Una campaña de ataque a gran escala descubierta en la naturaleza ha estado explotando el control de acceso basado en roles (RBAC) de Kubernetes (K8), con el fin de crear puertas traseras y ejecutar mineros de criptomonedas.

> *«Los atacantes también desplegaron DaemonSets para hacerse cargo y secuestrar los recursos de los clústeres K8 que atacan»,* dijo la compañía de seguridad en la nube Aqua.

La compañía israelí que denominó el ataque RBAC Buster, dijo que encontró 60 grupos de K8 expuestos que han sido explotados por el atacante detrás de la campaña.

La cadena de ataque comenzó cuando el atacante obtuvo acceso inicial a través de un servidor API mal configurado, seguido de la verificación de evidencia de malware minero de la competencia en el servidor comprometido y después usando RBAC para configurar la persistencia.

> *«El atacante creó un nuevo ClusterRole con privilegios cercanos al nivel de administrador. A continuación, el atacante creó un 'ServiceAccount', 'kube-controller' en el espacio de nombres 'kuber-system'. Finalmente, el atacante creó un 'ClusterRoleBinding', vinculando ClusterRole con Service-Account para crear una persistencia sólida y discreta»,* dijo la compañía.

En la intrusión observada contra sus honeypots K8, el atacante intentó armar las claves de acceso de AWS expuestas para obtener un punto de apoyo en el entorno, robar datos y escapar de los confines del clúster.

El paso final del ataque implicó que el hacker creara un DaemonSet para implementar una imagen de contenedor alojada en Docker (*«kuberntesio/kube-controller:1.0.1»*) en todos los nodos. El contenedor, que ha sido extraído 14,399 veces desde que se cargó hace cinco

meses, alberga un minero de criptomonedas.

> *«La imagen del contenedor llamada 'kuberntesio/kube-controller' es un caso de error tipográfico que se hace pasar por la cuenta legítima de 'kubernetesio'. La imagen también imita la popular imagen del contenedor 'kube-controller-manager', que es un componente crítico del plano de control, que se ejecuta dentro de un Pod en cada nodo maestro, responsable de detectar y responder a las fallas de los nodos»*, dijo Aqua.

Algunas de las tácticas descritas en la campaña tienen similitudes con otra operación ilícita de minería de criptomonedas que también aprovechó DaemonSets para acuñar Dero y Monero. Actualmente no está claro si los dos conjuntos de ataques están relacionados.