Una nueva operación de criptominería en la nube con enfoque en servicios poco comunes de Amazon Web Services (AWS), como AWS Amplify, AWS Fargate y Amazon SageMaker, ha surgido con la intención de extraer criptomonedas de manera no autorizada.

La actividad cibernética maliciosa ha sido identificada con el nombre en código AMBERSQUID por la firma de seguridad en la nube y contenedores Sysdig.

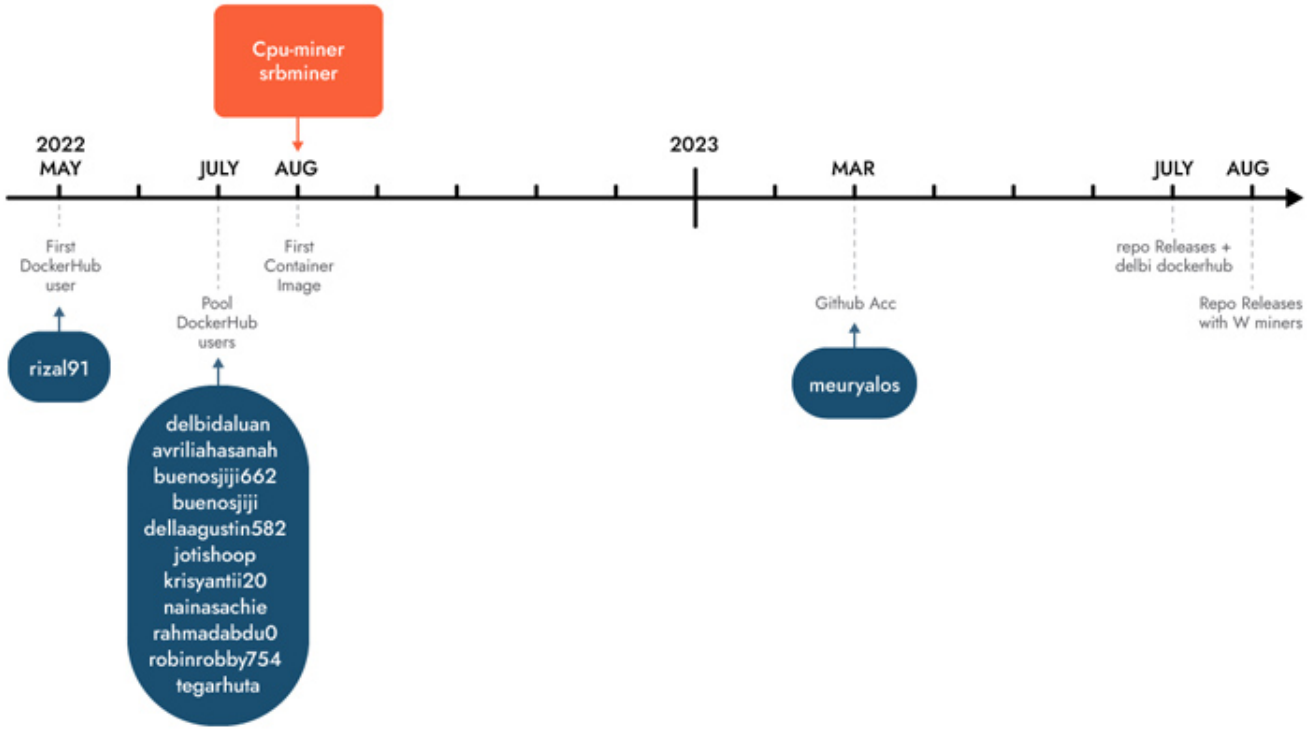
> *«La operación AMBERSQUID logró explotar servicios en la nube sin activar el requerimiento de AWS para la aprobación de más recursos, como sucedería si solo se hiciera un uso intensivo de instancias de EC2»,* afirmó Alessandro Brucato, investigador de seguridad de Sysdig.

> *«Apuntar a múltiples servicios también plantea desafíos adicionales, como la respuesta a incidentes, ya que implica la necesidad de localizar y desactivar todos los mineros en cada servicio explotado».*

Sysdig detectó esta campaña luego de analizar 1.7 millones de imágenes en Docker Hub, y la atribuyó con un nivel de confianza moderado a atacantes indonesios, basándose en el uso del idioma indonesio en los scripts y nombres de usuario.

Algunas de estas imágenes están configuradas para ejecutar mineros de criptomonedas descargados desde repositorios controlados por los actores en GitHub, mientras que otras ejecutan scripts de shell dirigidos hacia AWS.

Un rasgo distintivo es el mal uso de AWS CodeCommit, utilizado para alojar repositorios Git privados, para *«crear un repositorio privado que luego es utilizado en diversos servicios como fuente».*



Dentro del repositorio se encuentra el código fuente de una aplicación de AWS Amplify que, a su vez, es aprovechada por un script de shell para crear una aplicación web de Amplify y, finalmente, poner en marcha el minero de criptomonedas.

Los ciberdelincuentes también han sido observados utilizando scripts de shell para realizar actividades de criptominería en instancias de AWS Fargate y SageMaker, lo que resulta en costos significativos de computación para las víctimas.

Sysdig estimó que si AMBERSQUID se escalara para atacar todas las regiones de AWS, podría generar pérdidas de más de $10,000 al día. Un análisis adicional de las direcciones de billetera utilizadas revela que los atacantes han obtenido ingresos por más de $18,300 hasta la fecha.

No es la primera vez que se vincula a actores de amenazas indonesios con campañas de

criptominería. En mayo de 2023, Permiso P0 Labs detalló a un actor llamado GUI-vil, que se observó aprovechando las instancias de Amazon Web Services (AWS) Elastic Compute Cloud (EC2) para llevar a cabo operaciones de minería de criptomonedas.

> *«Aunque la mayoría de los atacantes motivados financieramente se enfocan en los servicios de cómputo, como EC2, es importante recordar que muchos otros servicios también ofrecen acceso a recursos de cómputo (aunque de manera más indirecta)»*, señaló Brucato.

> *«Estos servicios a menudo pasan desapercibidos desde una perspectiva de seguridad, ya que su visibilidad es menor en comparación con la que se obtiene a través de la detección de amenazas en tiempo de ejecución».*