Se ha observado una nueva campaña de phishing a gran escala que utiliza técnicas de adversario en le medio (AitM) para eludir las protecciones de seguridad y comprometer las cuentas de correo electrónico de empresas.

> *«Utiliza una técnica de ataque de adversario en el medio (AitM) capaz de eludir la autenticación de múltiples factores. La campaña está diseñada específicamente para llegar a los usuarios finales de las empresas que utilizan los servicios de correo electrónico de Microsoft»,* dijeron los investigadores de Zscaler, Sudeep Singh y Jagadeeswar Ramanukolanu.

Los objetivos destacados incluyen fintech, préstamos, seguros, energía, fabricación y coopertivas de ahorro y crédito federales ubicadas en Estados Unidos, Reino Unido, Nueva Zelanda y Australia.

Esta no es la primera vez que un ataque de phishing de este tipo sale a la luz. El mes pasado, Microsoft reveló que, desde septiembre de 2021, más de 10,000 organizaciones fueron afectadas mediante técnicas AitM para violar cuentas protegidas con autenticación multifactor (MFA).

La campaña en curso, a partir de junio de 2022, comienza con un correo electrónico con el tema de una factura enviado a los objetivos que contiene un archivo adjunto HTML, que incluye una URL de phishing incrustada.

Al abrir el archivo adjunto por medio de un navegador web, se redirige al destinatario del correo electrónico a la página de phishing que se hace pasar por una página de inicio de sesión de Microsoft Office, pero no antes de tomar las huellas digitales de la máquina comprometida para determinar si la víctima es realmente el objetivo previsto.

Lo que destaca aquí es el uso de distintos métodos, contando las páginas de redirección abiertas alojadas por Google Ads y Snapchat, para cargar la URL de la página de phishing en lugar de incrustar la URL maliciosa directamente en el correo electrónico.

Los ataques de phishing de AitM van más allá de los enfoques de phishing tradicionales diseñados para saquear las credenciales de usuarios involuntarios, particularmente en escenarios donde MFA está habilitado, una barrera de seguridad que evita que el atacante inicie sesión en la cuenta solo con las credenciales robadas.

Para eludir esto, la página de inicio no autorizada desarrollada utilizando un kit de phishing funciona como un proxy que captura y transmite toda la comunicación entre el cliente (es decir, la víctima) y el servidor de correo electrónico.

> *«Los kits interceptan el contenido HTML recibido de los servidores de Microsoft, y antes de retransmitirlo a la víctima, el kit manipula el contenido de varias formas según sea necesario, para asegurarse de que el proceso de phishing funciones»,* dijeron los investigadores.

Esto también implica reemplazar todos los enlaces a los dominios de Microsoft con enlaces equivalentes al dominio de phishing para garantizar que el ida y vuelta permanezca intacto con el sitio web fraudulento durante toda la sesión.

Zscaler dijo que observó que el atacante iniciaba sesión manualmente en la cuenta ocho minutos después del robo de credenciales, seguía leyendo correos electrónicos y verificando la información del perfil del usuario.

Además, en algunos casos, las bandejas de entrada de correo electrónico pirateadas se utilizan posteriormente para enviar correos electrónicos de phishing adicionales como parte de la misma campaña para realizar estafas de compromiso de correo electrónico comercial (BEC).

> *«Aunque las características de seguridad como la autenticación multifactor (MFA) agregan una capa adicional de seguridad, no deben considerarse como una bala de plata para proteger contra los ataques de phishing»*, dijeron los investigadores.

> *«Con el uso de kits de phishing avanzados (AitM) y técnicas de evasión inteligentes, los atacantes pueden eludir tanto las soluciones de seguridad tradicionales como las avanzadas».*