Investigadores de seguridad cibernética descubrieron la primera campaña ilícita de minería de criptomonedas usada para minar Dero desde principios de febrero de 2023.

> *«La nueva operación de cryptojacking de Dero se concentra en ubicar clústeres de Kubernetes con acceso anónimo habilitado en una API de Kubernetes y escuchar en puertos no estándar accesibles desde Internet»,* dijo Crowdstrike.

El desarrollo marca un cambio notable de Monero, que es una criptomoneda predominante usada en este tipo de campañas. Se sospecha que puede tener que ver con el hecho de que Dero *«ofrece mayores recompensas y proporciona las mismas o mejores características de anonimato».*

Los ataques, atribuidos a un hacker desconocido con motivaciones financieras, comienzan con la búsqueda de clústeres de Kubernetes con la autenticación configurada como –anonymous-auth=true, lo que permite que las solicitudes anónimas al servidor eliminen las cargas útiles iniciales de tres direcciones IP distintas con sede en Estados Unidos.

Esto incluye la implementación de un DaemonSet de Kubernetes llamado «*proxy-api*» que, a su vez, se utiliza para colocar un pod malicioso en cada nodo del clúster de Kubernetes para iniciar la actividad de minería.

Con ese fin, el archivo YAML de DaemonSet está orquestado para ejecutar una imagen de Docker que contiene un binario de «pausa», que en realidad es el minero de Dero.

> *«En una implementación legítima de Kubernetes, utiliza contenedores de 'pausa' para iniciar un pod. Los atacantes pueden haber usado este nombre para mezclarse y evitar una detección obvia»,* dijo la compañía.

La compañía de seguridad cibernética dijo que identificó una campaña paralela de minería de

Monero, que también apuntaba a los clústeres de Kubernetes expuestos al intentar eliminar el DaemonSet «*proxy-api*» existente asociado con la campaña Dero.

Esta es una indicación de la lucha en curso entre los grupos de cryptojacking que compiten por los recursos de la nube para tomar y retener el control de las máquinas y consumir todos sus recursos.

> *«Ambas campañas están tratando de encontrar superficies de ataque de Kubernetes no descubiertas y están luchando»,* dijeron los investigadores de CrowdStrike, Benjamin Grap y Manoj Ahuje.