Una sofisticada campaña de ataque denominada SCARLETEEL tiene como objetivo entornos en contenedores para perpetrar el robo de datos y software pantentados.

> *«El atacante explotó una carga de trabajo en contenedores y después la aprovechó para realizar una escalada de privilegios en una cuenta de AWS para robar credenciales y software propietario»*, dijo Sysdig.

El ataque avanzado en la nube también implicó el despliegue de software de criptominería, que según la compañía de seguridad cibernética es un intento de generar ganancias ilícitas o una estrategia para distraer a los defensores y sacarlos del camino.

El vector de infección inicial apostó por la explotación de un servicio público vulnerable en un clúster de Kubernetes autogestionado alojado en Amazon Web Services (AWS).

Al obtener un punto de apoyo exitoso, se lanzó un criptominero XMRig y se usó un script bash para obtener credenciales que podrían usarse para profundizar en la infraestructura de la nube de AWS y filtrar datos confidenciales.

> *«O la criptominería era el objetivo inicial del atacante y el objetivo cambió una vez que accedieron al entorno de la víctima, o la criptominería se usó como señuelo para evadir la detección de exfiltración de datos»,* dijo la compañía.

Particularmente, la intrusión también deshabilitó los registros de CloudTrail para minimizar la huella digital, evitando que Sysdig acceda a evidencia adicional. En total, permitió al atacante acceder a más de 1 TB de datos, incluyendo scripts de clientes, herramientas de solución de problemas y archivos de registro.

> *«También intentaron pivotar usando un archivo de estado de Terraform a otras*

> *cuentas de AWS conectadas para extender su alcance en toda la organización»,* dijo la compañía.

Los hallazgos se producen semanas después de que Sysdig también detallara otra campaña de cryptojacking montada por 8220 Gang entre noviembre de 2022 y enero de 2023 dirigida al servidor web Apache explotable y las aplicaciones Oracle Weblogic.