Una recién iniciada campaña conocida como EleKtra-Leak se ha enfocado en las credenciales de gestión de identidad y acceso (IAM) de Amazon Web Service (AWS) expuestas en repositorios públicos de GitHub con el propósito de facilitar actividades de cripto-minería.

> *«Como resultado de esto, el actor de amenazas relacionado con la campaña ha logrado crear múltiples instancias de AWS Elastic Compute (EC2) que utilizaron para llevar a cabo operaciones extensas y de larga duración de cripto-minería,»* afirmaron los investigadores de Palo Alto Networks Unit 42, en un informe técnico.

La operación, en curso desde al menos diciembre de 2020, está diseñada para minar Monero utilizando hasta 474 instancias únicas de Amazon EC2 entre el 30 de agosto y el 6 de octubre de 2023.

Un elemento destacado de estos ataques es la rápida identificación automatizada de las credenciales IAM de AWS en GitHub, tan solo cuatro minutos después de su exposición inicial. Esto sugiere que los actores de amenazas están clonando y escaneando los repositorios de manera programática para detectar las claves expuestas.

Además, se ha observado que el adversario bloquea cuentas de AWS que hacen públicas credenciales IAM, lo que probablemente es un intento de evitar un análisis más detallado.

Existen indicios que sugieren que el atacante podría estar relacionado con otra campaña de cripto-minería que fue revelada por Intezer en enero de 2021 y que se centraba en servicios Docker insuficientemente protegidos y utilizaba el mismo software de cripto-minería personalizado.

Una parte del éxito de esta campaña radica en la explotación de debilidades en la función de detección de secretos de GitHub y en la política de cuarentena de claves comprometidas de AWS, que tiene como objetivo señalar y prevenir el uso indebido de credenciales IAM comprometidas o expuestas para iniciar o ejecutar instancias EC2.

A pesar de que la política de cuarentena se activa en un lapso de dos minutos desde que las credenciales de AWS son accesibles públicamente en GitHub, se sospecha que las claves se están exponiendo mediante un método que aún no ha sido determinado.

> Unit 42 reportó que el *«agente de amenazas podría tener la capacidad de descubrir claves de AWS expuestas que no son detectadas de forma automática por AWS y, posteriormente, tomar control de estas claves fuera de la política de Cuarentena de Claves Comprometidas de AWS».*

Dentro de las secuencias de ataque identificadas por la compañía de ciberseguridad, las credenciales de AWS robadas se utilizan para llevar a cabo una operación de reconocimiento de cuentas, seguida de la creación de grupos de seguridad de AWS y el lanzamiento de múltiples instancias de EC2 en varias regiones desde detrás de una red privada virtual (VPN).

Las operaciones de criptomining se ejecutan en instancias de AWS c5a.24xlarge debido a su mayor capacidad de procesamiento, lo que permite a los operadores minar más criptomonedas en un período de tiempo más breve.

El software de minería utilizado para llevar a cabo el criptojacking se obtiene a través de una URL de Google Drive, destacando un patrón en el que actores maliciosos aprovechan la confianza asociada con aplicaciones ampliamente utilizadas para pasar desapercibidos.

> *«El tipo de Imágenes de Máquina de Amazon (AMI) utilizado por el agente de amenazas también presentaba características distintivas. Las imágenes identificadas eran de carácter privado y no estaban listadas en el AWS Marketplace»,* señalaron los investigadores.

Para reducir el riesgo de tales ataques, se recomienda que las organizaciones que accidentalmente expongan las credenciales de AWS IAM revocan de inmediato cualquier

conexión API que utilice dichas claves, las eliminen del repositorio de GitHub y realicen auditorías de eventos de clonación de repositorios de GitHub en busca de actividades sospechosas.

> *«El agente de amenazas puede detectar y llevar a cabo una operación completa de minería en tan solo cinco minutos desde que se exponen las credenciales de AWS IAM en un repositorio público de GitHub. A pesar de las exitosas políticas de cuarentena de AWS, la campaña mantiene una constante variación en el número y la frecuencia de cuentas de víctimas comprometidas»,* indicaron los investigadores.