SONICWALL



RESUMEN EJECUTIVO

# ¡Spam a la vista! Por qué el correo electrónico es el principal vector de ataque

La mayor parte de las devastadoras brechas actuales empieza con un simple correo electrónico.

## Resumen

El phishing no consiste solo en conseguir que se pulse en un enlace para ejecutar un malware. El objetivo de los cibercriminales es más insidioso; quieren robar las credenciales de los usuarios con permisos. Eso permite a los delincuentes obtener acceso, enviar correos, hacer peticiones económicas y extender el código malicioso allá donde la identidad robada tiene permisos.

El correo electrónico sigue siendo el principal vector. Las organizaciones tienen que mantenerse atentas para proteger a los empleados contra los ataques avanzados por phishing y malware, empezando por el BEC o Compromiso del correo electrónico de negocio, los ataques de suplantación y el fraude por correo electrónico.

## Introducción

En el mundo se envían casi 320.000 millones de correos electrónicos al día. El correo electrónico sigue siendo la principal forma de compartir información... y amenazas. La pandemia por COVID-19 y las iniciativas de teletrabajo han contribuido a que el correo sea el canal más utilizado para todo tipo de ataques de phishing y ransomware.

Filtraciones importantes de datos nos han enseñado que los ataques avanzados utilizan una gran diversidad de tácticas, técnicas y procedimientos para poner en peligro al usuario. Normalmente, el correo electrónico es el punto de partida de los ataques de ingeniería social, como el BEC o los ataques de robo de credenciales por phishing.

Por ejemplo, el Informe de investigación sobre filtración de datos de Verizon (2020) indica que el 22 % de esas brechas consistían en ingeniería social y que el 96 % llegaban por correo electrónico. En ese mismo informe, otro 22 % de las brechas era el producto de un fallo humano por el que la información sensible se enviaba por error al destinatario equivocado.

Otro estudio de 451 Research descubrió que, aunque el 87 % de las organizaciones tiene ya instalado un producto de seguridad para el correo, el 46 % admite que ese sigue suponiendo el riesgo más significativo para los datos. Asimismo, el 46 % citaba el correo como la mayor vulnerabilidad, casi cinco veces más que el siguiente factor que más les preocupaba.

Microsoft y Google dominan el mercado global del correo basado en la nube, como parte de sus ofertas de suites de aplicaciones. La cuota de mercado global de tecnologías para suites de oficina se reparte entre Google y Microsoft. A nivel mundial, Gmail es la plataforma de correo más popular, con más de 1800 millones de usuarios. Al terminar 2020, Microsoft Office 365 se utilizaba en más de un millón de empresas en todo el mundo; más de 650.000, solo en los EEUU.

Tentados por esa enorme cantidad de víctimas potenciales, los ciberdelincuentes invierten constantemente en nuevos sistemas para estafar a los usuarios de esos servicios de correo basados en la nube. Eso hace que el correo basado en la nube sea uno de los vectores de ataque más atractivos y lucrativos para los hackers oportunistas.



### La persistente efectividad del phishing y el fraude de correo electrónico

La confección de los e-mails de phishing para que parezcan genuinos y enviados desde identidades conocidas, robadas o falsas, puede engañar incluso al usuario más preparado y preocupado por la seguridad. A pesar de los esfuerzos por educar sobre la seguridad, los ataques por phishing siguen citándose a menudo como un eslabón débil de la seguridad. Los responsables de seguridad con quienes hemos hablado siguen viendo a los usuarios hacer clic en los correos de phishing basados en determinados temas y eventos personalizados que guardan

gran parecido con los mensajes legítimos. Muchos usuarios son incapaces de distinguir un correo electrónico legítimo de otro falso, de reconocer los enlaces sospechosos o tomar medidas de precaución como autenticar la URL, la identidad del remitente y las páginas de la empresa.

Sencillamente, la propagación se produce por un error humano. Los correos electrónicos y sus anexos entre empleados, partners, clientes (y, por supuesto, familia y amigos) son algo habitual en la plantilla actual, que es remota y colaborativa. Los aceptamos porque proceden de identidades de confianza y porque necesitamos acceder al contenido y la información para llevar a cabo nuestro trabajo colectivo.

### Compromiso del correo electrónico de negocio (BEC)

El BEC encabeza la lista de suplantaciones de identidad y fraudes por correo electrónico. Este tipo de ataque suele consistir en el uso de la cuenta comprometida de un CEO u otro directivo. Los estafadores utilizan la cuenta comprometida para enviar peticiones económicas falsas, como el pago de una factura falsa o el envío de dinero para cerrar una operación comercial falsa.

En muchos casos, tras el secuestro de las cuentas de correo de ejecutivos de alto nivel se esconden ataques de ingeniería social o de whaling para robar credenciales que permiten realizar los ataques. El Internet Crime Complaint Center del FBI (IC3) informa de que en 2020 las pérdidas causadas en EEUU por el cibercrimen superaron los 4100 millones de dólares. El BEC fue el vector de amenaza individual más dañino (1800 millones de dólares).

Cuando nos damos cuenta de que las credenciales del ejecutivo están comprometidas, ya es demasiado tarde. Solo hace falta una cuenta comprometida para crear una reacción viral de usuario a usuario, dispositivo a dispositivo y aplicación a aplicación que sea imposible detener antes de que se produzcan daños.

### La seguridad nativa de nube no es suficiente

Los desarrolladores de seguridad para el correo electrónico han creado formas de proteger a los usuarios de los enlaces maliciosos que evaden los filtros previos a la entrega y llegan al buzón, como la protección en el momento del clic, la retirada de e-mails después de la entrega y los filtros del navegador web. No obstante, los atacantes siguen dedicados a crear formas de llegar a los buzones.

Un reciente informe de Microsoft ATP 2020 publicó que más de uno de cada diez correos de phishing dirigido logran llegar al buzón del usuario. Cada ataque individual aprovecha diversas combinaciones de métodos de ofuscación diseñados expresamente para evadir las soluciones Exchange Online Protection (EOP) y Advanced Threat Protection (ATP) de Microsoft.

Algunos ataques muy extendidos que llegan por correo evitan los filtros de seguridad con bastante éxito. Un ejemplo de esos ataques son correos electrónicos de phishing dirigidos de poco volumen, pero muy bien hechos, que parecen proceder de Office 365 o Gmail. La presentación es buena, están personalizados y se envían a un conjunto concreto de usuarios, en lugar de utilizar una lista masiva de direcciones como en las campañas tradicionales de gran volumen. Esos ataques son sofisticados tanto por su técnica para llegar hasta el buzón como por la experiencia del usuario en el backend. Normalmente, cada enlace incluye la dirección de correo electrónico del usuario, de forma que la página de inicio tiene el aspecto de la segunda página del inicio de sesión de la cuenta, cuando se entra en una página de administración en la que ya se está registrado. Sabe quién es el destinatario y proporciona datos de forma oculta.

La curva de innovación del phishing ocurre ahora después de la entrega del correo. Eso quiere decir que, en vez de poner la URL maliciosa en el correo, los atacantes enlazan con un servidor de redirección que hace de pasarela y envía peticiones desde una compañía de seguridad a unas páginas inofensivas. En contraste, las consultas de las víctimas objetivo se dirigen al servidor de phishing.

Aunque ATP de Microsoft aplica cuatro motores de directivas para el antiphishing, la inteligencia sobre spoofing, Safe Links y Safe Attachments (para enlaces y adjuntos), sigue siendo una tecnología de seguridad basada en reglas. El análisis de seguridad depende solo de un filtrado estático basado en la reputación al cual los hackers pueden aplicar ingeniería inversa para descubrir cómo evadir esos filtros. Esa debilidad en la capa de seguridad pone a las empresas en un estado de riesgo constante, amenazadas por la posibilidad de que alguien de la organización abra el archivo incorrecto, haga clic en una URL maliciosa o escriba una contraseña en el lugar equivocado.

La visibilidad y el acceso a la gran población de usuarios del correo en la nube los convierten en objetivos fáciles para los ciberdelincuentes, que nunca habían tenido al alcance tantos buzones y cuentas de usuario con una seguridad idéntica. Asimismo, como esas cuentas en la nube son la forma de autenticarse en otras aplicaciones SaaS de la empresa, los hackers aprovechan para propagar el malware o robar datos. Este es el auténtico peligro actual del «monocultivo» en la seguridad de nube. Si se evade un control se evaden todos los demás.

SiteCloak es un buen ejemplo de la técnica que actualmente se utiliza para evadir ATP Safe Links de Microsoft 365, también conocido como protección por tiempo de clic. Lleva la ocultación del phishing al siguiente nivel: utiliza diversas tácticas y técnicas para encubrir la verdadera intención de la página de destino, que suele ser una página para recolectar credenciales.

Las víctimas de SiteCloak no necesitan introducir su dirección de correo electrónico; se les lleva directamente a la pantalla para escribir la contraseña, donde la página de recolección de credenciales utiliza la técnica ZeroFont para evadir los análisis de correo electrónico de Microsoft. Entre los caracteres de la página, se intercalan caracteres aleatorios de una fuente de tamaño cero, de forma que los filtros de lenguaje natural de Microsoft ven el texto aleatorio, mientras que los lectores humanos ven lo que los ataques quieren enseñarles. En otras palabras, Safe Links cree que es una página inofensiva, mientras que para la víctima parece una página real, y desde ella se recolecta la credencial. Los atacantes habilitan el contenido malicioso solo después de que el mensaje de correo haya llegado al buzón.

## Conclusiones

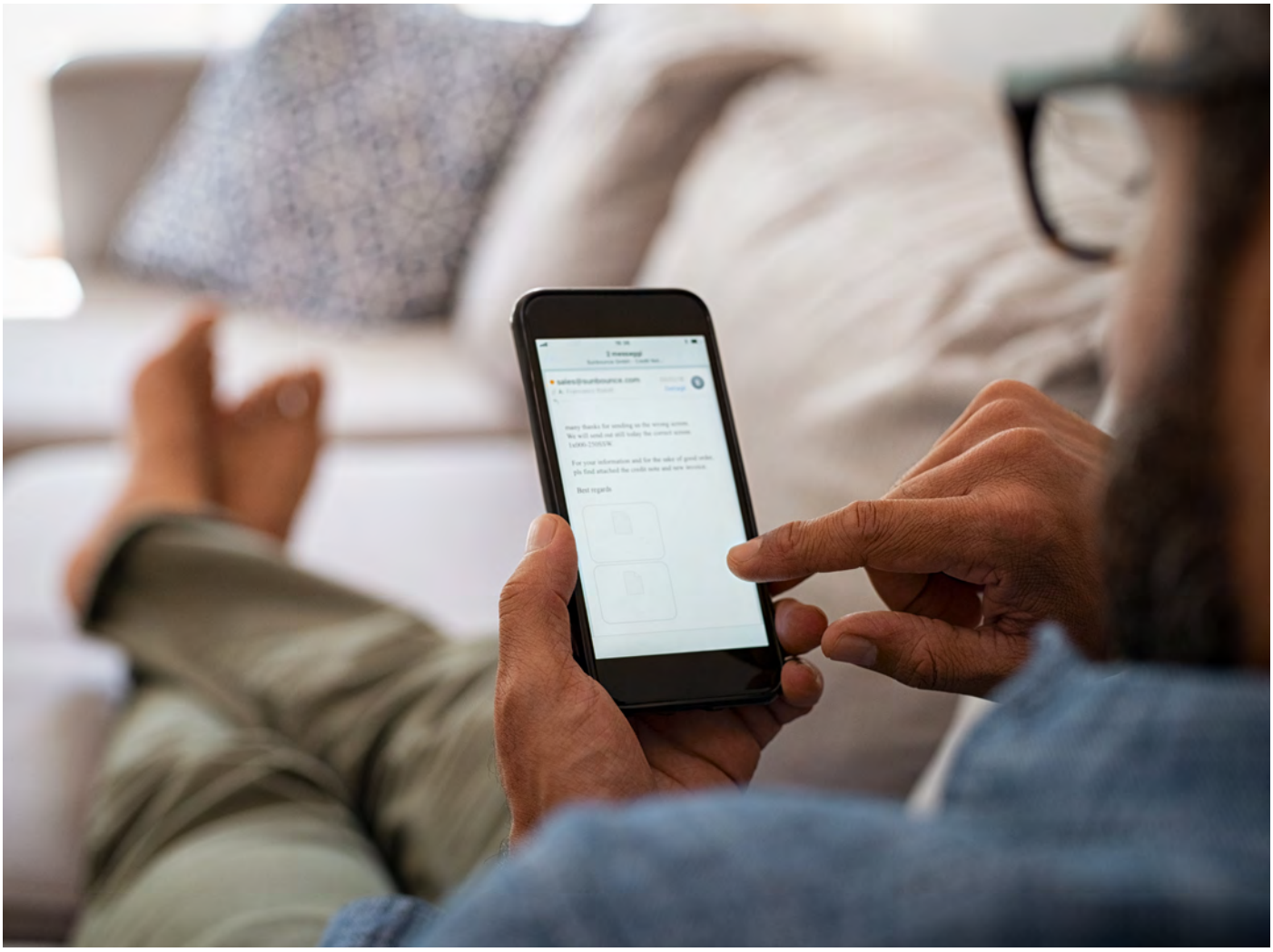
SiteCloak y otras formas de fraude de correo electrónico son el ejemplo de que los hackers pueden evadir la detección utilizando ataques de phishing muy elaborados y personalizados y bien preparados. Estos no serán los últimos que pasen inadvertidos por los filtros de seguridad en la nube de los proveedores. Las empresas necesitan niveles de protección adicionales aparte de la seguridad integrada de los proveedores de su sistema de oficina en la nube.

Se puede instalar SonicWall Email Security como una solución sólida de dispositivo virtual, aplicación de software, servicio hospedado o dispositivo físico reforzado (ideal para organizaciones que necesitan una solución local dedicada). La solución multicapa de SonicWall proporciona protección completa de correo entrante y saliente. Protege contra las amenazas avanzadas basadas en el correo electrónico, como ransomware, ataques de día cero, phishing, spear phishing y BEC (compromiso del correo electrónico de negocio).

**Obtenga más información** en www.sonicwall.com/email-security.

## Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el trabajo remoto y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la seguridad cibernética para empresas, gobiernos y pymes en todo el mundo. Si desea más información, visite www.sonicwall.com.



**SonicWall, Inc.**
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestro sitio web.
www.sonicwall.com

**© 2021 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.**

*SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. y/o sus filiales en EEUU y/u otros países. Las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos propietarios. La información incluida en este documento se proporciona en relación con los productos de SonicWall Inc. y/o sus filiales. No se otorga mediante este documento, ni en relación con la venta de productos SonicWall, ninguna licencia, expresa ni implícita, por doctrina de los propios actos ni de ningún otro modo, sobre ningún derecho de propiedad intelectual. A EXCEPCIÓN DE LO ESTABLECIDO EN LOS TÉRMINOS Y CONDICIONES TAL Y COMO SE ESPECIFICAN EN EL CONTRATO DE LICENCIA DE ESTE PRODUCTO, SONICWALL Y/O SUS FILIALES NO ASUMEN NINGUNA RESPONSABILIDAD Y RECHAZAN CUALQUIER GARANTÍA EXPRESA, IMPLÍCITA O LEGAL EN RELACIÓN CON SUS PRODUCTOS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN PARA UN DETERMINADO PROPÓSITO O NO VIOLACIÓN DE DERECHOS DE TERCEROS. SONICWALL Y/O SUS FILIALES NO SE HARÁN RESPONSABLES EN NINGÚN CASO DE DAÑOS DIRECTOS, INDIRECTOS, CONSECUENTES, PUNITIVOS, ESPECIALES NI INCIDENTALES (INCLUIDOS, SIN LIMITACIÓN, LOS DAÑOS RELACIONADOS CON LA PÉRDIDA DE BENEFICIOS, LA INTERRUPCIÓN DEL NEGOCIO O LA PÉRDIDA DE INFORMACIÓN) DERIVADOS DEL USO O DE LA INCAPACIDAD DE UTILIZAR EL PRESENTE DOCUMENTO, INCLUSO SI SE HA ADVERTIDO A SONICWALL Y/O SUS FILIALES DE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS. SonicWall y/o sus filiales no ofrecen declaración ni garantía alguna con respecto a la precisión ni a la integridad de la información contenida en el presente documento y se reservan el derecho de modificar las especificaciones y las descripciones de productos en cualquier momento y sin previo aviso. SonicWall Inc. y/o sus filiales no se comprometen a actualizar la información contenida en el presente documento.*

ExecBrief-EmailThreatVector-A4-COG-5264