Microsoft advirtió sobre una campaña de suplantación de identidad de credenciales generalizada que aprovecha los enlaces de redireccionamiento abiertos en las comunicaciones por correo electrónico, como un vector para engañar a los usuarios con el fin de que visiten sitios web maliciosos sin pasar por alto el software de seguridad.

> *«Los atacantes combinan estos enlaces con cebos de ingeniería social que se hacen pasar por herramientas y servicios de productividad conocidos para atraer a los usuarios a hacer clic»,* dijo el equipo de Inteligencia de Amenazas de Microsoft 365 Defender.
>
> *«Hacerlo conduce a una serie de redirecciones, incluida una página de verificación CAPTCHA que agrega un sentido de legitimidad e intenta evadir algunos sistemas de análisis automatizados, antes de llevar al usuario a una página de inicio de sesión falsa. Esto, en última instancia, conduce a un compromiso de credenciales, lo que abre al usuario y su organización a otros ataques»,* agregaron los investigadores.

Aunque los enlaces de redireccionamiento en los mensajes de correo electrónico son una herramienta vital para llevar a los destinatarios a sitios web de terceros o realizar un seguimiento de las tasas de clics y medir el éxito de las campañas de ventas y marketing, los adversarios pueden abusar de la misma técnica para redirigir dichos enlaces a su propia infraestructura, al mismo tiempo, mantener intacto el dominio de confianza en la URL completa para evadir el análisis de los motores anti malware, aún cuando los usuarios intentan desplazarse sobre los enlaces para comprobar si hay signos de contenido sospechoso.

Para llevar a las víctimas potenciales a sitios de phishing, las URL de redireccionamiento incrustadas en el mensaje de configuran mediante un servicio legítimo, mientras que los

dominios finales controlados por el actor contenidos en el enlace aprovechan los dominios de nivel superior .xyz, .club, .shop y .online, pero que se pasan como parámetros para esconderse de las soluciones de pasarela de correo electrónico.

Microsoft informó que observó al menos 350 dominios de phishing únicos como parte de la campaña, otro intento de ocultar la detección, subrayando el uso efectivo de la campaña de señuelos de ingeniería social convincentes que pretenden ser mensajes de notificación de aplicaciones como Office 365 y Zoom, un sistema bien diseñado como técnica de detección de evasión y una infraestructura duradera para llevar a cabo los ataques.

> *«Esto no solo muestra la escala con la que se está llevando a cabo este ataque, sino que también demuestra cuánto están invirtiendo los atacantes en él, lo que indica beneficios potencialmente significativos»,* dijo el investigador.

Para darle al ataque una apariencia de autenticidad, hacer clic en los enlaces especialmente diseñados redirige a los usuarios a una página de destino maliciosa que emplea Google reCaptcha para bloquear cualquier intento de escaneo dinámico. Una vez completada la verificación CAPTCHA, a las víctimas se les muestra una página de inicio de sesión fraudulenta que imita un servicio conocido como Microsoft Office 365, solo para deslizar sus contraseñas al enviar la información.

> *«Esta campaña de phishing ejemplifica la tormenta perfecta de ingeniería social, evasión de detección y una gran infraestructura de ataque en su intento de robar credenciales y finalmente infiltrarse en una red. Y dado que el 91% de todos los ciberataques se originan en el correo electrónico, las organizaciones deben tener una solución de seguridad que les proporcione una defensa de varios niveles contra este tipo de ataques»,* dijeron los investigadores.