Investigadores en ciberseguridad han revelado detalles de una campaña de phishing en la que los atacantes se hacen pasar por mensajes legítimos generados por Google, abusando del servicio Application Integration de Google Cloud para distribuir correos electrónicos.

Según indicó Check Point, la actividad explota la confianza asociada a la infraestructura de Google Cloud al enviar los mensajes desde una dirección de correo legítima (*"noreply-application-integration@google[.]com"*), lo que les permite evadir los filtros tradicionales de seguridad del correo y aumentar las probabilidades de llegar a la bandeja de entrada de los usuarios.

"Los correos imitan notificaciones empresariales rutinarias, como alertas de buzón de voz y solicitudes de acceso o permisos a archivos, lo que los hace parecer normales y confiables para los destinatarios", señaló la empresa de ciberseguridad.

Se ha observado que los atacantes enviaron 9,394 correos de phishing dirigidos a aproximadamente 3,200 clientes durante un periodo de 14 días en diciembre de 2025, con organizaciones afectadas en Estados Unidos, Asia-Pacífico, Europa, Canadá y América Latina.

En el núcleo de la campaña se encuentra el abuso de la tarea "Send Email" de Application Integration, que permite a los usuarios enviar notificaciones personalizadas desde una integración. Google aclara en su documentación de soporte que solo se puede agregar un máximo de 30 destinatarios a esta tarea.

El hecho de que estos correos puedan configurarse para enviarse a direcciones arbitrarias demuestra la capacidad del actor malicioso para aprovechar una función legítima de automatización en su beneficio y enviar mensajes desde dominios propiedad de Google, eludiendo de manera efectiva las verificaciones DMARC y SPF.

"Para aumentar aún más la confianza, los correos seguían de cerca el estilo y la estructura de las notificaciones de Google, incluyendo formatos y lenguaje familiares", afirmó Check Point. *"Los señuelos solían hacer referencia a mensajes de voz o a supuestos accesos concedidos a archivos o documentos compartidos, como un archivo 'Q4', incitando a los*

destinatarios a hacer clic en enlaces incrustados y actuar de inmediato”.

La cadena de ataque consiste en un flujo de redirecciones de varias etapas que comienza cuando el destinatario del correo hace clic en un enlace alojado en storage.cloud.google[.]com, otro servicio confiable de Google Cloud. Esta estrategia busca reducir la desconfianza del usuario y dotar al ataque de una apariencia de legitimidad.

Posteriormente, el enlace redirige al usuario a contenido servido desde googleusercontent[.]com, donde se presenta un CAPTCHA falso o una verificación basada en imágenes. Este paso actúa como barrera para bloquear escáneres automatizados y herramientas de seguridad, permitiendo que los usuarios reales continúen.

Una vez superada la fase de validación, la víctima es dirigida a una página de inicio de sesión falsa de Microsoft alojada en un dominio que no pertenece a Microsoft, donde finalmente se roban las credenciales introducidas.

Como respuesta a estos hallazgos, Google bloqueó los intentos de phishing que abusaban de la función de notificaciones por correo dentro de Google Cloud Application Integration y afirmó que está implementando medidas adicionales para evitar futuros abusos.

El análisis de Check Point reveló que la campaña se dirigió principalmente a los sectores de manufactura, tecnología, finanzas, servicios profesionales y comercio minorista, aunque también se identificaron objetivos en otras industrias como medios de comunicación, educación, salud, energía, gobierno, viajes y transporte.

“Estos sectores suelen depender de notificaciones automatizadas, documentos compartidos y flujos de trabajo basados en permisos, lo que hace que las alertas con marca de Google resulten especialmente convincentes”, añadió. *“Esta campaña pone de manifiesto cómo los atacantes pueden explotar funciones legítimas de automatización y flujos de trabajo en la nube para distribuir phishing a gran escala sin recurrir a la suplantación tradicional”*.

Actualización

Tanto xorlab como Ravenmail han dado a conocer detalles adicionales de la campaña de robo de credenciales. En particular, xorlab señaló que los ataques también se utilizan para llevar a cabo phishing de consentimiento OAuth, además de alojar las páginas falsas de inicio de sesión en buckets S3 de Amazon Web Services (AWS).

"Los atacantes engañan a las víctimas para que otorguen a una aplicación maliciosa de Azure AD acceso a sus recursos en la nube, obteniendo acceso a suscripciones de Azure, máquinas virtuales, almacenamiento y bases de datos mediante permisos delegados que persisten a través de tokens de acceso y actualización", explicó xorlab.

"Cada salto utiliza infraestructura confiable —Google, Microsoft y AWS— lo que hace que el ataque sea difícil de detectar o bloquear en un solo punto. Independientemente del punto de entrada, las víctimas terminan llegando a la página de inicio de sesión de Microsoft 365, lo que revela el objetivo principal de los atacantes: las credenciales de M365".