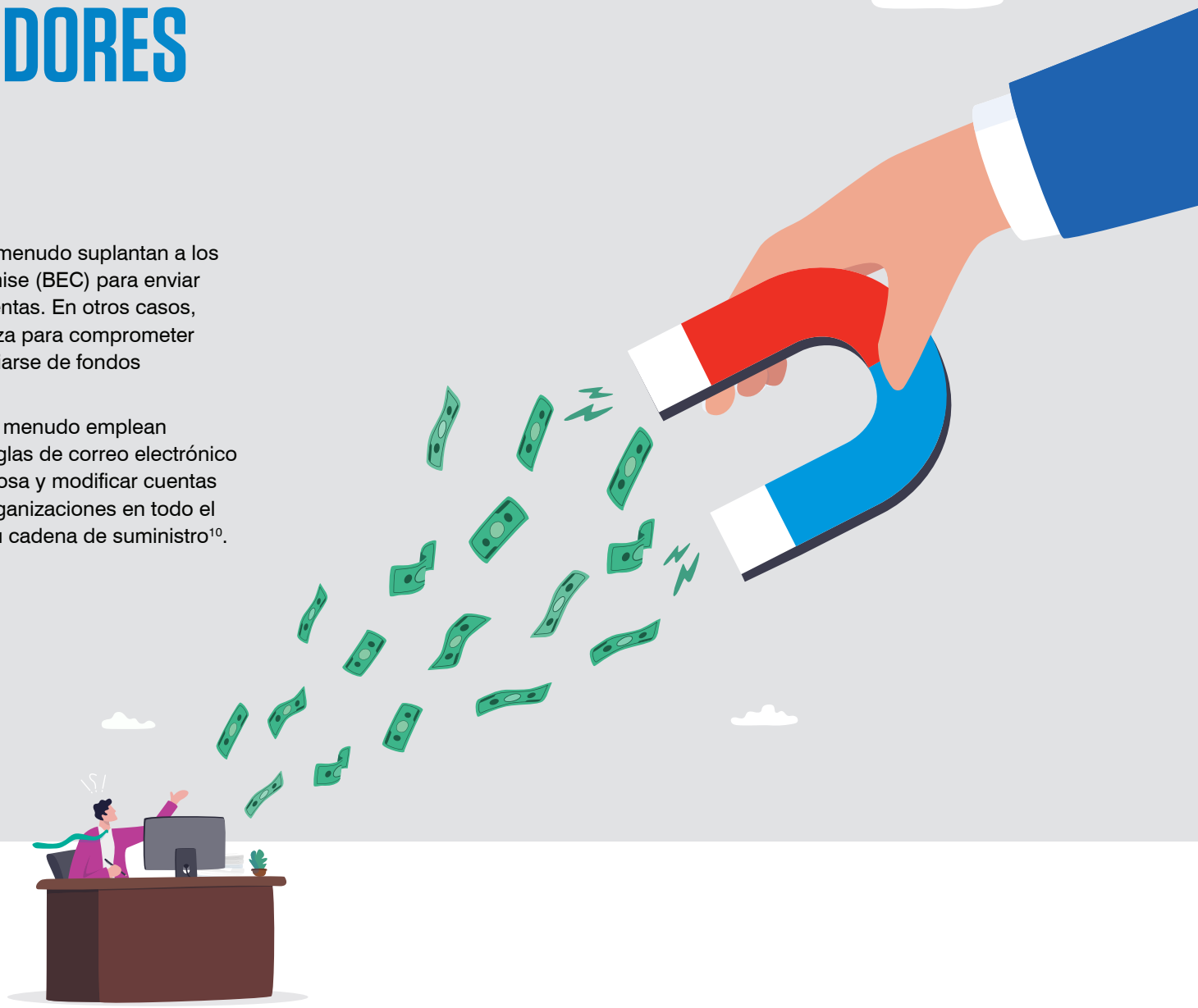
9 Proofpoint. Informe El factor humano. 2023.

SECCIÓN 5

CUENTAS DE PROVEEDORES COMPROMETIDAS

Como mencionamos anteriormente, los ciberdelincuentes a menudo suplantan a los proveedores cuando idean estafas Business Email Compromise (BEC) para enviar facturas fraudulentas o modificar los detalles de pago de cuentas. En otros casos, los atacantes se dirigen a proveedores y terceros de confianza para comprometer las cuentas de sus empleados, con el objetivo final de apropiarse de fondos y datos sensibles.

Una vez que logran introducirse en su red, estos atacantes a menudo emplean diversas tácticas para ocultar sus actividades, como crear reglas de correo electrónico para ocultar sus huellas, acceder a propiedad intelectual valiosa y modificar cuentas de pago, entre otras. En 2022, un asombroso 69 % de las organizaciones en todo el mundo experimentaron ciberataques que se originaron en su cadena de suministro[10].



10 Proofpoint. Informe State of the Phish. 2023.

Entorno:
Microsoft 365

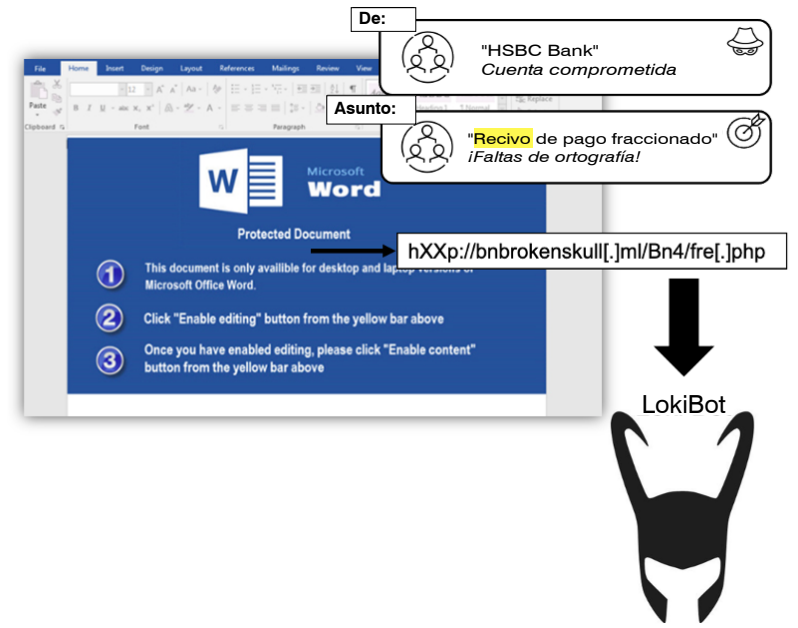
Categoría de amenaza:
basada en URL

Tipo de ataque:
descargador

Objetivo:
escondido en copia de carbón oculta (CCO) del mensaje

Amenaza de adjunto malicioso

Una forma de infiltrarse en una red es mediante el uso de malware. Recientemente, Proofpoint realizó un análisis interno de los datos de casi 4600 empresas. Descubrimos que el 85 % de estas empresas experimentaron ataques de correo electrónico basados en proveedores durante un período de siete días que finalizó el 31 de enero de 2023. El malware estuvo presente en cerca del 13 % de estos ataques[11].



Un ejemplo de ataque de LokiBot.

11 Proofpoint. "Hidden Risk: How to Recognize and Prevent Supply Chain Attacks" (Riesgo oculto: cómo reconocer y prevenir los ataques a la cadena de suministro), abril de 2023.

Este ataque se envió desde una cuenta de correo electrónico comprometida de un banco mundial. Dentro del mensaje había un enlace a un documento de Word que explotaba varias vulnerabilidades del Editor de ecuaciones para descargar LokiBot, un bot que puede robar contraseñas de navegadores, aplicaciones FTP/SSH y cuentas de correo electrónico.

Microsoft no detectó este ataque porque el mensaje se envió desde un dominio legítimo, por lo que el análisis de reputación estática no lo identificó como malicioso. El mensaje también superó la autenticación SPF. Además, la carga maliciosa utilizó técnicas de evasión de entorno aislado (sandbox) y de ocultación.

Entorno:
Microsoft 365

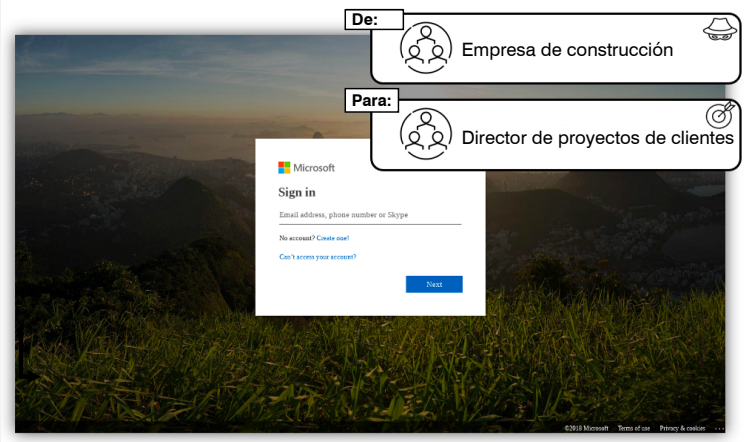
Categoría de amenaza:
basada en URL

Tipo de ataque:
phishing de credenciales

Objetivo:
director de proyectos de clientes

Amenaza de phishing de credenciales

Los actores de amenazas también abusan de las cuentas de proveedores comprometidas para robar las credenciales de usuario. Y en estos casos, el resultado puede ser aún más perjudicial. Desafortunadamente, los usuarios a menudo interactúan libremente con estas amenazas porque, incluso después de una inspección minuciosa, estos mensajes parecen legítimos al provenir de un dominio legítimo.



Esta página de credenciales imita un inicio de sesión de Microsoft 365.

El ataque anterior fue enviado desde una cuenta comprometida que pertenece a una empresa de construcción legítima. Esta cuenta envía regularmente mensajes de correo electrónico a un director de proyecto que es uno de sus clientes. El correo electrónico malicioso contenía una URL que enlazaba a una página que imitaba la marca de Microsoft con el fin de recopilar credenciales de Microsoft 365.

Esta amenaza fue entregada en la bandeja de entrada del director de proyecto por varias razones. En primer lugar, el análisis de reputación de Microsoft a menudo no detecta nuevas URL maliciosas, incluso cuando se hacen pasar por la marca de Microsoft. Además, el mensaje se envió desde el dominio legítimo de un proveedor, por lo que el análisis de reputación estática de Microsoft no identificaría al remitente como malicioso. El sobre no activó casos obvios de suplantación.

Entorno:
Microsoft 365

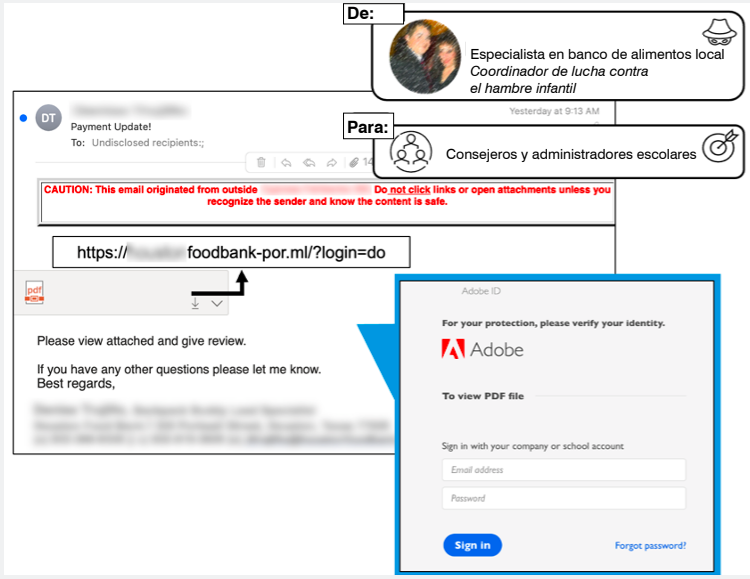
Categoría de amenaza:
basada en adjunto, con una amenaza basada en URL

Tipo de ataque:
phishing de credenciales

Objetivo:
consejeros y administradores escolares

Ataque con URL incrustada

No todos los actores de amenazas se centran en Microsoft 365. Con el crecimiento de las aplicaciones en la nube, a menudo es más fácil abusar de las cuentas cloud que tienen menos protección que Microsoft 365. Para aumentar la probabilidad de que su víctima active un ataque, un ciberdelincuente enviará un mensaje desde la cuenta comprometida de un partner.



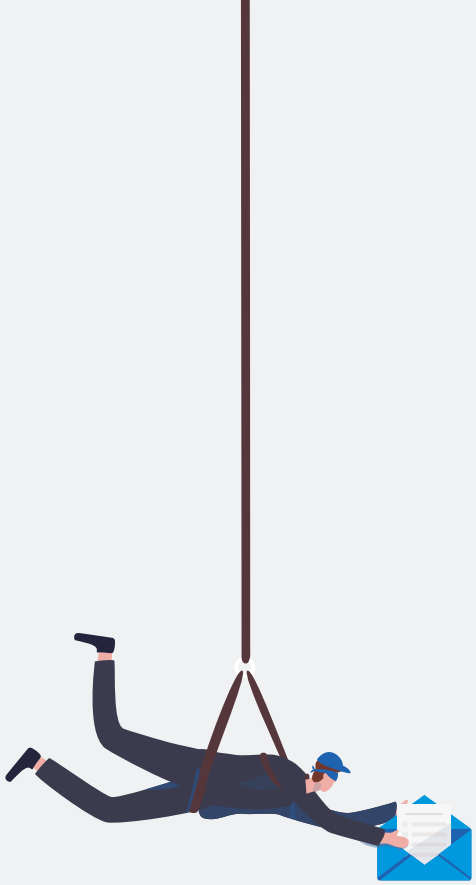
Información de amenazas

El ataque de phishing se envió desde una cuenta de partner comprometida y tenía como objetivo establecer una relación de confianza para engañar a los destinatarios y hacer que divulgaran sus credenciales, con el posible riesgo de pérdida de datos.

Riesgo de amenaza

1. Enviado desde partner comprometido
2. Autentificación SPF/DKIM superada
3. Nombre de confianza con correspondencia regular
4. Da lugar el compromiso de la cuenta

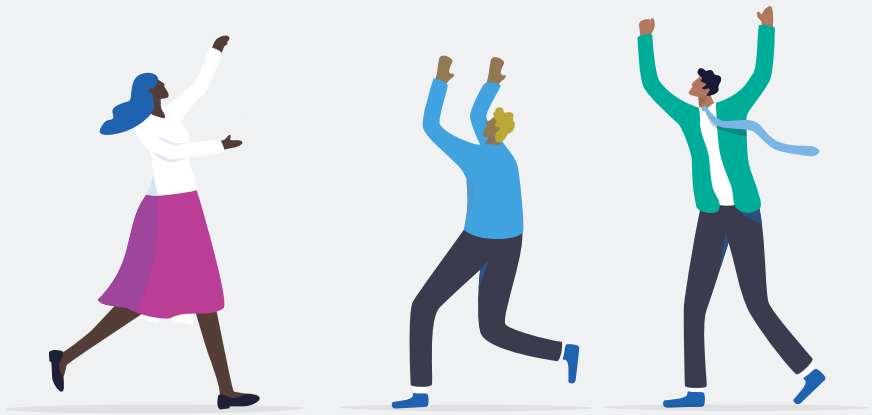
Esta página de credenciales imita el inicio de sesión de software de Adobe.



Este ataque de robo de credenciales se envió desde la cuenta comprometida de un partner legítimo con el que el usuario se comunica regularmente. Como se muestra, un enlace dentro del mensaje envía al usuario a una página que imita la marca de Adobe en un intento de obtener las credenciales de software del usuario.

Microsoft no detuvo el ataque por varias razones. En primer lugar, se envió desde la cuenta de un partner legítimo, por lo que pasó la autenticación SPF/DKIM. Y debido a que había correspondencia regular con esta cuenta, se consideraba un nombre de confianza, por lo que pasó la puntuación de reputación estática de Microsoft.

Además, el ciberdelincuente pudo evadir el sandboxing al colocar la payload (URL) dentro del archivo adjunto y no en mensaje de correo electrónico en sí. La URL no fue detectada por el análisis de reputación de Microsoft, que puede pasar por alto nuevas URL maliciosas.



Entorno:
Microsoft 365

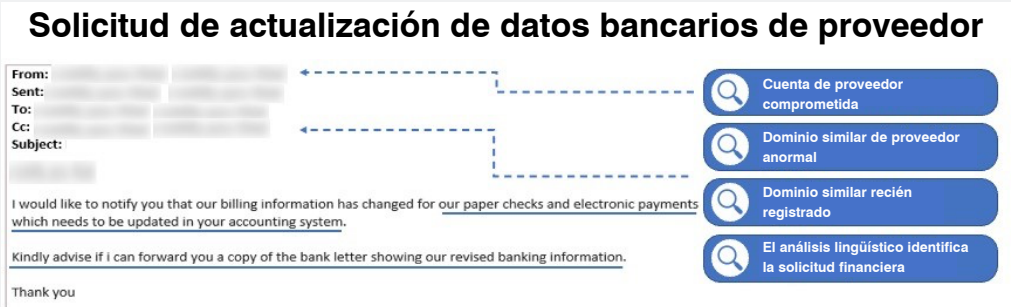
Categoría de amenaza:
ingeniería social, cuentas de proveedores comprometidas

Tipo de ataque:
fraude de facturas

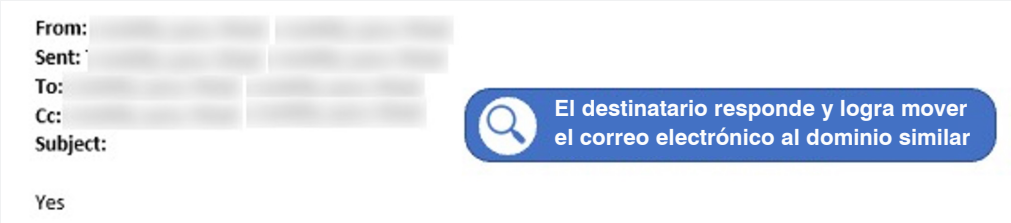
Objetivo:
responsables de cuentas

Amenaza de suplantación de proveedores

Las personas tienen más probabilidades de responder a un mensaje de correo electrónico malicioso cuando parece provenir de alguien que conocen. Cuando uno de estos ataques se envía desde un proveedor aparentemente legítimo, se vuelve aún más peligroso.



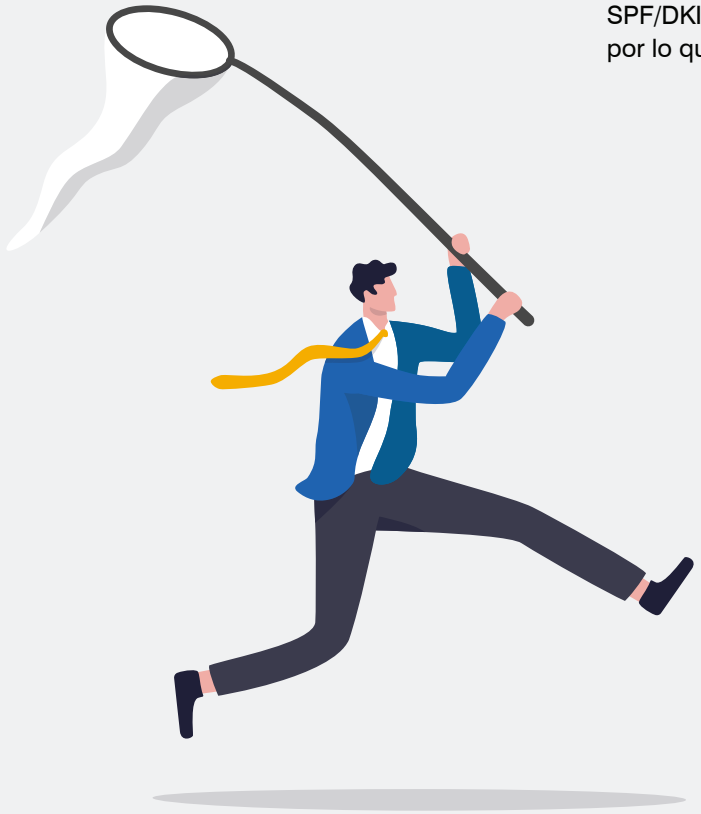
Este fue el mensaje de correo electrónico inicial del atacante.



Esta fue la respuesta del cliente, que se envió a un dominio falso.

El mensaje inicial fue recibido por un minorista mundial desde la cuenta de un proveedor legítimo. El remitente solicitó 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. El atacante intentaba redirigir los mensajes de correo electrónico de respuesta a un dominio similar recién registrado con el objetivo de interceptar información confidencial y desviar fondos.

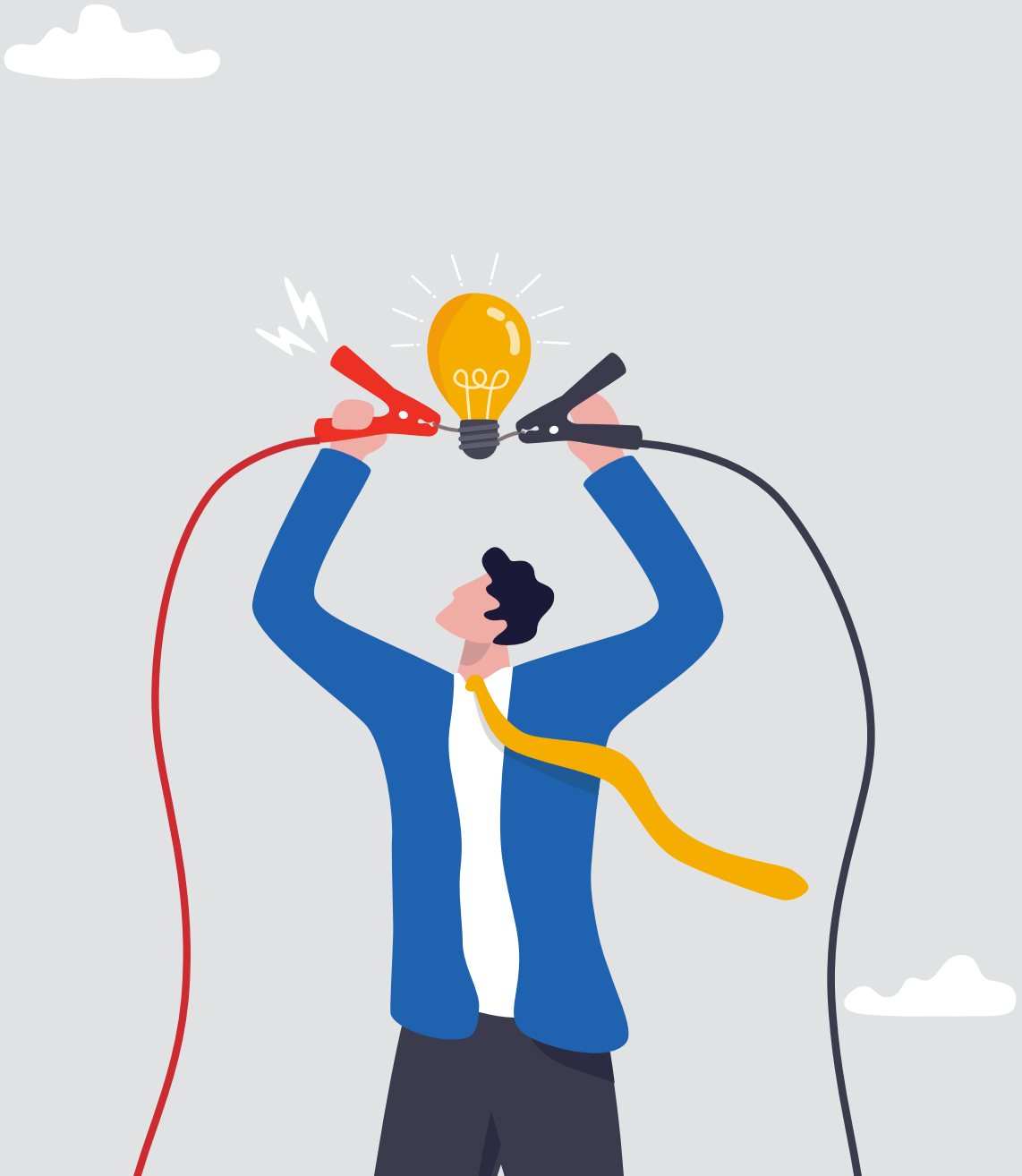
Microsoft no detuvo esta amenaza porque fue enviada por un cliente legítimo, por lo que pasó la autenticación SPF/DKIM. Y debido a que había correspondencia regular con esta cuenta, se consideraba un nombre de confianza, por lo que pasó la puntuación de reputación estática de Microsoft.



CONCLUSIÓN

Cuando se trata de mantener segura su organización, las funciones de seguridad integradas de Microsoft 365 son un buen punto de partida. Sin embargo, a medida que las amenazas se multiplican y evolucionan, necesita otras capas de seguridad.

Los ciberdelincuentes ya no dependen de técnicas aisladas. En cambio, combinan y mezclan tácticas avanzadas para explotar a las personas. También buscan relaciones que puedan utilizar, la confianza que puedan aprovechar y el acceso que puedan explotar. Es por eso que detenerlos requiere un enfoque multicapa centrado en las personas que abarque toda la cadena de ataque.
Para obtener más información sobre cómo puede Proofpoint mejorar la seguridad nativa de Microsoft 365 y proteger a sus empleados de los ciberataques avanzados, visite proofpoint.com/es.

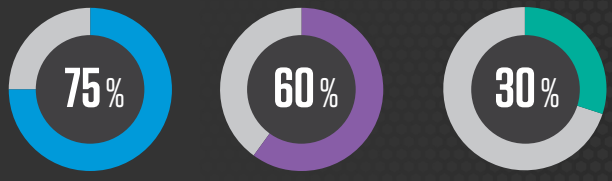


Por qué Proofpoint

A diario, analizamos más de:

2600 MILLONES DE MENSAJES DE CORREO	**49 000 MILLONES** DE URL	**1900 MILLONES** DE ADJUNTOS
1700 MILLONES DE MENSAJES DE MÓVIL	**430 MILLONES** DE DOMINIOS WEB	**143 000** CUENTAS DE REDES SOCIALES

Confían en nosotros más de:



DEL FORTUNE 100 | DEL FORTUNE 1000 | DEL FORTUNE GLOBAL 2000

8000 GRANDES EMPRESAS

200 000 PEQUEÑAS EMPRESAS

MÁS INFORMACIÓN

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