Los expertos en ciberseguridad han alertado sobre una campaña de criptominería activa que apunta a clusters de Kubernetes mal configurados para minar la criptomoneda Dero.

La empresa de seguridad en la nube Wiz, que sacó a la luz esta actividad, mencionó que se trata de una variante actualizada de una operación con fines económicos que fue documentada por primera vez por CrowdStrike en marzo de 2023.

> *«En este caso, el actor malicioso aprovechó el acceso anónimo a un cluster expuesto a Internet para lanzar imágenes de contenedores maliciosas alojadas en Docker Hub, algunas de las cuales tienen más de 10,000 descargas. Estas imágenes de Docker contienen un minero de Dero empaquetado con UPX llamado 'pause'»*, explicaron los investigadores de Wiz, Avigayil Mechtinger, Shay Berkovich y Gili Tikochinski.

El acceso inicial se consigue atacando servidores API de Kubernetes accesibles externamente con autenticación anónima habilitada para desplegar las cargas útiles del minero.

A diferencia de la versión de 2023 que desplegaba un DaemonSet de Kubernetes llamado «proxy-api,» la última variante utiliza DaemonSets aparentemente inofensivos denominados «k8s-device-plugin» y «pytorch-container» para finalmente ejecutar el minero en todos los nodos del cluster.

Además, la idea de nombrar al contenedor «pause» es tratar de hacerse pasar por el contenedor real «pause» que se utiliza para iniciar un pod y aplicar el aislamiento de red.

El minero de criptomonedas es un binario de código abierto escrito en Go que ha sido modificado para codificar la dirección de la billetera y las URL del pool de minería de Dero personalizadas. También está ofuscado utilizando el empaquetador de código abierto UPX para dificultar el análisis.

La idea principal es que, al integrar la configuración de minería dentro del código, es posible

ejecutar el minero sin argumentos de línea de comandos que normalmente son monitoreados por los mecanismos de seguridad.

Wiz mencionó que identificó herramientas adicionales desarrolladas por el actor malicioso, incluyendo una muestra de Windows de un minero de Dero empaquetado con UPX, así como un script shell de instalación diseñado para terminar procesos de mineros competidores en un host infectado e instalar GMiner desde GitHub.

> *«[El atacante] registró dominios con nombres inofensivos para evitar levantar sospechas y mezclarse mejor con el tráfico web legítimo, mientras enmascara la comunicación con pools de minería bien conocidos,»* dijeron los investigadores.
>
> *«Estas tácticas combinadas demuestran los continuos esfuerzos del atacante para adaptar sus métodos y mantenerse un paso adelante de los defensores.»*