Un grupo de hackers detrás de una campaña de phishing a gran escala del tipo Adversary-in-the-middle (AiTM) dirigida a los usuarios empresariales de los servicios de correo electrónico de Microsoft, también pusieron su mirada en los usuarios de Google Workspace.

> *«Esta campaña se dirigió específicamente a los directores ejecutivos y otros miembros senior de varias organizaciones que utilizan [Google Workspace]»,* dijeron los investigadores de Zscaler, Sudeep Singh y Jagadeeswar Ramanukolanu.

Las investigaciones sugieren que los ataques de phishing de AiTM comenzaron a mediados de julio de 2022, siguiendo un modus operandi similar al de una campaña de ingeniería social diseñada para desviar las credenciales de Microsoft de los usuarios e incluso, eludir la autenticación multifactor.

La campaña de phishing de Gmail AiTM de bajo volumen también implica el uso de los correos electrónicos comprometidos de los directores ejecutivos para realizar más ingeniería social, y los ataques también usan varios dominios comprometidos como un redireccionador de URL intermedio para llevar a las víctimas a la página de destino final.

Las cadenas de ataque implican el envío de correos electrónicos de caducidad de contraseña a objetivos potenciales que contienen un enlace malicioso incrustado para supuestamente *«ampliar su acceso»,* tocando lo que lleva al destinatario a abrir páginas de redirección de Google Ads y Snapchat para cargar la URL de la página de phishing.

Además del abuso de redireccionamiento abierto, una segunda variante de los ataques se basa en sitios infectados que albergan una versión codificada en Base64 del redireccionador de la siguiente etapa y la dirección de correo electrónico de la víctima en la URL. Este redirector intermedio es un código JavaScript que apunta a una página de phishing de Gmail.

En un caso destacado por Zscaler, la página de redireccionamiento utilizada en el ataque de phishing de Microsoft AiTM el 11 de julio de 2022 se actualizó para llevar al usuario a una página de phishing de Gmail AiTM el 16 de julio de 2022, conectando las dos campañas con

el mismo atacante.

> *«También hubo una superposición de infraestructura, e incluso identificamos varios casos en los que el actor de amenazas cambió el phishing de Microsoft AiTM al phishing de Gmail usando la misma infraestructura»,* dijeron los investigadores.

Los hallazgos son una indicación de que las salvaguardias de autenticación multifactor por sí solas no pueden ofrecer protección contra ataques de phishing avanzados, lo que requiere que los usuarios analicen las URL antes de ingresar las credenciales y se abstengan de abrir archivos adjuntos o hacer clic en enlaces de correos electrónicos enviados desde fuentes no confiables o desconocidas.