Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°186	Fecha: 09-08-2023
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Campaña de phishing EvilProxy dirigida a 120.000 usuarios de Microsoft 365		
Tipo de Ataque	Phishing**¡Error! Marcador no definido.**	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

EvilProxy se está convirtiendo en una de las plataformas de phishing más populares para atacar cuentas protegidas por MFA, y los investigadores vieron 120 000 correos electrónicos de phishing enviados a más de cien organizaciones para robar cuentas de Microsoft 365.

Esta nueva investigación proviene de Proofpoint, que advierte sobre un aumento dramático de incidentes exitosos de adquisición de cuentas en la nube en los últimos cinco meses, que afectaron principalmente a ejecutivos de alto rango. Anteriormente, estos métodos se habían visto en campañas dirigidas de APT y grupos de ciberespionaje; sin embargo, ahora se ejecutaron con éxito en EvilProxy, lo que destaca la importancia del crecimiento de los ataques contra los servicios en línea y los mecanismos de autorización de MFA.

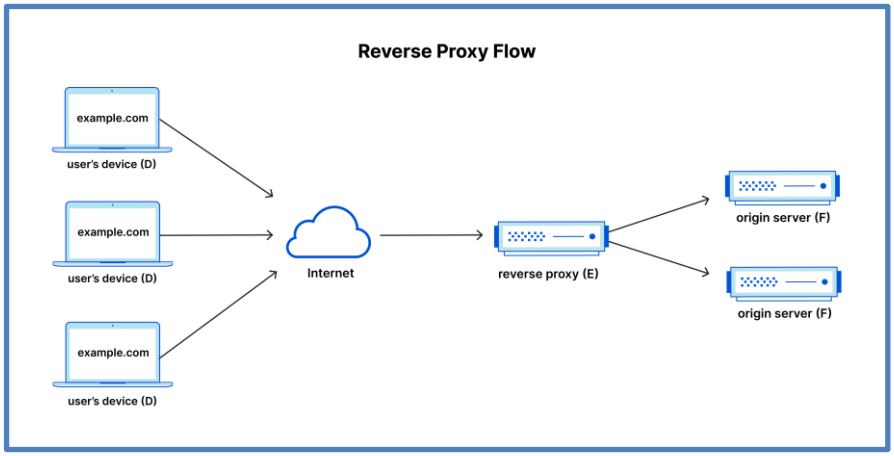
EvilProxy es un kit de herramientas de phishing que puede robar credenciales de usuario y tokens de autenticación multifactor (MFA). Funciona interponiéndose entre el objetivo y una página web legítima.

La primera mención de EvilProxy se detectó a principios de mayo de 2022, cuando los actores que lo ejecutan publicaron un video de demostración que detalla cómo podría usarse para entregar enlaces de phishing avanzados con la intención de comprometer las cuentas de los consumidores que pertenecen a las principales marcas como Apple, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, Yandex y otros.

Algunos Conceptos:

A. **Autenticación Multifactor o MFA.-** Es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción. La autenticación multifactor combina dos o más credenciales independientes: lo que el usuario sabe, como una contraseña; lo que tiene el usuario, como un token de seguridad; y qué es el usuario, mediante el uso de métodos de verificación biométrica. El objetivo de MFA es crear una defensa en capas que dificulte que una persona no autorizada acceda a un objetivo. Si un factor se ve comprometido o roto, el atacante todavía tiene al menos una o más barreras que romper antes de entrar con éxito en el objetivo.

B. **Proxy Inverso.-** Es un servidor que se sitúa delante de los servidores web, intercepta y reenvía las solicitudes del cliente a esos servidores web. La diferencia entre un proxy de reenvío y uno inverso es sutil pero importante. Una forma simplificada de resumirla sería decir que un proxy de reenvío se sitúa delante de un cliente y se asegura de que ningún servidor de origen se comunique nunca directamente con ese cliente específico. Por otro lado, un proxy inverso se sitúa delante de un servidor de origen y se asegura de que ningún cliente se comunique nunca directamente con ese servidor de origen.

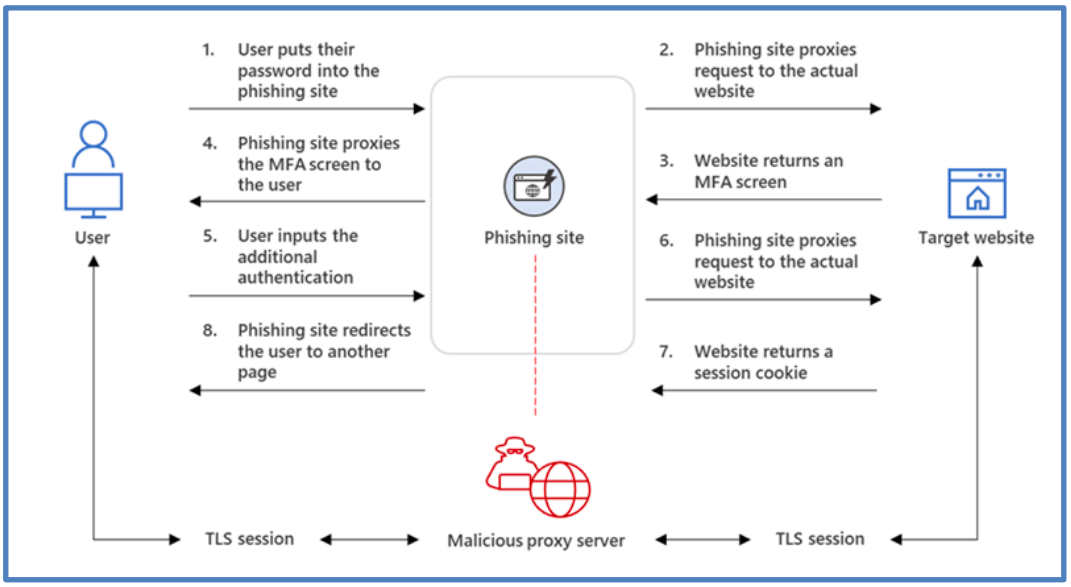


2. DETALLES:

La empresa de ciberseguridad ha observado una campaña a gran escala respaldada por EvilProxy, que combina suplantación de identidad de marca, evasión de detección de bots y redirecciones abiertas.

La nueva herramienta de phishing EvilProxy es anunciada en la clandestinidad por los delincuentes informáticos con la finalidad de evadir los controles de seguridad como por ejemplo la autenticación de 2 factores (2FA). Para realizar la evasión, los autores utilizan el método de inyección de cookies y proxy inverso con la finalidad de pasar por alto la 2FA.

El principio de "Proxy Inverso" se trata de lo siguiente: los ciberdelincuentes conducen a las víctimas a una página de phishing, usan el proxy inverso para obtener todo el contenido legítimo que el usuario espera, incluidas las páginas de inicio de sesión; es decir, se le presenta una página de inicio de sesión falsa que parece y actúa como el portal de inicio de sesión real, detectando su tráfico a medida que pasa por el proxy. De esta manera, pueden recolectar cookies de sesión válidas, capturando las credenciales del usuario y el token de sesión de autenticación, y así evitar la necesidad de autenticarse con nombres de usuario, contraseñas y/o tokens 2FA.



La compañía de seguridad adquirió videos publicados por actores de EvilProxy que demuestran cómo se puede robar la sesión de la víctima y pasar con éxito a través de los servicios de correo electrónico de Microsoft 2FA y Google.

EvilProxy se vende a los ciberdelincuentes por $400 al mes, prometiendo la capacidad de apuntar a las cuentas de Apple, Google, Facebook, Microsoft, Twitter, GitHub, GoDaddy y PyPI, y se puede acceder a ella a través de la red de TOR.

3. RECOMENDACIONES:

- Asegurarse de que los empleados y clientes reciben formación de concienciación en seguridad sobre todos los tipos de ataques de phishing, incluidos los mensajes de correo electrónico fraudulentos y las páginas de inicio de sesión falsas.
- Incorporar un software de solución avanzada que utilice algoritmos de aprendizaje automático para identificar y detener estas amenazas.
- Asegurarse de buscar una solución automatizada que identifique los ataques de usurpación de cuentas, así como evitar el acceso no autorizado a sus recursos sensibles en la nube.
- Programar evaluaciones periódicas de amenazas para identificar las vulnerabilidades que puedan ir surgiendo en el tiempo, y así mejorar la capacidad de respuesta ante incidentes.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/evilproxy-phishing-campaign-targets-120-000-microsoft-365-users/ • hxxps://www.resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web?&web_view=true • hxxps://www.cloudflare.com/es-es/learning/cdn/glossary/reverse-proxy/ • hxxps://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA • hxxps://www.proofpoint.com/es/blog/email-and-cloud-threats/defending-against-evilproxy-phishing-toolkit