Un grupo de hackers que ha atacado distintos entornos de nube de Docker y Kubernetes, ha evolucionado para reutilizar las herramientas de monitoreo de nube genuinas como una backdoor para llevar a cabo ataques maliciosos.

> *«Hasta donde sabemos, esta es la primera vez que se detecta a atacantes utilizando software legítimo de terceros para atacar la infraestructura de la nube»,* dijo la compañía israelí de seguridad, Intezer.

Mediante el software llamado Weave Scope, que se utiliza como una herramienta de visualización y monitoreo para los servicios de Docker y Kubernetes, el grupo de piratas informáticos TeamTNT, no solo mapeó el entorno de nube de sus víctimas, sino que también ejecutó comandos del sistema sin tener que implementar código malicioso en el servidor de destino explícitamente.

TeamTNT ha estado activo al menos desde finales de abril de 2020, dirigiendo sus ataques a puertos Docker mal configurados para instalar un malware de minería de criptomonedas y un bot de denegación de servicio distribuido (DDoS).

El mes pasado, los hackers actualizaron su forma de operar para filtrar los inicios de sesión de Amazon Web Services (AWS) escaneando los sistemas infectados de Docker y Kubernetes en busca de información confidencial de credenciales almacenada en los archivos de configuración de AWS.

Una vez que los atacantes encontraron su objetivo, configuraron un nuevo contenedor privilegiado con una imagen limpia de Ubuntu, usándolo para descargar y ejecutar criptomineros, obtener acceso de root al servidor creando un usuario privilegiado local llamado *«hilde»* para conectarse al servidor a través de SSH, y finalmente, instalar Weave Scope.

> *«Al instalar una herramienta legítima como Weave Scope, los atacantes obtienen*

> *todos los beneficios como si hubieran instalado una puerta trasera en el servidor, con mucho menos esfuerzo y sin necesidad de usar malware»,* dijo Nicole Fishbein, de Intezer.

Es recomendable que los puntos finales de la API de Docker tengan acceso restringido para evitar que los adversarios tomen el control de los servidores.

> *«Weave Scope usa el puerto predeterminado 4040 para hacer que el tablero sea accesible y cualquier persona con acceso a la red puede ver el tablero. Similar al puerto de la API de Docker, este puerto debe estar cerrado o restringido por el firewall»*, dijo la compañía de seguridad.