Microsoft advirtió el jueves sobre un ataque dirigido al consumidor, que hizo uso de aplicaciones OAuth no autorizadas implementadas en inquilinos de la nube comprometidos para que, en última instancia, tomen el control de los servidores de Exchange y propaguen spam.

> *«El actor de amenazas lanzó ataques de relleno de credenciales contra cuentas de alto riesgo que no tenían habilitada la autenticación multifactor (MFA) y aprovechó las cuentas de administrador no seguras para obtener acceso inicial»,* dijo el equipo de investigación de Microsoft 365 Defender.

El acceso no autorizado al inquilino de la nube permitió al adversario registrar una aplicación OAuth maliciosa y otorgarle permisos elevados, y finalmente, modificar la configuración del servidor de Exchange para permitir que los correos electrónicos entrantes de diferentes direcciones IP específicas se enruten por medio del servidor de correo electrónico comprometido.

> *«Estas modificaciones en la configuración del servidor de Exchange permitieron que el actor de amenazas realizara su objetivo principal en el ataque: enviar correos electrónicos no deseados. Los correos electrónicos no deseados se enviaron como parte de un esquema de sorteo engañoso destinado a engañar a los destinatarios que se registren en suscripciones pagas recurrentes»,* dijo Microsoft.

Los mensajes de correo electrónico instaban a los destinatarios a hacer clic en un enlace para recibir un premio, lo que redirigiría a las víctimas a una página de destino que les pedía que ingresaran los detalles de su tarjeta de crédito por una pequeña tarifa de envío para cobrar la recompensa.

El atacante llevó a cabo una serie de pasos para evadir la detección y continuar sus operaciones durante períodos prolongados de tiempo, incluido tomarse semanas o incluso

meses para usar la aplicación OAuth maliciosa después de que se configuró y eliminar las modificaciones realizadas en el servidor de Exchange después de cada campaña de spam.

La división de inteligencia de amenazas de Microsoft dijo que el atacante ha estado ejecutando activamente campañas de correo electrónico no deseado durante varios años, generalmente enviando grandes volúmenes de correos electrónicos no deseados en ráfagas cortas por medio de una variedad de métodos.

Aunque el objetivo principal del ataque parece ser engañar a los usuarios involuntarios para que se registren en servicios de suscripción no deseados, podría haber representado una amenaza mucho más grave si se hubiera utilizado la misma técnica para robar credenciales o distribuir malware.

> *«Mientras que la campaña de spam de seguimiento se dirige a las cuentas de correo electrónico de los consumidores, este ataque se dirige a los inquilinos empresariales para usarlos como infraestructura para la campaña. Este ataque expone las vulnerabilidades de seguridad que podrían ser utilizadas por otros actores de amenazas en ataques que podrían afectar directamente a las empresas afectadas»,* dijo Microsoft.