Expertos en ciberseguridad han revelado un nuevo kit de phishing del tipo *«adversario en el medio»* (AitM, por sus siglas en inglés) diseñado para atacar cuentas de Microsoft 365, con el objetivo de sustraer credenciales y códigos de autenticación en dos pasos (2FA). Este kit ha estado activo al menos desde octubre de 2024.

Este nuevo kit de phishing, denominado Sneaky 2FA por la empresa de ciberseguridad francesa Sekoia, fue identificado en diciembre. Hasta la fecha, se han detectado casi 100 dominios que alojan páginas de phishing de Sneaky 2FA, lo que sugiere que está siendo utilizado por un número moderado de actores maliciosos.

> *«El kit se ofrece como un servicio de phishing (PhaaS, Phishing-as-a-Service) por el grupo de ciberdelincuencia 'Sneaky Log,' que utiliza un bot totalmente funcional en Telegram. Los clientes reciben acceso a una versión ofuscada y con licencia del código, que implementan de forma independiente»,* señaló Sekoia en su análisis.

Las campañas de phishing asociadas a este kit envían correos electrónicos relacionados con recibos de pago falsos para convencer a las víctimas de abrir documentos PDF fraudulentos que incluyen un código QR. Al escanearlo, los usuarios son redirigidos a las páginas de phishing de Sneaky 2FA.

Sekoia explicó que estas páginas falsas se alojan en infraestructura comprometida, principalmente sitios web basados en WordPress y otros dominios controlados por los atacantes. Las páginas fraudulentas están diseñadas para completar automáticamente la dirección de correo electrónico de las víctimas, lo que aumenta su apariencia de autenticidad.

El kit también implementa medidas avanzadas para evitar bots y análisis, como el filtrado de tráfico y desafíos de Cloudflare Turnstile, garantizando que solo las víctimas que cumplan ciertos requisitos sean redirigidas a las páginas de captura de credenciales. Asimismo, realiza verificaciones técnicas para identificar y frustrar intentos de análisis mediante herramientas de desarrollo web.

Un elemento interesante de este PhaaS es que los visitantes cuyo IP proviene de centros de datos, proveedores de nube, bots, proxys o VPNs son redirigidos a una página de Wikipedia sobre Microsoft mediante el servicio href[.]li. Esta táctica llevó a TRAC Labs a apodarlo WikiKit.

> *«El kit Sneaky 2FA utiliza imágenes desenfocadas como fondo en sus páginas falsas de autenticación de Microsoft. Estas imágenes, que son capturas de pantalla de interfaces legítimas de Microsoft, buscan engañar a los usuarios para que ingresen sus credenciales y accedan al contenido desenfocado»*, indicó Sekoia.

La investigación también reveló que el kit se conecta a un servidor central, probablemente gestionado por los operadores, para confirmar que la suscripción esté activa. Esto significa que solo los clientes con una clave de licencia válida pueden emplear Sneaky 2FA en sus campañas de phishing. El servicio tiene un costo de $200 al mes.

Además, referencias en el código fuente sugieren un vínculo con un grupo de phishing conocido como W3LL Store, expuesto previamente por Group-IB en septiembre de 2023. Este grupo estaba detrás de un kit de phishing llamado W3LL Panel y otras herramientas diseñadas para comprometer correos electrónicos empresariales (BEC).

Las similitudes en la implementación del relay AitM también han llevado a considerar que Sneaky 2FA podría estar basado en W3LL Panel, que opera con un modelo de licencias similar, requiriendo validaciones periódicas con un servidor central.

En un giro adicional, algunos dominios vinculados a Sneaky 2FA fueron utilizados previamente por kits de phishing AitM conocidos, como Evilginx2 y Greatness, lo que indica que ciertos actores maliciosos han comenzado a usar este nuevo servicio.

> *«El kit emplea cadenas de User-Agent codificadas de manera específica para las solicitudes HTTP según el paso del proceso de autenticación. Este comportamiento es poco común en procesos legítimos de autenticación, ya que implicaría realizar pasos consecutivos desde navegadores diferentes»,* dijeron los investigadores de Sekoia.
>
> *«Aunque las transiciones de User-Agent pueden ocurrir en escenarios legítimos (por ejemplo, autenticación iniciada en aplicaciones de escritorio que abren navegadores web o WebView para manejar 2FA), la secuencia utilizada por Sneaky 2FA no corresponde a un caso realista, lo que permite identificar el kit con alta precisión».*