Aislamiento de enlaces del correo electrónico

Aísla los enlaces del correo electrónico para reducir la superficie de ataque y simplificar las operaciones

Reduce los riesgos de phishing mediante la aplicación de protección y controles de aislamiento del navegador

Reto: phishing multicanal sofisticado

El phishing multicanal abarca el correo electrónico y la entrega web de manera que puede eludir hábilmente las reglas de filtrado. Los tipos más comunes de phishing son:

- **Phishing diferido**: un enlace inicialmente inofensivo dentro de un correo electrónico se convierte en un arma con un destino malicioso después de la entrega.
- **Phishing de servicio en la nube:** enlaces HTTPS peligrosos que se parecen a los de servicios de la nube comunes (p. ej., Google Drive, Box)

Para detener este tipo de amenazas, la protección moderna del correo electrónico debe estar equipada para aplicar la política de análisis Zero trust "nunca confíes, verifica siempre" a todos los enlaces.

Solución: aislamiento de los enlaces del correo electrónico

La integración del aislamiento remoto del navegador (RBI) en la seguridad del correo electrónico en la nube (CES) aplica este control para aumentar la protección contra el phishing. Los clientes de Cloudflare Area 1 pueden activar la solución de aislamiento de navegador de Cloudflare para neutralizar estas amenazas multicanal.

Los administradores pueden controlar las interacciones de los usuarios (como restringir las entradas de teclado y las cargas de archivos) en páginas web aisladas para evitar el impacto del phishing, como el robo de credenciales o datos confidenciales.

Además, abrir los enlaces de correos electrónicos en un navegador aislado neutraliza el malware, ya que ejecuta todo el código en la nube, lejos de los dispositivos locales.

Lo que dicen los analistas:

"Las URL de los correos electrónicos que se resuelven externamente se suelen utilizar para lanzar ataques de phishing a los usuarios. Aislarlas puede reducir el número de ataques de phishing exitosos".

"La mayoría de los ataques se realizan a través de la red pública de Internet, ya sea a través de la navegación web o de enlaces enviados por correo electrónico que engañan al usuario para que visite sitios maliciosos. El simple hecho de eliminar (o, más aún, aislar) el navegador del escritorio del usuario final mejora significativamente la postura de seguridad de la empresa, incluida la protección contra los ataques de ransomware".

"Evalúa y pon a prueba una solución de aislamiento de navegador para usuarios específicos de alto riesgo (como los equipos de finanzas) o casos de uso (como la representación de la URL del correo electrónico), especialmente si tu organización tiene aversión al riesgo". [1]

Gartner

Más información

Beneficios de la integración CES y RBI para empresas

Mejora la protección contra el phishing

El aislamiento del correo electrónico no solo impide que el código dañino de un enlace de phishing se ejecute localmente, sino que también aplica controles de protección de datos para evitar que la información confidencial caiga en manos equivocadas.

Aprovecha la productividad de los equipos de seguridad y TI

Activa el aislamiento del correo electrónico para cualquier sitio web con unos clics.

Evita a los equipos de TI y de seguridad la complicación de configurar políticas de filtrado que acarrean el riesgo de "bloquear por exceso" (y limitar la productividad de los usuarios) o "bloquear por defecto" (y dejar entrar amenazas).

Ejemplo de caso de uso: detener el phishing diferido

Problema: el ataque de phishing diferido evade la detección

Con las tácticas y la motivación adecuadas, las campañas de phishing diferido pueden eludir las protecciones tradicionales.

Configuración de la campaña: los atacantes pueden empezar enviando un correo electrónico de aspecto auténtico desde un dominio recién creado, utilizando una autenticación del correo electrónico adecuada (SPF, DKIM, DMAR) y una página web inofensiva.

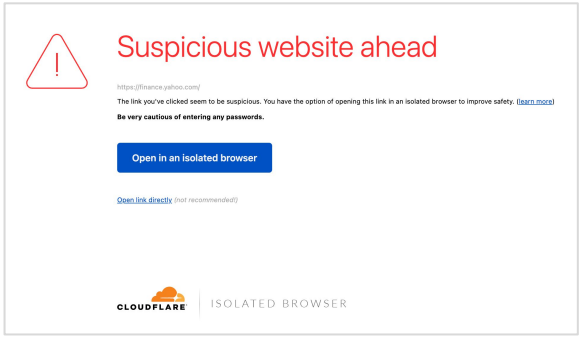
Entrega exitosa a las bandejas de entrada: estos correos electrónicos pueden eludir la detección ofrecida por las puertas de enlace de correo electrónico seguras, los filtros basados en la autenticación u otros servicios que dependen de señales basadas en la reputación y otras técnicas deterministas.

Redireccionamiento a un enlace malicioso: una vez que el correo electrónico se ha entregado correctamente, el atacante puede redirigir el enlace a un destino malicioso cambiando la página web controlada por el atacante. Por ejemplo, un redireccionamiento común es a una página de inicio de sesión falsa utilizada para recopilar credenciales.

Solución: aislar los enlaces sospechosos después de la entrega

El aislamiento de los enlaces de correos electrónicos proporciona una capa crítica de protección posterior a la entrega. Cloudflare analiza cualquier enlace del correo electrónico en el que el usuario haga clic. Si el enlace se considera sospechoso o peligroso, Cloudflare muestra una página de advertencia *(véase más abajo)* y, a continuación, aísla la página web si el usuario navega por ella.

Los administradores evitan que el código malicioso se ejecute en los dispositivos locales y pueden aplicar controles de protección de datos, como restringir la carga y descarga de archivos, impedir la entrada de teclado del usuario o abrir la página en modo de solo lectura.



Cronograma de una campaña de phishing diferido

Cloudflare analiza cada enlace en el momento del clic

Enlace seguro: se redirigirá a los usuarios al sitio de forma transparente.

Enlace malicioso: se bloquea la navegación de los usuarios.

Enlace sospechoso: se disuade a los usuarios de navegar y se les presenta una página de advertencia que les sugiere ver el enlace en un navegador aislado.

Integración de la seguridad del correo electrónico en la nube con Cloudflare Zero Trust

Seguridad moderna con Zero Trust

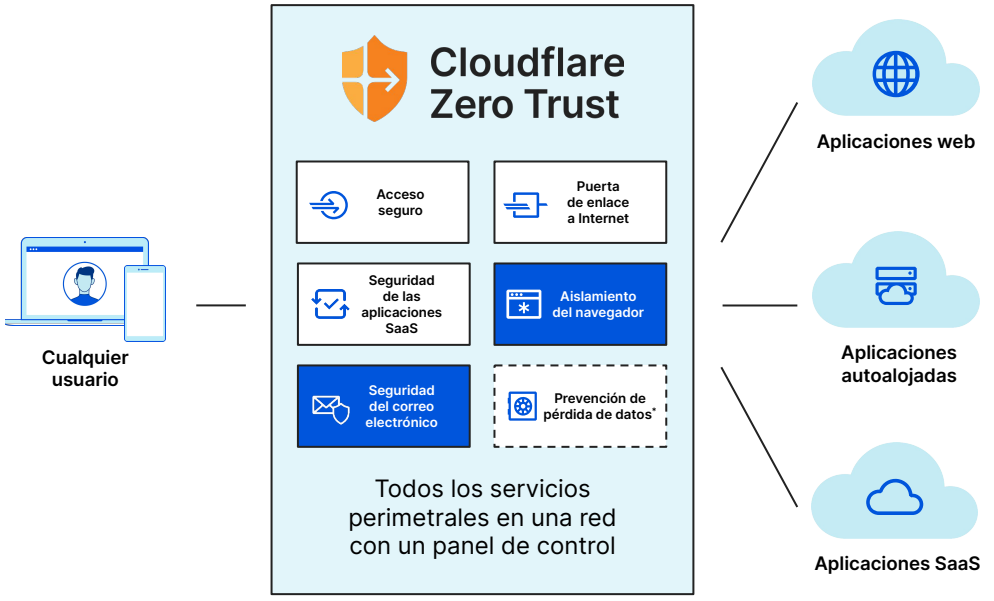
Cloudflare Zero Trust aumenta la visibilidad, elimina la complejidad y reduce los riesgos cuando los usuarios remotos y presenciales se conectan a las aplicaciones y a la red pública de Internet.

El 1 de abril de 2022, Cloudflare completó la adquisición de Area 1 Security con la intención de aumentar la protección que la plataforma Zero Trust ofrece a los usuarios contra los ataques de phishing en entornos de correo electrónico, web y red. Más información.

Seguridad del correo electrónico: clave para Zero Trust

La seguridad del correo electrónico de Cloudflare Area 1 mejora la arquitectura Zero Trust, ya que elimina la confianza implícita en el correo electrónico para detener de forma preventiva los ataques de phishing y contra el correo electrónico corporativo (BEC).

No confía nunca en el remitente, aunque sea interno. En su lugar, verifica, filtra e inspecciona todo el tráfico del usuario y lo aísla de las amenazas de Internet. La seguridad del correo electrónico se integrará en los servicios Zero Trust de Cloudflare en integración eficaz con RBI, CASB y otras soluciones.



Sustitución de la VPN
Simplifica y protege la conexión de cualquier usuario a cualquier recurso.

Protección web
Protege tus datos de las amenazas a través de cualquier puerto y protocolo.

Optimiza la seguridad de SaaS
Visibilidad y control de las aplicaciones, incluido el correo electrónico.

Modernización de la seguridad
Mejora la productividad, simplifica las operaciones y reduce la superficie de ataque.

* Regístrate en nuestra lista de espera DLP

Seguridad del correo electrónico en la nube (CES)

- Reduce un 90 % los tiempos de respuesta a incidentes de phishing.
- Identifica la infraestructura del atacante y los mecanismos de entrega con antelación para detener el phishing en las primeras etapas del ciclo de ataque.
- Elimina la confianza implícita del correo electrónico mediante el análisis del contenido, el contexto y los gráficos sociales de comunicaciones.
- Aprovecha las integraciones con Microsoft, Google y otros entornos para mejorar la seguridad integrada.

Aislamiento remoto del navegador (RBI)

- Evita el riesgo del robo de credenciales abriendo sitios peligrosos en modo solo lectura gracias al control de las interacciones del usuario (p. ej., entrada de teclado, copiado y pegado, cargas y descargas).
- Ejecuta todo el código del navegador en la red de Cloudflare, aislando los dispositivos locales del código malicioso.
- Proporciona experiencias rápidas y sin interrupciones a los usuarios finales. En lugar de la típica secuencia de píxeles, preparamos una réplica exacta de la página desde un navegador remoto, a menos de 50 m/s de distancia del 95 % de los usuarios de Internet a nivel mundial.

Solicita ya una evaluación del riesgo de phishing — **Te ayudamos**

+34 518 880 290 | enterprise@cloudflare.com | http://www.cloudflare.com/es-es/

REV: PMM-JUN2022

[1] *Gartner Hype Cycle for Network Security, 2021* |