Un nuevo conjunto de herramientas de phishing como servicio (PhaaS) denominado EvilProxy se anuncia en la clandestinidad criminal como un medio para que los atacantes eludan las protecciones de autenticación de dos factores (2FA) empleadas contra los servicios en línea.

> *«Los actores de EvilProxy están usando métodos de inyección de cookies y proxy inverso para eludir la autenticación 2FA, lo que hace que la sesión de la víctima sea un proxy»*, dijeron los investigadores de Resecurity.

La plataforma genera enlaces de phishing que no son más que páginas clonadas diseñadas para comprometer cuentas de usuarios asociadas con Apple iCloud, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, NPM, PyPI, RubyGems, Twitter, Yahoo y Yandex.

EvilProxy es similar a los ataques de adversario en el medio (AiTM) en el sentido de que los usuarios interactúan con un servidor proxy malicioso que actúa como intermediario para el sitio web de destino, recopilando de forma encubierta las credenciales y códigos de acceso 2FA ingresados en las páginas de inicio de sesión.

Se ofrece por suscripción por servicio en un período de tiempo de 10, 20 o 31 días, con el kit disponible por $400 dólares al mes y se accede por medio de la red de anonimato TOR luego de que el pago se organiza de forma manual con un operador en Telegram. Los ataques contra las cuentas de Google, por el contrario, cuestan hasta 600 dólares al mes.

> *«Después de la activación, se pedirá al operador que proporcione credenciales SSH para implementar aún más un contenedor Docker y un conjunto de scripts»*, dijo Resecurity.

La compañía agregó que la técnica refleja la de otro servicio PhaaS llamado Frappo, que salio

a la luz a inicios de 2022.

Aunque la venta de EvilProxy a posibles clientes está sujeta a la investigación de antecedentes por parte de los atacantes, no hace falta decir que el servicio ofrece una *«solución rentable y escalable»* para realizar ataques de ingeniería social.

El desarrollo es una indicación más de que los atacantes están actualizando su arsenal de ataques para orquestar sofisticadas campañas de phishing dirigidas a los usuarios de una forma que pueda vencer las salvaguardas de seguridad existentes.

Por otro lado, la orientación de código público y repositorios de paquetes como GitHub, NPM, PyPI y RubyGems sugiere que los operadores también tienen como objetivo facilitar los ataques a la cadena de suministro por medio de dichas operaciones.

Obtener acceso no autorizado a cuentas e inyectar código malicioso en proyectos ampliamente usados por desarrolladores confiables puede ser una mina de oro para los actores de amenazas, lo que amplía de forma significativa el impacto de las campañas.

> *«Es muy probable que los actores apunten a los desarrolladores de software e ingenieros de TI para obtener acceso a sus repositorios con el objetivo final de hackear objetivos descendentes»,* dijeron los investigadores.