Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°171	Fecha: 24-07-2024 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos abusan de Google Cloud para realizar phishing		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Los piratas informáticos utilizan plataformas de todo tipo para lanzar sus ataques y campañas maliciosas. Pueden hacer uso de redes sociales, del correo electrónico o de la nube, entre otros muchos. En este caso, están utilizando la nube de Google para realizar ataques Phishing.

Google Cloud es el objetivo debido a sus amplios y potentes recursos, que podrían utilizarse para una multitud de actividades maliciosas.

La enorme cantidad de datos y la capacidad de procesamiento que ofrecen los servicios de Google Cloud suelen atraer a los actores maliciosos. Debido a la complejidad de los entornos de la nube, esto también puede permitirles pasar desapercibidos.

2. DETALLES:

Google Cloud Threat Horizons reveló recientemente que los piratas informáticos han estado abusando activamente de Google Cloud para realizar phishing.

El informe Google Cloud Threat Horizons, elaborado por varios equipos de Google, como TAG y Mandiant, revela inteligencia estratégica sobre amenazas a la seguridad de la nube entre proveedores.

Los profesionales de seguridad en la nube deben tener en cuenta tres áreas clave a la hora de desarrollar estrategias para abordar las amenazas emergentes de la nube sin servidor. Estas incluyen la mitigación de los riesgos derivados de las configuraciones incorrectas de los clientes y el aprovechamiento de la capacidad de expansión y la reducción de los costos operativos.

Las consideraciones que deben priorizarse son:

Credenciales comprometidas. Las contraseñas débiles o inexistentes siguen siendo la principal vía de entrada ilícita.

Configuración incorrecta explotada. Las configuraciones erróneas afectan a más del 30% de los casos y en su mayoría involucran claves de cuentas de servicio gratuitas.

Distribución de malware. Los cibercriminales, podrían distribuir de forma masiva software malicioso de todo tipo. Pueden ser keyloggers, ransomware, spyware, etc.

3. RECOMENDACIONES:

- Administrar estrictamente las cuentas con altos privilegios. Aplicar el principio del mínimo privilegio en las demás cuentas.
- Implementar controles de detección de malware. Colaborar con CISA para el análisis de malware. Utilizar la detección de amenazas de contenedores. Evitar los contenedores que no sean de confianza. Configurar los ajustes de red de Cloud Functions. Controlar el ingreso y egreso de la red para Cloud Run.
- Tener el equipo actualizado. Asegurarse de usar siempre las últimas versiones, ya sea del sistema operativo o de cualquier otro programa que tengas instalado.

Fuente de Información:	• hxxps://gbhackers.com/hackers-abusing-google-cloud/ • hxxps://www.redeszone.net/noticias/seguridad/nube-google-robo-contrasenas/