Los agentes de amenazas están cada vez más empleando un conjunto de herramientas de phishing como servicio (PhaaS) conocido como EvilProxy para llevar a cabo ataques de usurpación de cuentas dirigidos a altos ejecutivos en destacadas empresas.

Según Proofpoint, una campaña híbrida en curso ha utilizado este servicio para apuntar a miles de cuentas de usuarios de Microsoft 365, enviando aproximadamente 120,000 correos electrónicos de phishing a cientos de organizaciones en todo el mundo entre marzo y junio de 2023.

Casi el 39% de los cientos de usuarios comprometidos se dice que son ejecutivos de nivel C, incluyendo directores ejecutivos (9%) y directores financieros (17%). Los ataques también han focalizado al personal con acceso a activos financieros o información delicada. Al menos el 35% de todos los usuarios comprometidos tenían habilitadas protecciones de cuenta adicionales.

Estas campañas se perciben como una reacción a la creciente adopción de la autenticación multifactorial (MFA) en las empresas, lo que ha llevado a los agentes de amenazas a adaptar sus tácticas para eludir las nuevas capas de seguridad mediante la inclusión de kits de phishing de adversario-en-el-medio (AitM) para extraer credenciales, cookies de sesión y contraseñas de un solo uso.

> *«Los atacantes utilizan una nueva automatización avanzada para determinar con precisión en tiempo real si un usuario víctima de phishing es un perfil de alto nivel, y obtienen acceso inmediato a la cuenta, pasando por alto perfiles de phishing menos lucrativos»,* dijo la firma de seguridad empresarial.

EvilProxy fue registrado por primera vez por Resecurity en septiembre de 2022, detallando su capacidad para comprometer cuentas de usuarios relacionadas con Apple iCloud, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, NPM, PyPI, RubyGems, Twitter, Yahoo y Yandex, entre otros.

Se comercializa como una suscripción por $400 al mes, una cifra que puede aumentar a $600 para las cuentas de Google.

Las herramientas de tipo PhaaS representan una evolución en la economía del cibercrimen, reduciendo las barreras para que los delincuentes con habilidades técnicas más modestas puedan llevar a cabo ataques de phishing sofisticados a gran escala de manera fluida y rentable.

> *«Hoy en día, un atacante solo necesita configurar una campaña utilizando una interfaz de apuntar y hacer clic con opciones personalizables, como la detección de bots, proxies y geovallado»,* señalaron los investigadores de seguridad Shachar Gritzman, Moshe Avraham, Tim Kromphardt, Jake Gionet y Eilon Bendet.

> *«Esta interfaz relativamente sencilla y de bajo costo ha abierto las puertas a una actividad exitosa de phishing con autenticación multifactor (MFA)».*

La última oleada de ataques comienza con correos electrónicos de phishing que se hacen pasar por servicios confiables como Adobe y DocuSign para engañar a los destinatarios y lograr que hagan clic en URL maliciosas. Estas URL activan una serie de redirecciones en varias etapas que llevan a los usuarios a una página de inicio de sesión falsa de Microsoft 365. Esta página funciona como un proxy inverso para capturar de manera sigilosa la información ingresada en el formulario.

Pero en un giro interesante, los ataques evitan intencionalmente el tráfico de usuarios que proviene de direcciones IP turcas al redirigirlos a sitios web legítimos. Esto podría indicar que los operadores de la campaña podrían tener su base en el país.

Después de lograr un exitoso control de cuenta, el actor de amenazas procede a *«afianzar su posición»* en el entorno en la nube de la organización añadiendo su propio método de

autenticación multifactor (MFA), como una aplicación de autenticación de dos factores, con el propósito de obtener un acceso remoto persistente y llevar a cabo movimientos laterales y propagación de malware.

Luego, este acceso se convierte en una fuente de beneficios al utilizarse para realizar fraudes financieros, extraer datos confidenciales o vender las cuentas de usuario comprometidas a otros atacantes.

> *«Las amenazas de proxy inverso (y en particular EvilProxy) son una amenaza poderosa en el panorama dinámico actual y están superando a los kits de phishing menos capaces del pasado. Ni siquiera el MFA es una solución infalible contra amenazas sofisticadas basadas en la nube»,* comentaron los investigadores,

> *«Aunque el punto de entrada inicial de estos ataques sea el correo electrónico, su objetivo final es comprometer y explotar valiosas cuentas de usuario en la nube, así como activos y datos».*

La evolución se presenta mientras Imperva detalla información sobre una campaña en curso de origen ruso que busca engañar a posibles objetivos y robar sus datos bancarios y de tarjetas de crédito desde al menos mayo de 2022 a través de enlaces maliciosos compartidos en mensajes de WhatsApp.

Esta actividad abarca 800 dominios de estafa distintos, haciéndose pasar por más de 340 compañías en 48 idiomas. Esto incluye bancos reconocidos, servicios postales, empresas de envío de paquetes, redes sociales y sitios de comercio electrónico.

> *«Al aprovechar una aplicación de página única de alta calidad, los estafadores pudieron crear un sitio web convincente que imitaba a uno legítimo, engañando a*

> *los usuarios y generando una falsa sensación de seguridad»,* explicó Imperva.

En una variación adicional de un ataque de ingeniería social identificado por eSentire, se ha observado que actores maliciosos contactan a profesionales de marketing en LinkedIn con el fin de distribuir un malware de carga basado en .NET llamado HawkEyes, que a su vez se utiliza para lanzar Ducktail, un recolector de información que se enfoca en recopilar datos de cuentas comerciales de Facebook.

> *«Se sabe que Ducktail tiene como objetivo las cuentas comerciales y de anuncios de Facebook. Los operadores utilizarán los datos de inicio de sesión robados para añadir direcciones de correo electrónico a las cuentas comerciales de Facebook. Cuando se añaden los correos electrónicos, se genera un enlace de registro a través del cual el actor de amenazas puede otorgarse acceso»,* informaron los investigadores de eSentire.