Se ha estado haciendo cada vez más notoria una nueva técnica de phishing llamada «*archivador de archivos en el navegador*» para emular un software de archivador en un navegador web cuando una víctima visita un dominio con extensión .ZIP.

> *«Con este ataque de phishing, se simula un software de compresión de archivos (por ejemplo, WinRAR) en el navegador y usa un dominio .zip para que parezca más legítimo»*, dijo la semana pasada el investigador de seguridad mr.d0x.

Los hackers, en pocas palabras, podrían crear una página de inicio de phishing de aspecto realista usando HTML y CSS que imita el software de compresión de archivos legítimo y alojarlo en un dominio .zip, elevando así las campañas de ingeniería social.

En un escenario de ataque potencial, un atacante podría recurrir a dichos trucos para redirigir a los usuarios a una página de recolección de credenciales cuando se hace clic en un archivo «contenido» dentro del archivo ZIP falso.

> *«Otro caso de uso interesante es enumerar un archivo no ejecutable y cuando el usuario hace clic para iniciar una descarga, descarga un archivo ejecutable. Digamos que tiene un archivo 'factura.pdf'. Cuando un usuario hace clic en este archivo, se iniciará la descarga de un .exe o cualquier otro archivo»*, dijo mr.d0x.

Además de eso, la barra de búsqueda en el Explorador de archivos de Windows puede emerger como un conducto furtivo donde la búsqueda de un archivo .ZIP inexistente se abre directamente en el navegador web si el nombre del archivo corresponde a un dominio .zip legítimo.

> *«Esto es perfecto para este escenario, ya que el usuario esperaría ver un archivo .ZIP. Una vez que el usuario realice esto, se iniciará automáticamente el dominio*

> *.zip que tiene la plantilla del archivo, que parece bastante legítimo»,* dijo el investigador.

El desarrollo se produce cuando Google lanzó ocho nuevos dominios de nivel superior (TLD), incluyendo «.zip» y «.mov», que han generado algunas preocupaciones de que podría invitar al phishing y otros tipos de estafas en línea.

Esto se debe a que .ZIP y .MOV son nombres de extensión de archivos legítimos, lo que podría confundir a los usuarios desprevenidos para que visiten un sitio web malicioso en lugar de abrir un archivo y engañarlos para que descarguen accidentalmente malware.

> *«Los archivos .ZIP por lo general se usan como parte de la etapa inicial de una cadena de ataque, y generalmente se descargan después de que un usuario accede a una URL maliciosa o abre un archivo adjunto de correo electrónico»,* dijo Trend Micro.

> *«Más allá de que los archivos ZIP se usen como carga útil, también es probable que los actores maliciosos usen URL relacionadas con ZIP para descargar malware con la introducción del TLD .zip».*

Aunque las reacciones son decididamente mixtas sobre el riesgo que representa como resultado de la confusión entre los nombres de dominio y los nombres de archivo, se espera que equipe a los hackers con otro vector más para el phishing.

El descubrimiento también se produce cuando la compañía de seguridad cibernética Group-IB dijo que detectó un aumento del 25% en el uso de kits de phishing en 2022, identificando 3677 kits únicos, en comparación con el año anterior.

Es de particular interés el repunte en la tendencia del uso de Telegram para recopilar datos robados, casi duplicándose del 5.6% en 2021 al 9.4% en 2022.

> *«Los operadores de phishing crean carpetas aleatorias de sitios web a las que solo puede acceder el destinatario de una URL de phishing personalizada y no se puede acceder sin el enlace inicial»,* dijo la compañía.

> *«Esta técnica permite a los phishers evadir la detección y la lista negra, ya que el contenido de phishing no se revelará».*

Según un nuevo informe de Perception Point, la cantidad de ataques de phishing avanzados intentados por hackers en 2022 aumetó un 356%. El número total de ataques aumentó un 87% en el transcurso del año.

Esta evolución continua de los esquemas de phishing se ejemplifica con una nueva ola de ataques se han observado aprovechando cuentas comprometidas de Microsoft 365 y correos electrónicos cifrados con mensajes de permiso restringido (.rpmsg) para recopilar las credenciales de los usuarios.

> *«El uso de mensajes .rpmsg encriptados significa que el contenido de phishing del mensaje, incluidos los enlaces URL, se oculta de las puertas de enlace de escaneo de correo electrónico»,* dijeron los investigadores de Trustwave, Phil Hay y Rodel Mendrez.

Otra instancia destacada por Proofpoint implica el posible abuso de funciones legítimas en Microsoft Teams para facilitar la entrega de phishing y malware, incluyendo la utilización de invitaciones a reuniones posteriores al compromiso al reemplazar las URL predeterminadas con enlaces maliciosos a través de llamdas API.

> *«Un enfoque distinto que los atacantes pueden usar, dado el acceso al token de Teams de un usuario, es utilizar la API o la interfaz de usuario de Teams para armar los enlaces existentes en los mensajes enviados»*, dijo la empresa de seguridad.

> *«Esto podría hacerse simplemente reemplazando los enlaces benignos con enlaces que apuntan a sitios web nefastos o recursos maliciosos».*