Los hackers están explotando instancias de Google Cloud Platform (GCP) incorrectamente aseguradas, para descargar software de minería de criptomonedas a los sistemas comprometidos, así como abusar de su infraestructura para instalar ransomware, organizar campañas de phishing e incluso, generar tráfico a videos de YouTube para la manipulación del conteo de vistas.

«Aunque los clientes de la nube siguen enfrentándose a una variedad de amenazas en las aplicaciones e infraestructura, muchos ataques exitosos se deben a una falta de higiene y falta de implementación de control básico», dijo el Equipo de Acción de Ciberseguridad (CAT) de Google, como parte de su reciente informe Threat Horizons publicado la semana pasada.

De las 50 instancias de GCP comprometidas recientemente, el 86% de ellas se utilizaron para realizar minería de criptomonedas, en algunos casos dentro de los 22 segundos posteriores a la violación exitosa, mientras que el 10% de las instancias fueron explotadas para realizar escaneos de otros hosts de acceso público en Internet para identificar sistemas vulnerables, y el 8% de las instancias se usaron para atacar a otras entidades. Aproximadamente el 6% de las instancias de GCP se utilizaron para alojar software malicioso.

En la mayoría de los casos, el acceso no autorizado se atribuyó al uso de contraseñas débiles o nulas para cuentas de usuario o conexiones API (48%), vulnerabilidades en software de terceros instalado en las instancias en la nube (26%) y filtración de credenciales de proyectos en GitHub (4%).

Otro ataque notable fue una campaña de phishing de Gmail lanzada por ATP28 (también conocido como Fancy Bear), hacia fines de septiembre de 2021, que implicó el envío de un correo electrónico masivo a más de 12 mil titulares de cuentas principalmente en Estados Unidos, Reino Unido, Canadá, India, Rusia, Brasil y naciones de la UE, con el objetivo de robar sus credenciales.

Además, Google CAT dijo que observó a los adversarios abusando de los créditos gratuitos en la nube mediante el uso de proyectos de prueba y haciéndose pasar por startups falsas para generar tráfico en YouTube.

En otro incidente, un grupo de atacantes respaldado por el gobierno de Corea del Norte se hizo pasar por reclutadores de Samsung para enviar oportunidades de trabajo falsas a los empleados de varias empresas de seguridad de la información de Corea del Sur, que venden soluciones anti-malware.

> *«Los correos electrónicos incluían un PDF que supuestamente afirmaba ser una descripción de trabajo para un puesto en Samsung; sin embargo, los PDF tenían un formato incorrecto y no se abrían en un lector PDF estándar. Cuando los objetivos respondieron que no podían abrir la descripción del trabajo, los atacantes respondieron con un enlace malicioso a malware que pretendía ser un lector de PDF seguro almacenado en Google Drive que ahora fue bloqueado»,* dijeron los investigadores.

Google conectó los ataques al mismo actor de amenazas que previamente puso su mirada en los profesionales de seguridad que trabajan en investigación y desarrollo de vulnerabilidades a inicios del año para robar exploits y organizar más ataques contra objetivos vulnerables a su elección.

> *«Los recursos alojados en la nube tienen el beneficio de una alta disponibilidad y acceso en cualquier lugar, en cualquier momento. Si bien los recursos alojados en la nube agilizan las operaciones de la fuerza laboral, los atacantes pueden intentar aprovechar la naturaleza ubicua de la nube para comprometer los recursos de la misma. A pesar de la creciente atención pública a la seguridad cibernética, las tácticas de ingeniería social y el spear-phishing suelen tener éxito»,* dijo Google CAT.