Los entornos basados en la nube continúan siendo objeto de una campaña de ataque avanzada en curso conocida como SCARLETEEL, y ahora los actores maliciosos están centrándose en Amazon Web Services (AWS) Fargate.

> *«Aunque los entornos en la nube siguen siendo su objetivo principal, han adaptado las herramientas y técnicas utilizadas para evadir las nuevas medidas de seguridad, al tiempo que han desarrollado una arquitectura de comando y control más resistente y sigilosa»,* informó Alessandro Brucato, investigador de seguridad de Sysdig, en un nuevo informe.

SCARLETEEL fue descubierto por primera vez por la empresa de ciberseguridad en febrero de 2023, detallando una sofisticada cadena de ataques que culminó con el robo de datos propietarios de la infraestructura de AWS y el despliegue de mineros de criptomonedas para obtener ganancias ilegales aprovechando los recursos de los sistemas comprometidos.

Un análisis posterior realizado por Cado Security reveló posibles conexiones con un grupo prolífico de criptominería conocido como TeamTNT, aunque Sysdig le dijo a The Hacker News que *«podría tratarse de alguien que copia su metodología y patrones de ataque».*

La actividad más reciente continúa con la predilección del actor malicioso por atacar cuentas de AWS mediante la explotación de aplicaciones web accesibles al público que presentan vulnerabilidades, con el objetivo último de obtener persistencia, robar propiedad intelectual y generar posibles ingresos de hasta $4,000 al día utilizando mineros de criptomonedas.

> *«El actor descubrió y aprovechó un error en una política de AWS que les permitió aumentar sus privilegios a AdministratorAccess y obtener el control de la cuenta, lo que les permitió hacer con ella lo que quisieran»,* explicó Brucato.

Todo comienza cuando el adversario aprovecha los contenedores de cuadernos JupyterLab desplegados en un clúster de Kubernetes, utilizando la posición inicial para llevar a cabo reconocimiento de la red objetivo y obtener credenciales de AWS para acceder más profundamente al entorno de la víctima.

A continuación, se instala la herramienta de línea de comandos de AWS y un marco de explotación llamado Pacu para futuras acciones de explotación. El ataque también se destaca por el uso de diversos scripts de shell para obtener las credenciales de AWS, algunos de los cuales se enfocan en las instancias del motor informático AWS Fargate.

«Se observó que el atacante utiliza el cliente de AWS para conectarse a sistemas rusos compatibles con el protocolo S3», mencionó Brucato, agregando que los actores de SCARLETEEL emplean técnicas sigilosas para asegurarse de que los eventos de extracción de datos no sean registrados en los registros de CloudTrail.

Entre las acciones tomadas por el atacante también se encuentra el uso de una herramienta de pruebas de penetración para Kubernetes conocida como Peirates, así como un malware de botnet DDoS llamado Pandora, lo que indica que el actor intenta monetizar el host.

«Los actores de SCARLETEEL continúan operando contra objetivos en la nube, incluyendo AWS y Kubernetes. Su método preferido para ingresar es explotar servicios informáticos abiertos y aplicaciones vulnerables. Si bien su enfoque principal es obtener ganancias monetarias a través de la minería de criptomonedas, también consideran importante obtener propiedad intelectual», afirmó Brucato.