proofpoint.

LIBRO ELECTRÓNICO

5 ataques reales y cómo neutralizarlos

Vol. 2: ataques técnicos

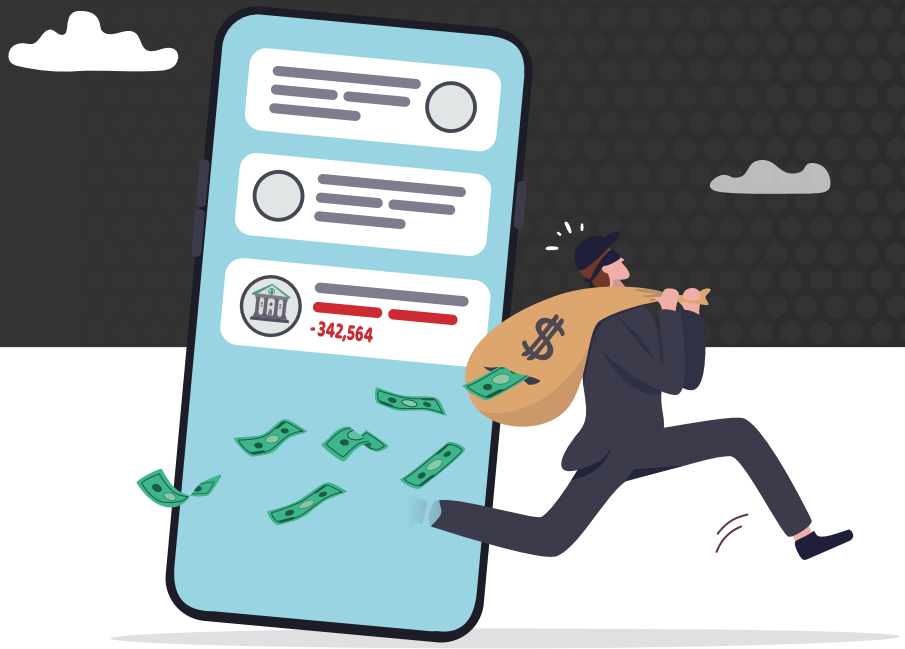
Introducción

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.

En el volumen 1, analizamos los ataques mediante ingeniería social. Este volumen cubre 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

Toolkit de phishing EvilProxy

EvilProxy es un kit de herramientas de phishing que puede robar credenciales de usuario y tokens de autenticación multifactor (MFA).

Se oculta detrás una página web legítima para actuar. Cuando el usuario se conecta a una página de phishing, se le presenta una página de inicio de sesión falsa que parece y actúa como un portal de inicio de sesión real. EvilProxy captura entonces las credenciales del usuario y el token de sesión de autenticación. El ciberdelincuente puede utilizar esta información para saltarse las protecciones MFA y conectarse en nombre del usuario.

EvilProxy y otras amenazas que eluden la MFA son cada vez más frecuentes a medida que los ciberdelincuentes se adaptan a las mejoras de controles de seguridad. Los métodos tradicionales, como la reputación de IP o URL, no bastan para detener estas amenazas.

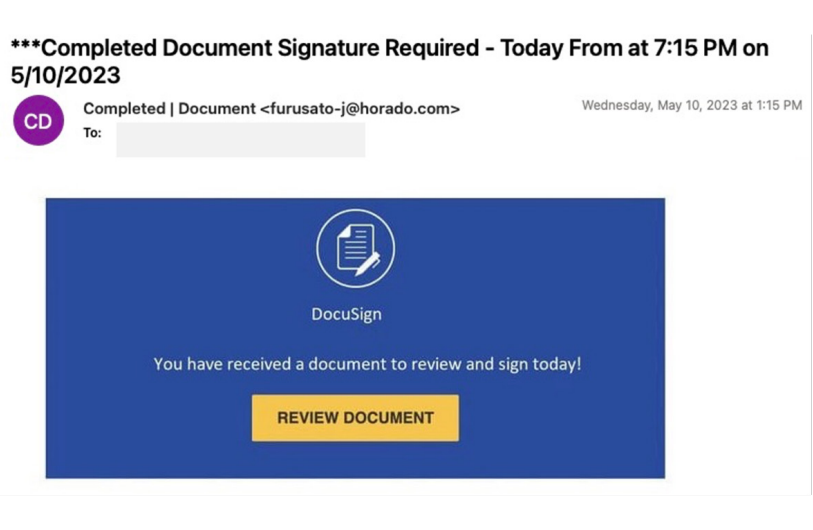
La situación

Durante una de nuestras recientes evaluaciones de amenazas asociadas al correo electrónico, descubrimos que un empresa tecnológica con 1500 clientes había estado expuesta a EvilProxy. La solución de seguridad de correo electrónico existente no había sido capaz de detectar esta amenaza.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

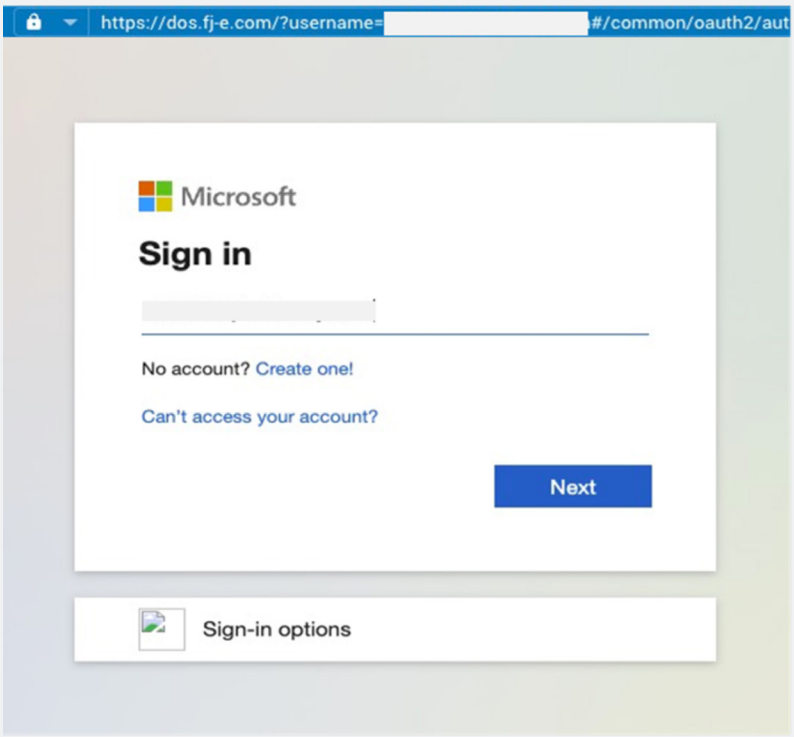
1. **El mensaje engañoso.** El ataque comenzó con un mensaje de correo electrónico que parecía un aviso legítimo de DocuSign. Informaba a los destinatarios que había un documento listo para firmar. Este mensaje aparentemente inofensivo era en realidad la puerta de entrada a un sofisticado ciberataque.



El correo electrónico engañoso inicial recibido por el cliente.

2. **La URL maliciosa.** Cuando los destinatarios hacían clic en la URL incrustada, se les dirigía a su propia página de inicio de sesión de Microsoft, en la que se había configurado el proxy del ciberdelincuente. En esta página es donde el atacante intentaba conseguir que los usuarios introdujeran sus credenciales.

3. **El marco de phishing EvilProxy.** El marco de phishing EvilProxy fue el catalizador de este ataque. Los atacantes emplearon una técnica de proxy inverso para interceptar los intentos de inicio de sesión de los usuarios a través de la página de inicio de sesión real de Microsoft. De este modo extraían en secreto los códigos MFA y las credenciales de usuario.



La página maliciosa de inicio de sesión de Microsoft.

4. **Socavamiento de la verificación MFA.** Con los códigos MFA y las credenciales de inicio de sesión del usuario en su poder, los ciberdelincuentes obtuvieron libre acceso a las cuentas comprometidas. Como pudieron eludir la verificación MFA, pudieron acceder al entorno de la empresa.

Cómo detectó Proofpoint el ataque

Proofpoint utiliza el aprendizaje automático para descifrar el contexto de los mensajes entrantes y analizar su lenguaje para detectar posibles amenazas. Determinamos si un mensaje de correo electrónico es inofensivo, malicioso o sospechoso analizando el cuerpo del mensaje y el contexto. También examinamos el comportamiento habitual de envío del remitente. Si el mensaje tiene payloads sospechosas, Proofpoint lo envía a un entorno aislado (sandbox) para realizar una análisis en profundidad. Esto nos ayuda a detectar contenido malicioso, incluso si nunca se ha visto antes.

En este caso, Proofpoint concluyó que el mensaje era sospechoso por varias razones. Para empezar, el destinatario no solía recibir mensajes de correo electrónico de ese remitente. Además, el remitente pedía al destinatario que realizara una acción (hacer clic en la URL). Como inicialmente no podíamos determinar si la URL era inofensiva o maliciosa, la analizamos de forma preventiva en un entorno aislado.

Al seguir la URL, descubrimos que utilizaba una táctica de redireccionamiento para ocultar su naturaleza maliciosa. Nuestro motor de análisis de URL descubrió que dirigía a una página web muy parecida a una página de inicio de sesión de Microsoft. Teniendo en cuenta el comportamiento de esta página web, Proofpoint detectó un marco de URL que utilizaba un servicio proxy para robar las credenciales de inicio de sesión de los usuarios y las respuestas MFA en tiempo real. Estas características coincidían con EvilProxy. Al interceptar las credenciales de inicio de sesión y la respuesta a un desafío MFA en tiempo real, los ciberdelincuentes pueden acceder rápidamente a la cuenta de un usuario, incluso si la protección MFA está activada.

Malicious URLs

Credential phish caught by machine learning engine

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	dc890227-7740-11e9-8d93-12ba71d80a0c

phishing url

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	2930c017-0415-11eb-bab7-12ba71d80a0c

Detected by rule e7461bcaf73c18c64b12ed7fbb7283e6

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	behavior_e7461bcaf73c18c64b12ed7fbb7283e6

Redirect Chain

A URL with multiple redirects was visited

URL	https://doc.yg-r.com/?username=redacted_email&auth=1-0.79432671181593

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

Behaviors

Malicious content dropped during execution

Rule	behavior_d27be4c0bb9ef4dc79fb5309c19e5b3d

ETPRO Suricata IDS Alerts

Rule	behavior_28f6b6c79e0dc5b5fc7664b918b773caa

SocGholish redirect domain: trademark.jglesiaclarea.com

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0b76

SocGholish compromised script detected: http://jc.efleasing.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0676

Detección del marco de phishing EvilProxy en Proofpoint.

SECCIÓN 2

Ataque SocGholish

Observada por primera vez en circulación allá por 2018, SocGholish es una variante de malware que sigue causando estragos. Utiliza una amplia variedad de fases, comprobaciones de elegibilidad y rutinas de ofuscación, lo que la convierte en una de las familias de malware más escurridizas hasta la fecha. La ausencia de detalles sobre la selección de objetivos, la lógica de evasión y los procedimientos específicos de las fases intermedias contribuyen al misterio que la rodea.

Observamos cuatro fases básicas:

Fase 1: Inyecciones maliciosas
Un ciberdelincuente compromete un sitio web legítimo e inyecta un script JavaScript malicioso que realiza un perfil de los usuarios para identificar objetivos de ataque.

Fase 2: Descarga de SocGholish
Si un usuario cumple ciertos criterios, el script JavaScript introduce de manera furtiva SocGholish, que suele parecer una falsa actualización del navegador. Si el usuario hace clic en él, SocGholish se descarga en su dispositivo.

Fase 3: Mando y control
A continuación, el malware se comunica con proxies de mando y control para obtener más instrucciones.

Fase 4: Distribución de malware secundario e infección
SocGholish sigue analizando el dispositivo del usuario y a continuación se comunica con servidores de mando y control para distribuir malware secundario, por lo general troyanos de acceso remoto o ransomware.

Es difícil defenderse de SocGholish. La amenaza está muy extendida y puede eludir las herramientas de protección de correo electrónico más avanzadas. En un solo mes de 2023, Proofpoint detectó miles de instancias de SocGholish que habían escapado a otras capas de seguridad en todo el mundo.

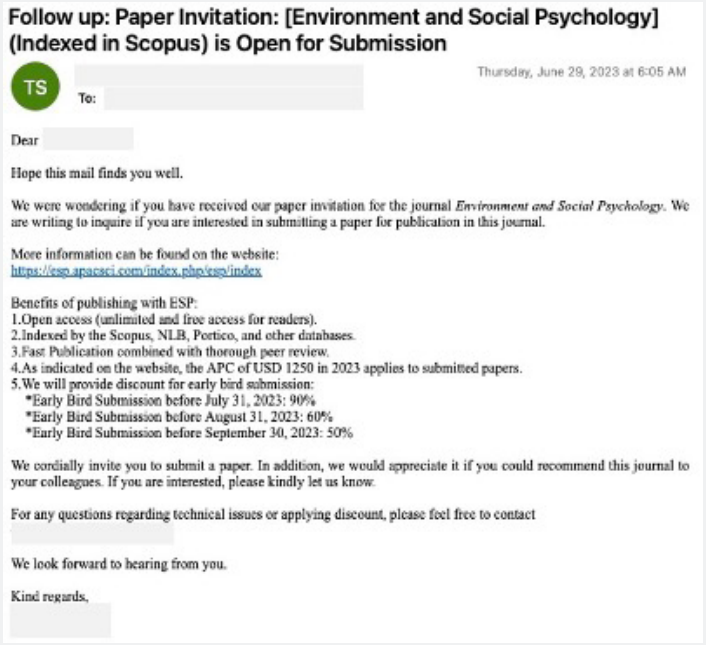
La situación

Durante una de nuestras recientes evaluaciones de amenazas asociadas al correo electrónico, descubrimos que una empresa tecnológica con 4000 usuarios había estado expuesta a un ataque de SocGholish. La herramienta de seguridad del correo electrónico existente no había sido capaz de interceptar esta amenaza.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

1. **El mensaje inicial.** Los usuarios recibieron un correo electrónico en el que se les invitaba a enviar un artículo para su publicación en una prestigiosa revista especializada. El mensaje de correo electrónico en sí no era malicioso y no había sido creado por un ciberdelincuente. Como siempre ocurre con las campañas de SocGholish, el código malicioso no se manifestó hasta que el usuario llegó al sitio web comprometido pero legítimo.



Follow up: Paper Invitation: [Environment and Social Psychology] (Indexed in Scopus) is Open for Submission

TS

To:

Thursday, June 29, 2023 at 6:05 AM

Dear

Hope this mail finds you well.

We were wondering if you have received our paper invitation for the journal *Environment and Social Psychology*. We are writing to inquire if you are interested in submitting a paper for publication in this journal.

More information can be found on the website:
https://esp.apacsci.com/index.php/esp/index

Benefits of publishing with ESP:
1.Open access (unlimited and free access for readers).
2.Indexed by the Scopus, NLB, Portico, and other databases.
3.Fast Publication combined with thorough peer review.
4.As indicated on the website, the APC of USD 1250 in 2023 applies to submitted papers.
5.We will provide discount for early bird submission:
*Early Bird Submission before July 31, 2023: 90%
*Early Bird Submission before August 31, 2023: 60%
*Early Bird Submission before September 30, 2023: 50%

We cordially invite you to submit a paper. In addition, we would appreciate it if you could recommend this journal to your colleagues. If you are interested, please kindly let us know.

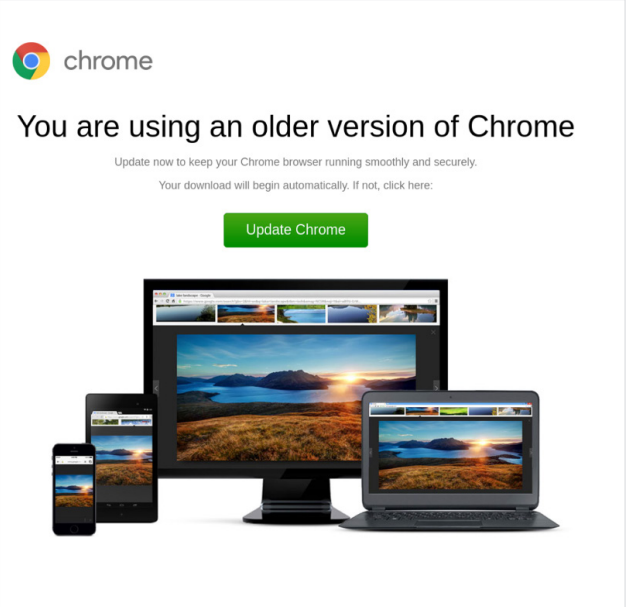
For any questions regarding technical issues or applying discount, please feel free to contact

We look forward to hearing from you.

Kind regards,

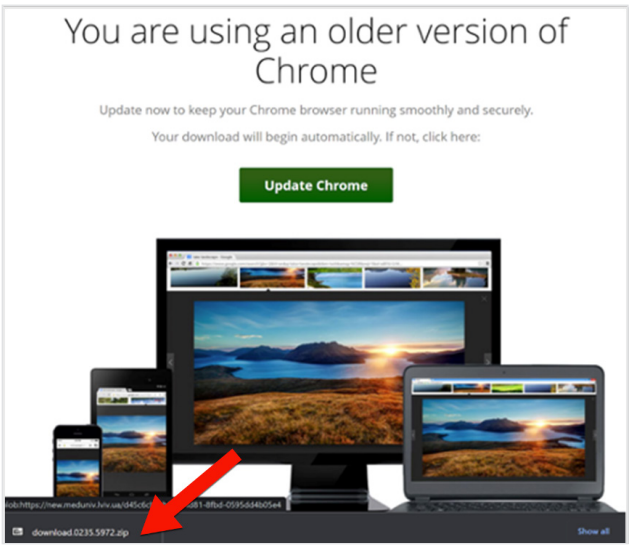
El mensaje de correo electrónico inicial recibido por nuestro cliente.

2. **La URL comprometida.** Si el usuario hacía clic en la URL del correo electrónico, el script JavaScript inyectado en el destino comenzaba a elaborar un perfil del usuario para determinar si era un objetivo de ataque. Aparecía una ventana emergente para los usuarios objetivo, informándoles de que era necesario actualizar su navegador.



La solicitud de actualización del navegador falsa.

3. **Instalación de SocGholish.** Si el usuario descargaba el paquete de actualización, SocGholish analizaba el dispositivo del usuario, su configuración y los elementos a los que tenía acceso.
A continuación, SocGholish se comunicaba con proxies de mando y control para obtener más instrucciones y determinar si era necesario instalar malware secundario.



El archivo descargado al iniciar una falsa actualización del navegador.

Por qué estas amenazas son difíciles de detectar

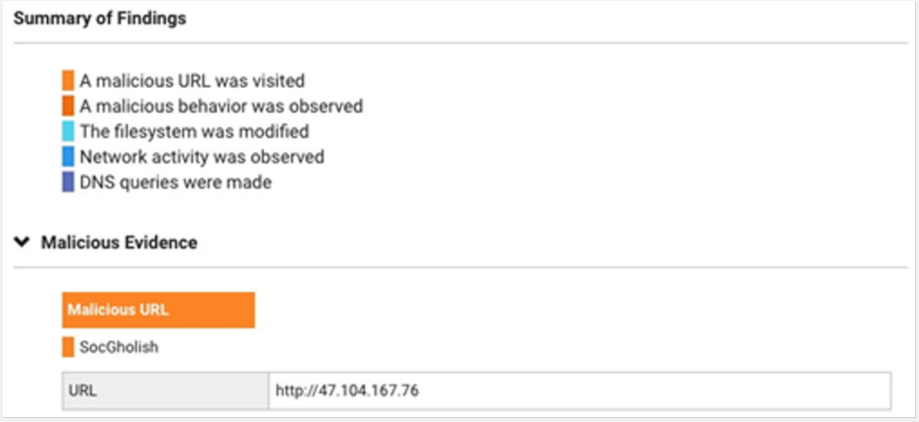
La mayoría de las herramientas de protección de correo electrónico pueden detectar JavaScript malicioso, pero SocGholish es escurridizo por naturaleza. Muchas soluciones de protección del correo electrónico tienen dificultades para detectar estas técnicas de elaboración de perfiles, en particular, la inspección de la dirección IP del dispositivo, el sistema operativo, el navegador y el idioma local. Además, las herramientas que se basan exclusivamente en la detección de anomalías tienen dificultades para detectar ataques como SocGholish, porque tanto el correo electrónico como la URL son legítimos.

SocGholish también utiliza tácticas de evasión capaces de detectar los entornos aislados. Por lo tanto, no se manifestará si detecta un entorno simulado, como el entorno aislado de un analista de amenazas. Además, las herramientas de protección del correo electrónico que aseguran analizar las amenazas mediante IA y aprendizaje automático también tienen problemas para detectar SocGholish, porque el correo electrónico en sí no es malicioso. El comportamiento previo de envío tampoco le identificaría como sospechoso.

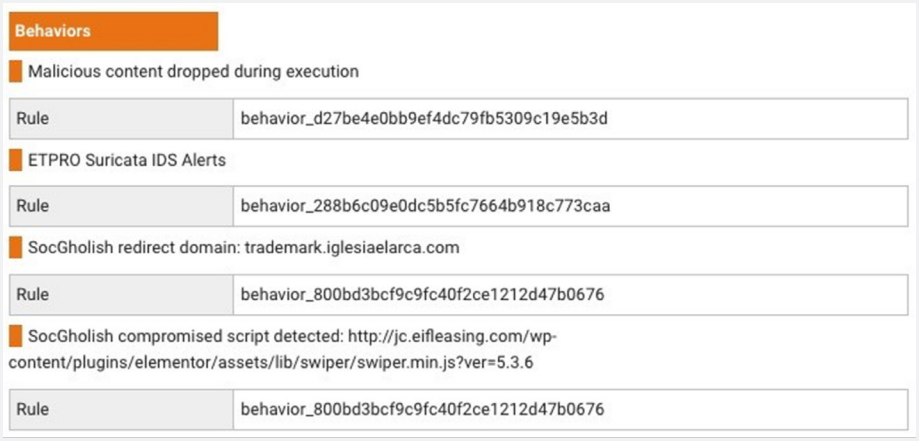
Cómo detectó Proofpoint el ataque

Proofpoint utiliza un análisis en profundidad del comportamiento de las URL para detectar una serie de comportamientos sospechosos asociados a SocGholish, como la elaboración de perfiles. Al analizar la actividad de la red, podemos ver que el malware se comunica con proxies de mando y control. También hemos identificado otra táctica utilizada por SocGholish: la redirección a un servicio DNS y la explotación de scripts comprometidos.

En este caso, Proofpoint detectó comportamientos de envío atípicos. Por lo tanto, analizamos las URL en un entorno aislado antes de que los usuarios hicieran clic en los enlaces. El análisis predictivo en entorno aislado de URL selectivas es una función específica de Proofpoint. Esta es una de las razones por las que podemos detectar amenazas basándonos en URL que nunca se han visto antes.



Informe de análisis forense del panel de TAP que muestra actividad indicativa de un ataque SocGholish.



Informe de análisis forense del panel de TAP que muestra comportamientos específicos que son indicativos de un ataque SocGholish.

Proofpoint también da prioridad al análisis frecuente y exhaustivo de las URL. El grupo de ciberdelincuentes TA569, a menudo asociado con SocGholish, consiguió mantener el control sobre los sitios inyectados. Hemos observado casos en los que páginas web limpias se han visto comprometidas de nuevo por ataques similares o diferentes.

Por lo tanto, analizamos proactivamente las URL en un entorno aislado una vez que han sido identificadas como inofensivas o limpiadas. La supervisión continua garantiza la rápida detección de cualquier riesgo potencial.

SECCIÓN 3

Phishing mediante códigos QR

El phishing mediante códigos QR desplaza el canal de ataque del entorno protegido del correo electrónico al dispositivo móvil del usuario, que suele ser mucho menos seguro.

Con los códigos QR, la URL no se muestra en el cuerpo del mensaje de correo electrónico. Este enfoque hace que la mayoría de los análisis de protección del correo electrónico resulten ineficaces. Además, el descifrado de códigos QR fraudulentos mediante reconocimiento de imágenes o reconocimiento óptico de caracteres (OCR) consume rápidamente muchos recursos y es difícil de aplicar a gran escala.

La situación

Proofpoint detectó recientemente uno de estos ataques en una empresa agrícola con más de 16 000 empleados. Un ciberdelincuente había creado un señuelo de phishing que parecía proporcionar información sobre el salario de un empleado. El mensaje pedía a los empleados que escanearan un código QR con su teléfono móvil para acceder a la información, en lugar de hacer clic en un enlace. Una vez escaneado, una falsa pantalla de inicio de sesión en SharePoint pedía al usuario que introdujera sus credenciales.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

1. **El mensaje engañoso.** El empleado recibió un correo electrónico que parecía proceder del departamento de Recursos Humanos de la empresa y que supuestamente contenía información relativa a los salarios.

Mensaje de correo electrónico malicioso bloqueado por Proofpoint antes de que llegue a la bandeja de entrada del usuario. (Nota: por motivos de seguridad, hemos sustituido el código QR malicioso por un código QR que redirige a la página Proofpoint.com. El resto del mensaje es una captura de pantalla del original con alguna información oculta).

2. **Secuencia de ataque mediante códigos QR.** El mensaje pedía a los empleados que escanearan el código QR con su teléfono móvil.

Secuencia de ataque mediante códigos QR típica.

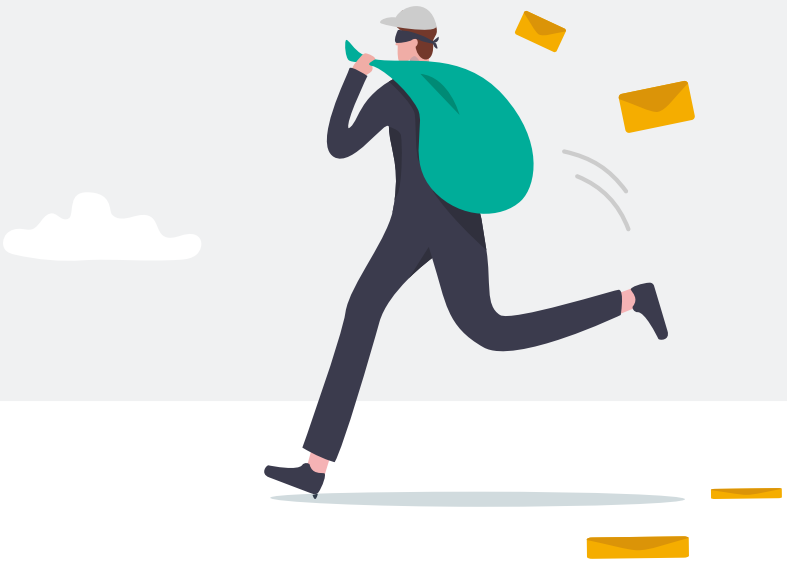
3. **Señuelos de phishing de SharePoint.** Una vez descifrada la URL por el empleado, una pantalla falsa de inicio de sesión en SharePoint le pedía que introdujera sus datos de acceso.

Código QR descodificado que redirige al usuario a una página de phishing de SharePoint.

Por qué estas amenazas son difíciles de detectar

Para empezar, una URL de phishing incrustada en un código QR no es fácil de extraer y analizar. Para colmo, los códigos QR están por todas partes. La mayoría de las firmas de correo electrónico inofensivas contienen logotipos, enlaces a páginas de redes sociales incrustados en imágenes e incluso códigos QR que redirigen a sitios web legítimos. Por lo tanto, la presencia de un código QR no es un signo seguro de un ataque de phishing.

A menudo, las herramientas de seguridad intentan bloquear estas amenazas centrándose exclusivamente en comportamientos de envío inusuales. Sin embargo, no son suficientes para identificar un mensaje como malicioso y pueden llevar a que un mensaje inofensivo se clasifique incorrectamente como peligroso. Este suele ser el caso de las herramientas de protección del correo electrónico que intentan neutralizar las amenazas después de la entrega.



Cómo detectó Proofpoint el ataque

Proofpoint utiliza una combinación avanzada de señales y capas de análisis para distinguir entre códigos QR trampa e inofensivos. Analizamos:

- El remitente
- Los comportamientos del remitente
- La relación entre remitente y el destinatario en función de las comunicaciones anteriores

Todos estos indicios nos ayudan a identificar a los remitentes sospechosos y a determinar si su comportamiento se desvía de un perfil establecido. En este ejemplo, nuestros sistemas nunca antes habían observado que este remitente se comunicara con esta empresa o este destinatario.

Indicios utilizados por Proofpoint para identificar el mensaje como una amenaza.

Sin embargo, no nos basamos únicamente en un comportamiento de envío inusual. Para reducir el número de falsos positivos, combinamos numerosos indicios para extraer la naturaleza y las metonimias del contenido del correo electrónico. (Una metonimia es una palabra o frase utilizada para representar otra cosa, por ejemplo "la Corona" para referirse a la monarquía británica. Este tipo de análisis nos ayuda a deducir la intención de un remitente independientemente de las palabras que utilice).

Inspeccionamos el historial de correo electrónico del remitente y realizamos un análisis lingüístico y semántico del cuerpo del mensaje. Con este enfoque, identificamos el lenguaje que indicaba que el correo electrónico pedía al destinatario que realizara una acción (en este caso, escanear un código QR con su dispositivo móvil).

Además del análisis del comportamiento y del lenguaje, también detectamos tácticas de suplantación en los encabezados de los mensajes. Los ciberdelincuentes intentan a menudo usurpar la identidad de entidades fiables u otros empleados para inspirar confianza. En este caso, los ciberdelincuentes han creado los encabezados de los correos electrónicos para que parezcan proceder de los departamentos de RR. HH. y nóminas de la empresa.

También hemos ido un paso más allá analizando el código QR. Utilizando las tecnologías OCR y de reconocimiento de imágenes de nuestros motores de detección, analizamos y neutralizamos las URL maliciosas ocultas en el propio código QR. Extraemos las URL y el texto para asegurarnos de que los mensajes que deben entregarse se entregan y los que no deben entregarse se bloquean o corrigen.

SECCIÓN 4

Manipulación de la autenticación multifactor

La manipulación de la autenticación multifactor (MFA) es una de las principales amenazas para las plataformas en la nube. Se trata de una sofisticada técnica en la que los ciberdelincuentes aplican su propio método MFA a una cuenta cloud comprometida.

Hay varias opciones a disposición de los ciberdelincuentes que deseen eludir la MFA. Pueden lanzar un ataque de intermediario (adversary-in-the-middle, AiTM): el ciberdelincuente inserta un servidor proxy entre la víctima y el sitio web al que intenta conectarse. A partir de ahí puede robar la contraseña y la cookie de sesión del usuario.

No hay nada que indique al usuario que ha sido atacado; tiene la impresión de que ha iniciado sesión en su cuenta como de costumbre. Sin embargo, los ciberdelincuentes tienen lo que necesitan para establecerse de forma duradera. Por tanto, pueden conservar el acceso aunque los datos de acceso MFA robados se revoquen o se consideren inválidos.

Los ataques de manipulación de la MFA se despliegan tras una usurpación de cuentas cloud. Desafortunadamente, estos ataques son muy habituales. En 2023, los investigadores de amenazas de Proofpoint descubrieron que casi todas las empresas (96 %) sufrieron ataques basados en la nube. Es más, el 60 % de ellas se han visto comprometidas y al menos una cuenta ha sido ocupada.

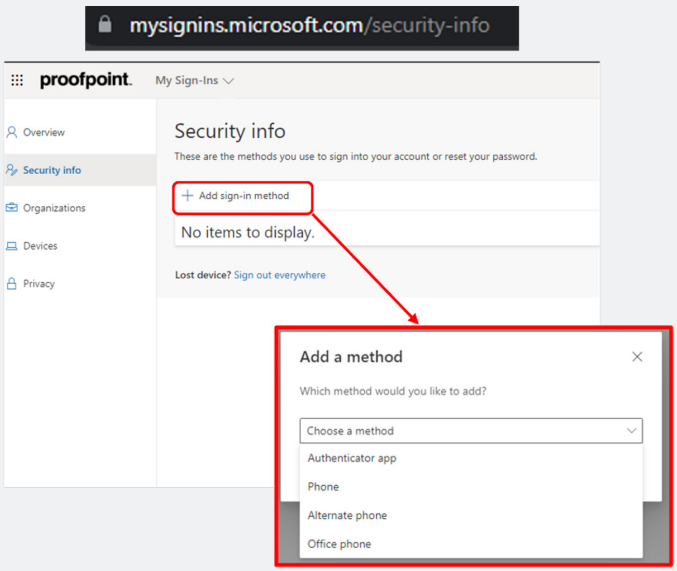
La situación

Proofpoint interceptó una serie de ataques de manipulación de MFA dirigidos a una importante empresa del sector inmobiliario. En un caso, los ciberdelincuentes utilizaron un ataque AiTM para robar las credenciales de inicio de sesión del controlador financiero de la empresa, así como la cookie de sesión. A continuación, accedieron a la cuenta profesional de este usuario y generaron 27 actividades de acceso no autorizado.

Desarrollo del ataque

Veamos cómo se desarrolló el ataque:

1. **Implantación en el sistema.** Los ciberdelincuentes utilizaron la aplicación nativa "Mis inicios de sesión" para añadir sus propios métodos MFA y comprometer las cuentas de Microsoft 365. Descubrimos que los ciberdelincuentes habían registrado su propia aplicación de autenticación con notificación y código. Este registro tuvo lugar justo después de que accedieran a la cuenta pirateada como parte de un ataque automatizado. Esto les ha permitido afianzarse de forma duradera en el entorno de la nube objetivo.



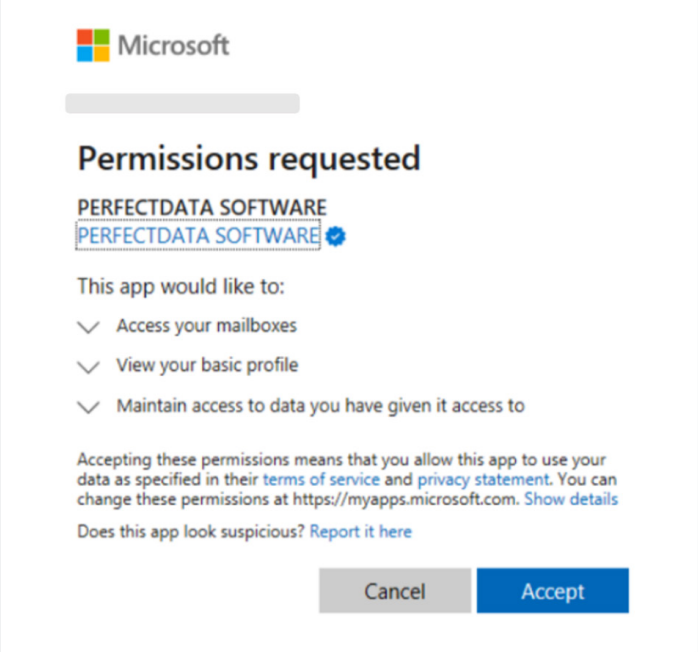
Flujo de trabajo típico de gestión de MFA mediante la aplicación "Mis inicios de sesión" de Microsoft.

2. **Combinación de varias técnicas de ataque.** Los ciberdelincuentes han adoptado un enfoque muy sofisticado. Combinaron la manipulación de la MFA con el uso de aplicaciones OAuth. En pocas palabras, la explotación de OAuth se produce cuando un ciberdelincuente utiliza una aplicación de terceros para robar datos, propagar malware o provocar el caos.

3. **Establecimiento de acceso persistente.** Los ciberdelincuentes también utilizan una aplicación de abuso para conservar el acceso incluso después de haber revocado su acceso inicial a una cuenta comprometida. En este caso, los ciberdelincuentes solicitaron autorizaciones para que la aplicación "PERFECTDATA SOFTWARE", aparentemente inofensiva, estableciera un acceso persistente a la cuenta y los sistemas del usuario, así como a recursos y aplicaciones. Estas son las autorizaciones que los ciberdelincuentes solicitaban para esta aplicación:

    - Acceso total y permanente al buzón de correo electrónico del usuario
    - Acceso sin conexión a los datos
    - Acceso al perfil del usuario

Si se hubieran concedido estas autorizaciones, los ciberdelincuentes habrían tenido vía libre para robar datos sensibles de forma continuada. Esto les habría facilitado la distribución de amenazas a cuentas de usuarios internos o externos.



La solicitud de autorización para la aplicación "PERFECTDATA SOFTWARE", que muestra el alcance de estas autorizaciones.

Por qué estas amenazas son difíciles de detectar

Estos ataques multifase explotan funcionalidades legítimas de la nube. Además, se integran perfectamente en sus actividades habituales. Por eso suelen escapar a las medidas de seguridad tradicionales. Otros proveedores, que se centran en eventos aislados, tienen dificultades para establecer vínculos.

Cómo detectó Proofpoint el ataque

Proofpoint utilizó varias estrategias para determinar cómo se infiltraron los ciberdelincuentes en el sistema y qué hicieron después del ataque. Estas estrategias incluían el uso de inteligencia interna sobre amenazas y el análisis del comportamiento de usuarios y entidades (UEBA).

Los siguientes pasos consistieron en automatizar la corrección de las sesiones maliciosas y revocar la aplicación PERFECTDATA SOFTWARE utilizada. Esto permitió al equipo de seguridad de la inmobiliaria tomar medidas correctivas inmediatas.

Los investigadores de amenazas en la nube de Proofpoint también asesoraron a la empresa mientras analizaba el incidente. Se aseguraron de que todos los métodos MFA controlados por el ciberdelincuente habían sido eliminados definitivamente, para reducir el riesgo en el futuro.

Datos de la aplicación de terceros revocada.

SECCIÓN 5

Ataque multicapa mediante códigos QR

Por lo general, en un ataque mediante código QR, se incrusta un código QR malicioso directamente en un mensaje de correo electrónico. Pero recientemente, los ciberdelincuentes han ideado una nueva y sofisticada variante. En estos ataques multicapa, el código QR malicioso se oculta en lo que parece ser un archivo PDF adjunto inofensivo.

Para ralentizar la detección automática y confundir a las herramientas tradicionales de protección del correo electrónico, los ciberdelincuentes recurren a tácticas de evasión como añadir un CAPTCHA a la página de destino. Por ello, las herramientas tradicionales de detección basadas en el análisis de la reputación de URL tienen cada vez más dificultades para identificar estas amenazas.

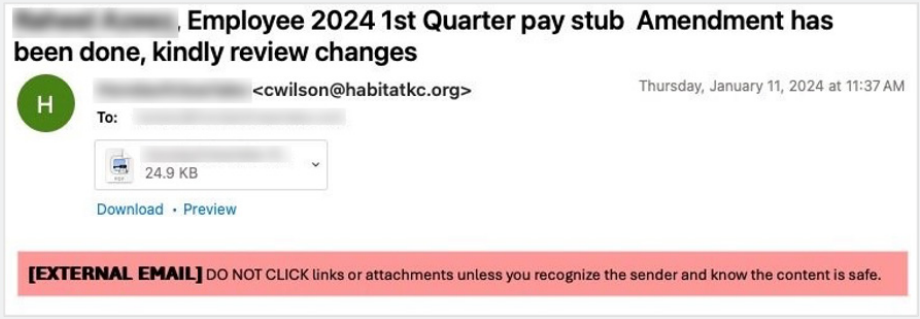
La situación

Proofpoint detectó recientemente una de estas amenazas mientras realizaba una evaluación de amenazas en una empresa automovilística estadounidense con 11 000 empleados. Las herramientas de seguridad existentes de la empresa (una solución de protección del correo electrónico basada en API con seguridad nativa) contaban con funciones de análisis de códigos QR. Sin embargo, clasificaron el correo electrónico como inofensivo y se lo entregaron al usuario.

La amenaza: ¿cómo se produjo el ataque?

Veamos cómo se desarrolló el ataque:

1. **Un señuelo engañoso.** El mensaje de correo electrónico parecía completamente legítimo y aprovechaba la urgencia del período de declaración de la renta. Le pedía al destinatario que abriera un archivo adjunto en formato PDF.

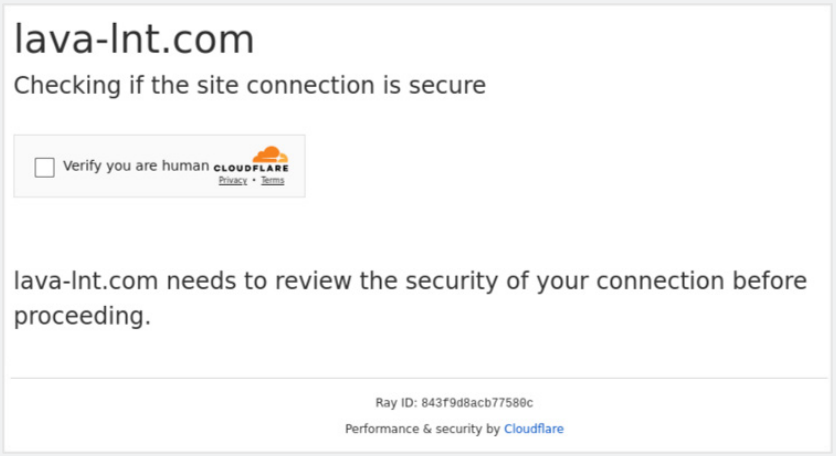


Mensaje de correo electrónico inicial recibido por el usuario final.

2. **Código QR malicioso incrustado en el PDF.** A diferencia de anteriores ataques con códigos QR, la URL maliciosa utilizada en este ataque no se veía directamente en el correo electrónico. Estaba oculta en el PDF adjunto. Dada la omnipresencia de los códigos QR, al destinatario no le habría parecido particularmente sospechoso.

PDF adjunto con el código QR incrustado (oculto).

3. **CAPTCHA de Cloudflare.** El ciberdelincuente ha añadido una capa más de señuelo. Utilizó un CAPTCHA de Cloudflare en la página de destino de la URL del código QR para ocultar aún más la amenaza subyacente. Esta fase se diseñó para eludir las herramientas de detección que se basan exclusivamente en el análisis de la reputación de las URL.



CAPTCHA de Cloudflare en la página de destino de la URL del código QR.

4. **Phishing de credenciales.** Una vez resuelto el CAPTCHA, el código QR malicioso dirigía a una página de destino de phishing diseñada para robar las credenciales del usuario. El robo de las credenciales de un usuario puede permitir a un ciberdelincuente acceder a la cuenta de un usuario para propagar ataques internamente. Los ciberdelincuentes también pueden utilizar estos identificadores externamente para engañar a partners o proveedores, por ejemplo para comprometer cuentas de proveedores.

Por qué estas amenazas son difíciles de detectar

El uso del reconocimiento óptico de caracteres (OCR) u otras técnicas de análisis de códigos QR desempeña un papel fundamental en la defensa contra las amenazas basadas en códigos QR. Sin embargo, el análisis del código QR no es el único mecanismo utilizado para extraer la URL oculta. No es un mecanismo de detección que pueda distinguir los códigos QR legítimos de los maliciosos.

Muchas herramientas, incluidas las soluciones de protección del correo electrónico utilizadas por la empresa automovilística, afirman inspeccionar los códigos QR y extraer la URL para su análisis. Sin embargo, no son capaces de analizar las URL dentro de una imagen incrustada en un archivo adjunto.

Cómo detectó el ataque Proofpoint

Hay muy pocas herramientas que puedan realizar un análisis en profundidad de las URL a la misma escala que Proofpoint. Combinamos el análisis de códigos QR con una pila de detección multicapa que utiliza tecnologías avanzadas de IA y aprendizaje automático. Dado que analizamos tanto la URL como su comportamiento, somos capaces de comprender el contexto de los mensajes de correo electrónico y detectar amenazas avanzadas basadas en URL que otras herramientas pasan por alto.

Esto es lo que utilizamos para detectar y neutralizar esta amenaza:

Análisis de códigos QR. Proofpoint utilizó el análisis de códigos QR para convertir imágenes a un formato legible por máquina. Esto nos permitió extraer la URL oculta para su posterior análisis. Nuestra tecnología de análisis de códigos QR admite archivos PDF, cuerpos de mensajes de correo electrónico, imágenes, archivos de Microsoft Word y mucho más.

Indicadores de comportamiento. Proofpoint analizó el comportamiento de los usuarios, el contexto del mensaje de correo electrónico y la naturaleza temática del mensaje. Detectamos patrones que indicaban que era muy probable que el mensaje fuera malicioso.

Análisis en entorno aislado de URL. Una vez se extrae la URL de un entorno aislado, Proofpoint puede analizar elementos visuales, patrones de redireccionamiento, procesos de endpoints, actividad de red, llamadas DNS y procesos de CPU y de memoria. También podemos detectar tácticas utilizadas para eludir medidas antifraude como CAPTCHA. Incluso si la URL parece inofensiva, a pesar de la observación de indicadores de comportamiento asociados a una actividad maliciosa, seguiremos vigilándola y analizándola para detectar cualquier otro compromiso.

SECCIÓN 6

Conclusión

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

Para ir un paso por delante de peligros como estos, 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 uno de cada siete 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**.