RESUMEN EJECUTIVO

¿Son realmente seguros sus correos electrónicos 0365 y G-Suite?

Por qué no basta con la seguridad nativa en la nube

RESUMEN

Las comunicaciones por correo electrónico 0365 y G-Suite en la nube están presentes en todas las organizaciones actuales. Sin embargo, también es un vector principal para los ciberataques que eluden la defensa nativa y los gateways de seguridad del correo electrónico (SEG). Este resumen examina las brechas de seguridad inherentes y los requisitos para proteger verdaderamente el correo electrónico en la nube frente a los sofisticados ataques actuales.

INTRODUCCIÓN

Según un estudio[1] de 451 Research, casi 9 de cada 10 organizaciones ya tienen desplegado un producto de seguridad para los correos electrónicos. Sin embargo, casi la mitad de los encuestados admite que el correo electrónico sigue representando la mayor amenaza para los datos. Por un amplio margen, esta cifra es mayor que otras amenazas del estudio. Y casi la mitad señala el correo electrónico como su mayor vulnerabilidad.

Los ciberdelincuentes que generan amenazas a través de los correos electrónicos responden rápidamente a las grandes tendencias. El movimiento del trabajo desde el hogar y la COVID-19 son solo los últimos ejemplos de lo que convierte al tráfico por correo electrónico en el canal ideal de ataques. Dado que este tipo de servicio de mensajería sigue siendo la principal forma en la que nos comunicamos y compartimos datos, tanto a nivel profesional como personal, miles de millones de personas lo utilizan a diario. Sin embargo, la mayoría no ha recibido una formación adecuada para distinguir los correos electrónicos legítimos de los fraudulentos, reconocer enlaces sospechosos o adoptar medidas de precaución, como autenticar la URL o el sitio web de la empresa del remitente.

Además, hoy en día, los ciberdelincuentes son tan hábiles para crear correos electrónicos phishing que parezcan auténticos que incluso los usuarios expertos en seguridad pueden ser engañados. Por ejemplo, los ataques de phishing que imitan el correo electrónico correspondiente a la Ley de Ayuda, Alivio y Seguridad Económica contra el Coronavirus (CARES) se aprovecharon de víctimas ansiosas y confundidas durante la pandemia de la COVID-19.

Con un grupo tan grande de víctimas nuevas y desconocidas, que comparten la misma monocultura sobre la seguridad, los piratas informáticos han cambiado y multiplicado sus ataques a los servicios en la nube como Office 365 y G Suite. No hay un objetivo mejor ni un premio mayor, ya que sus usuarios en conjunto aumentan el crecimiento anual de dos dígitos. Sin duda, esto sigue convirtiendo a las aplicaciones de correo electrónico en la nube y al conjunto de programas Office en los vectores de ataque más deseables y lucrativos para todo tipo de piratas informáticos oportunistas.

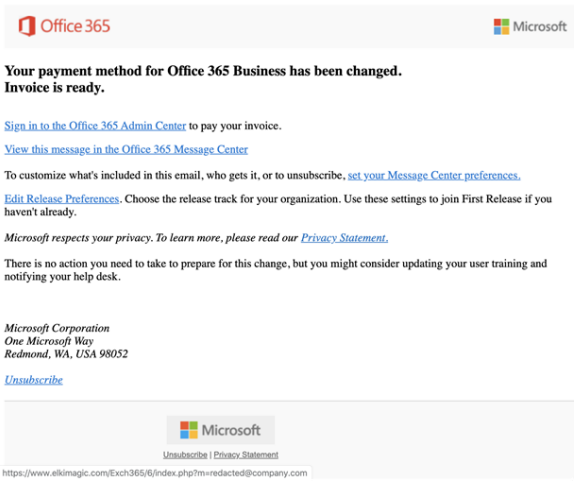
Según el Informe sobre las investigaciones de fugas de datos[2] de 2019 de Verizon, el 90% de los ataques comenzaron con un mensaje de correo electrónico phishing. Aproximadamente el 60% de las veces, el vector de aplicaciones web afectado era el front-end de los servidores de correo electrónico en la nube. Los servicios de correo electrónico en la nube plantean varios desafíos para la seguridad:

- La seguridad nativa en la nube no es suficiente.
- Los SEG no están diseñados para la nube.
- Los SEG solo protegen los correos electrónicos entrantes y salientes.
- Los SEG se limitan al correo electrónico.
- Los SEG se transmiten a los piratas informáticos.

La seguridad nativa en la nube no es suficiente.

Un reciente informe de Microsoft ATP[3] de 2020 reveló que, de más de quinientos mil mensajes analizados, más de uno de cada diez correos electrónicos phishing dirigidos puede llegar a la bandeja de entrada del usuario. Cada ataque individual aprovecha diversos métodos de ofuscación diseñados específicamente para eludir Microsoft ATP. Estas técnicas probadas incluyen múltiples redirecciones, divisiones de URL, manipulación de etiquetas HTML, malware polimórfico y scripts ocultos y dinámicos.

Aunque Microsoft ATP aplica cuatro motores de políticas principales para antiphishing, inteligencia contra la suplantación de identidad, enlaces seguros y archivos adjuntos seguros, sigue siendo una tecnología de seguridad


Office 365 Microsoft

Your payment method for Office 365 Business has been changed.
Invoice is ready.

Sign in to the Office 365 Admin Center to pay your invoice.

View this message in the Office 365 Message Center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message Center preferences.

Edit Release Preferences. Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

Microsoft

Unsubscribe | Privacy Statement

https://www.elkimagic.com/Exch365/6/index.php?m=redacted@company.com

Estos ataques son sofisticados tanto en su técnica para llegar a la bandeja de entrada como en la experiencia del usuario en back-end. Cada enlace incluía la dirección de correo electrónico del usuario para que la página de inicio de sesión a la que llegaban pareciera la segunda página de una comprobación de cuentas de Microsoft, que es exactamente lo que sucede cuando intenta ir a una página del administrador cuando ya ha iniciado sesión. El ataque demostró que ya conoce la identidad de la víctima.

La Figura 2, a continuación, examina el mismo ejemplo de campaña de ataque en múltiples organizaciones durante el período de prueba. En casi todos los casos, independientemente de si una organización encontró 5 o 50, la mayoría de los correos electrónicos maliciosos han pasado por alto EOP y ATP. En dos casos que figuran con la barra azul, EOP pudo llegar a bloquear el ataque, pero solo después de haber pasado por alto más de 30 instancias del ataque.

La adopción generalizada de Office 365 y G-Suite lo convierte en un blanco fácil para todos los piratas informáticos. Nunca tantos buzones de correo tuvieron la misma seguridad. Los piratas informáticos también aprovechan el hecho de que estas cuentas en la nube son fuentes de autenticación para otras aplicaciones SaaS empresariales. Este es el peligro de la monocultura de seguridad en la nube. Lo que pasa por alto a uno, pasa por alto a todo.

basada en reglas como los SEG tradicionales. El análisis de seguridad depende exclusivamente del filtrado estático basado en la reputación que los piratas informáticos pueden utilizar para realizar ingeniería inversa hasta que encuentren formas de eludir estos filtros. Esto coloca a las empresas en un estado de riesgo constante, amenazadas por la posibilidad de que alguien de su organización abra el archivo incorrecto, haga clic en la URL incorrecta o introduzca la contraseña en el lugar incorrecto.

Algunos ataques parecen legítimamente enviados desde Microsoft, como se muestra en la Figura 1 a continuación. Se desempeñan muy bien, se personalizan de manera profesional y se envían a un conjunto específico de usuarios en lugar de a toda la compañía.

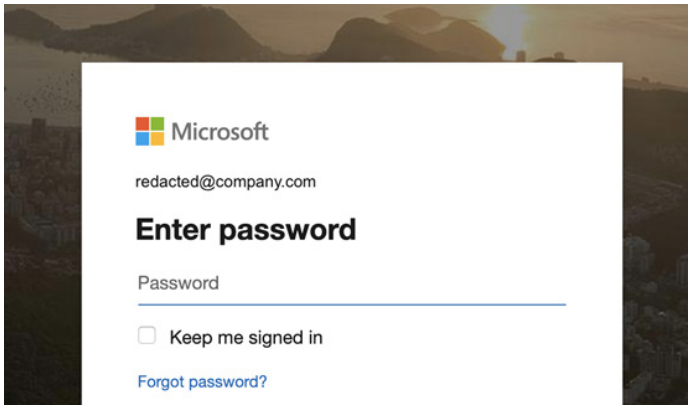


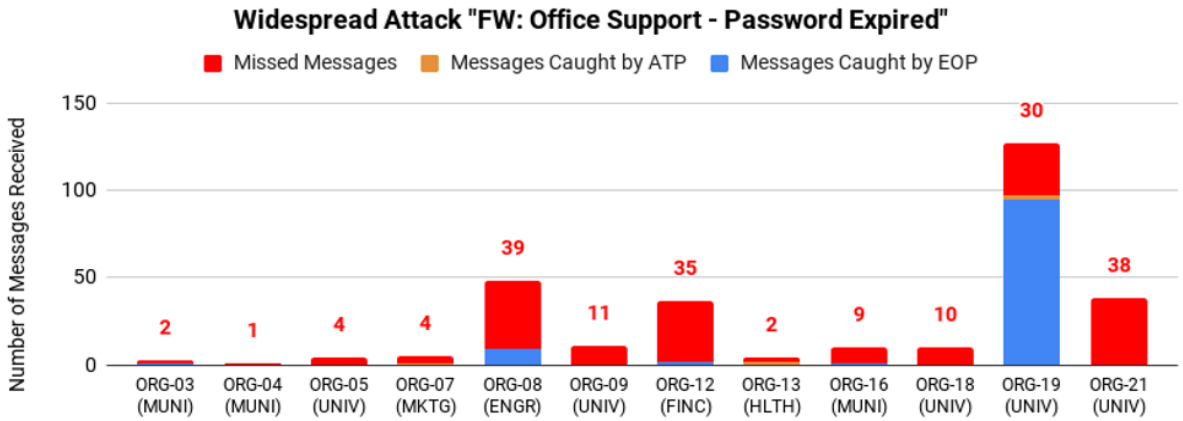
Figura 1

Los piratas informáticos han demostrado constantemente su ingenio para evadir la detección mediante ataques phishing dirigidos y escapar de los filtros de seguridad de los proveedores de servicios en la nube. Está claro que las organizaciones necesitan niveles de protección adicionales a los de Microsoft ATP y otros SEG.

Los SEG no están diseñados para la nube.

Los SEG se diseñaron originalmente en un perímetro reforzado para proteger los entornos de correo electrónico locales. A medida que el correo electrónico se trasladaba a la nube a través de servicios como Office 365 Email y Gmail, los SEG se reorganizaron y adaptaron a este nuevo entorno. Sin embargo, el enfoque padece muchas deficiencias debido a su diseño no nativo.

La mayor deficiencia del SEG es el impedimento para la seguridad existente. Sus cambios requeridos en los registros MX perjudican o eliminan completamente los filtros integrados. Esto significa que, en lugar de aumentar los análisis de seguridad, reemplazan completamente el valor predeterminado y, a su vez, desactivan las defensas valiosas de esas capas inherentes. Además, estas soluciones se implementan en el perímetro, por lo que tienen una visibilidad limitada. Por lo general, no conocen las amenazas internas, como las cuentas afectadas y los mensajes entre empleados.



Los SEG solo protegen los correos electrónicos entrantes y salientes.

Dado que los SEG se conectan al flujo de correo fuera de la nube del proveedor de correo electrónico, los correos electrónicos internos no se analizan en busca de amenazas. En un entorno de nube, el riesgo de las cuentas es mucho más común debido al acceso a las credenciales. Los correos electrónicos internos pueden ser tan amenazados como aquellos entrantes y salientes.

Algunos gateways de los correos electrónicos utilizan reglas de registro diario para analizar correos electrónicos internos. Sin embargo, este método solo los analiza después de la entrega y no impide que lleguen a la bandeja de entrada. Esto no protege adecuadamente a los usuarios de mensajes de correos electrónicos internos maliciosos, ya que el destinatario puede hacer clic en el mensaje en el intervalo de tiempo entre la entrega y el análisis.

Los SEG se limitan al correo electrónico.

En un entorno de nube, el correo electrónico no es el único vector de ataque. El intercambio de archivos, las aplicaciones de mensajería y otras aplicaciones de SaaS están interconectadas, lo que proporciona canales adicionales para que las amenazas lleguen a los usuarios dentro de una organización. La protección de la bandeja de entrada que proporcionan los SEG simplemente no es suficiente en este panorama interconectado. A menos que el cliente compre módulos de seguridad adicionales, los SEG no tienen visibilidad en estas aplicaciones conectadas. Como consecuencia, no pueden identificar amenazas en esa parte del entorno.

Los SEG se transmiten a los piratas informáticos.

Para redirigir el correo electrónico a través de un SEG, una organización debe cambiar sus registros MX por los del gateway. Se trata de información pública a través de sitios como MXToolbox, que permite a los piratas informáticos diseñar ataques dirigidos y confeccionados para eludir el análisis de un SEG específico.

Conclusión

Los ciberataques a través de los correos electrónicos están aumentando y son más sofisticados que nunca. Por lo tanto, es vital poner en práctica un enfoque escalonado para reducir las brechas de seguridad. Cloud App Security (CAS) de SonicWall ofrece protección integral para aplicaciones de correo electrónico en la nube y SaaS. Detecta los ataques de día cero que se propagan por correo electrónico que las soluciones de Microsoft y SEG pasan por alto a través de un sistema de prevención de amenazas en línea y multicapa que se implementa fácilmente en cuestión de minutos a través de una API. CAS detiene los ataques que ponen en riesgo el correo electrónico corporativo, el phishing dirigido, los malware, los ataques de día cero, la apropiación de cuentas y las amenazas internas en toda la empresa.

Obtenga más información. *Visite www.sonicwall.com/cas.*

[1]451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects, Q1 2019

[2]https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[3]https://track.eng.sonicwall.com/browse/WWW2-3226

Acerca de SonicWall

SonicWall ofrece una ciberseguridad sin límites para la era de la hiperdistribución y una realidad laboral en la que todo el mundo es remoto, móvil y poco seguro. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y permitir un gran avance económico, SonicWall reduce la brecha del negocio de la ciberseguridad para las empresas, los gobiernos y las pequeñas y medianas empresas (SMB) de todo el mundo. Para obtener más información, visite www.sonicwall.com

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nuestro sitio web para obtener información adicional.
www.sonicwall.com