I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Backdoor
Nivel de riesgo: Alto

II. ALERTA

En abril de 2023, investigadores del equipo de seguridad de Aqua Nautilus, dieron a conocer que obtuvieron evidencias de ataques que han explotado el control de acceso basado en roles (RBAC) de Kubernetes (K8) para crear puertas traseras. Los atacantes también implementaron DaemonSets para secuestrar los recursos de los clústeres de K8 que atacan.

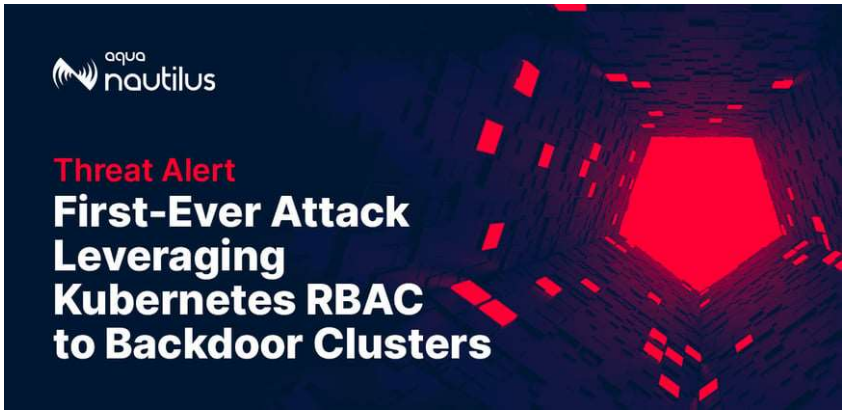


Figura Nro. 1.- Ilustración asociada a Kubernetes RBAC
Fuente: https://blog.aquasec.com/

III. INTRODUCCIÓN

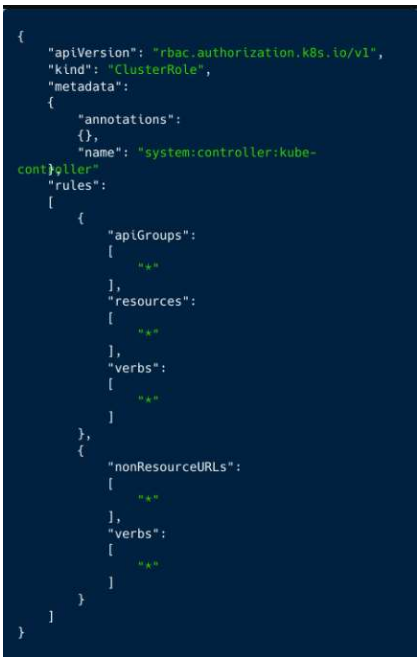
La empresa Aqua Nautilus, registró y analizó un ataque a una de sus *honeypots* K8, que utilizó el sistema RBAC para ganar persistencia, el atacante implementó contenedores utilizando *DaemonSets* para ejecutar el "*cryptominer Monero*".

Monero es una criptomoneda, que debido a su naturaleza anónima, se ha convertido en la moneda preferida para los delincuentes cibernéticos en todo el mundo. La minería de Monero, también conocida como XMR, se ha convertido en una actividad lucrativa para los delincuentes cibernéticos que buscan obtener ganancias de forma ilegal.

La investigación realizada Aqua Nautilus, indica el atacante obtuvo el acceso inicial a través de un servidor API mal configurado que permitía solicitudes no autenticadas de usuarios anónimos con privilegios. El atacante envió algunas solicitudes HTTP para enumerar *secretos* y luego realizó dos solicitudes API para obtener información sobre el clúster, al enumerar las entidades en el espacio de nombres *'kube-system'*, a continuación, el atacante verificó si con el ataque se implementó en el clúster la implementación denominada *'kube-controller'*.

El atacante también intentó eliminar algunas implementaciones existentes en varios espacios de nombres, incluidos*'kube-secure-fhgxtsjh', 'kube-secure-fhgxt', 'api-proxy'* y *'worker-deployment'.*

La parte interesante de este ataque fue cuando el atacante usó RBAC para ganar persistencia. El atacante creó un nuevo *ClusterRole* con privilegios semejantes al de administrador, debido a que era un rol de clúster, no estaba vinculado a un espacio de nombres específico. A continuación, el atacante creó un *'ServiceAccount* ', *'kube-controller* ' en el espacio de nombres *'kube-system'*. Por último, el atacante creó un *'ClusterRoleBinding'*, vinculando el *ClusterRole* con *ServiceAccount* para crear persistencia oculta.



```
{
    "apiVersion": "rbac.authorization.k8s.io/v1",
    "kind": "ClusterRole",
    "metadata":
    {
        "annotations":
        {},
        "name": "system:controller:kube-
controller"
    },
    "rules":
    [
        {
            "apiGroups":
            [
                "*"
            ],
            "resources":
            [
                "*"
            ],
            "verbs":
            [
                "*"
            ]
        },
        {
            "nonResourceURLs":
            [
                "*"
            ],
            "verbs":
            [
                "*"
            ]
        }
    ]
}
```

Figura Nro. 2: ClusterRole creado por el atacante con privilegios de administrador
Fuente: https://blog.aquasec.com/

Una vez que el atacante logró lo anterior, incluso si el acceso de usuario anónimo está deshabilitado, el atacante creó una persistencia que permite una mayor explotación del clúster. Además, si bien vincular el rol de '*cluster-admin*' a un usuario nuevo o sospechoso puede activar alarmas, el atacante crea una forma de combinarse con los registros de auditoría de la API, eventualmente, al configurar el *'system:controller:kube-controller'* del *ClusterRoleBinding*, el atacante podría permanecer oculto sin activar ninguna alarma.

Como parte del escenario de la *honeypots* de la empresa Aqua Nautilus, se expusieron las claves de acceso de AWS en varias ubicaciones del clúster, el atacante utilizó las claves de acceso para intentar obtener más acceso a la cuenta del proveedor de servicios en la nube del objetivo y aprovechar el ataque para robar más recursos, datos y salir del alcance específico de los *clusters k8*.

Luego, el atacante creó un *DaemonSet* para desplegar contenedores en todos los nodos con una sola solicitud de API. El objeto de solicitud de creación de *DaemonSet* contenía la imagen del contenedor *'kuberntesio/kube-controller:1.0.1'*, alojada en el registro público *Docker Hub*, el impacto en el clúster fue el secuestro de recursos.

```
{
    "name": "kube-controller",
    "namespace": "kube-system",
    "labels":
    {
        "app": "kube-controller"
    },
    "annotations":
    {
        "kubectl.kubernetes.io/last-applied-configuration":
        {
            "apiVersion": "apps/v1",
            "kind": "DaemonSet",
            "spec":
            {
                "containers":
                [
                    {
                        "image": "kuberntesio/kube-
controller:1.0.1",       "imagePullPolicy": "IfNotPresent",
                        "name": "kube-controller"
                    }
                ]
            }
        }
    }
}
```

Figura Nro. 3: Implementación de un *DaemonSet* con la imagen del contenedor *kuberntesio/kube-controller*
Fuente: https://blog.aquasec.com/

Al inspeccionar la imagen del contenedor *'kuberntesio/kube-controller:1.0.1'* en *Docker Hub*, los investigadores de Aqua Nautilus encontraron que el contenedor se extrajo

14.399 veces desde que se cargó hace cinco meses, lo que indica que esta campaña está muy extendida, también encontraron otros 60 clústeres K8 expuestos que tenían evidencia de ataques activos por parte de este atacante.

El contenedor *'kuberntesio/kube-controller'* tiene 3 etiquetas. Dentro de cada una de las imágenes del contenedor se encuentran el controlador binario *kube* (*MD5*= *2833c82055bf2d29c65cd9cf6684449a*), que fue detectado en VirusTotal como *cryptominer*. En cada una de las imágenes del contenedor el archivo de configuración, la dirección de la billetera indicaba que el atacante ya había extraído 5 XMR y, a este ritmo de extracción, podría obtener otros 5 por año ($ 200 USD) de un solo *trabajador*.

La imagen del contenedor denominada *'kuberntesio/kube-controller'* es un caso de error tipográfico que suplanta la cuenta legítima de *'kubernetesio'*, y ha acumulado millones de extracciones, a pesar de tener solo unas pocas docenas de imágenes de contenedores. La imagen también imita a *'kube-controller-manager'*, que es un componente crítico del plano de control, que se ejecuta dentro de un *Pod* en cada nodo maestro, que es responsable de detectar y responder a las fallas del nodo. Esencialmente, es un componente K8 ampliamente utilizado que debe existir en el clúster y se podría pensar que es una implementación legítima, y no sospechar que se trata de un *cryptominer*.

IV. VECTOR DE ATAQUE:

Sistema mal configurado

V. IMPACTO:

Monero cryptominers son programas maliciosos que utilizan la capacidad de procesamiento de las computadoras comprometidas para extraer la criptomoneda Monero, sin el consentimiento del propietario de la computadora. El impacto de estos programas puede ser:

1. Rendimiento de la computadora: La ejecución de un programa de minería de Monero puede ralentizar significativamente el rendimiento de la computadora, lo que puede hacer que las tareas cotidianas, como navegar por la web o utilizar aplicaciones, sean más lentas y frustrantes.
2. Consumo de energía: El programa de minería también consume una gran cantidad de energía eléctrica, lo que puede aumentar la factura de electricidad del propietario de la computadora y contribuir al calentamiento global.

3. Malware y vulnerabilidades: La instalación de un programa de minería de Monero en una computadora puede abrir la puerta a otros programas maliciosos y vulnerabilidades de seguridad, lo que puede poner en riesgo los datos personales y financieros del propietario de la computadora.
4. En el ámbito empresarial, los cryptominers de Monero pueden tener consecuencias graves. Si se infectan los servidores de una organización, puede haber una pérdida de datos, una disminución en la capacidad de procesamiento y la posibilidad de que la organización sea utilizada como plataforma para ataques de amplificación de DDoS.

VI. INDICADORES DE COMPROMISO

No se detallan

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Revisar y analizar las configuraciones de los *clusters* K8, es importante protegerlos, para evitar dejarlos vulnerables.
- Mantener actualizado el software del sistema operativo y las aplicaciones, incluyendo los navegadores web.
- Instalar un software antivirus y mantenerlo actualizado.
- Evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables.
- Deshabilitar la ejecución de scripts en los navegadores web o usar un bloqueador de scripts.
- Deshabilitar los complementos y extensiones de los navegadores que no se utilizan regularmente.
- Usar contraseñas seguras y diferentes para cada cuenta.
- Deshabilitar el inicio automático de aplicaciones en el arranque del sistema.
- Usar herramientas de detección y eliminación de malware para buscar y eliminar Monero cryptominers.
- Configurar el firewall del sistema para bloquear el tráfico malicioso.
- Realizar copias de seguridad de forma regular.

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima de Monero cryptominers y proteger los dispositivos y datos personales, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo de infección por *cryptominers* de *Monero*.

Para ayudar a mitigar tales ataques, los investigadores de Aqua Nautilus que descubrieron esta vulnerabilidad, recomiendan que se puede usar "Aqua Trivy" (https://blog.aquasec.com/kubernetes-cluster-security-with-trivy) para asegurar los *clusters* K8.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Goodin, D. (2018). The Monero-mining malware epidemic is coming. Ars Technica. Recuperado de https://arstechnica.com/information-technology/2018/02/the-monero-mining-malware-epidemic-is-coming/

Katchinskiy, M. (2023, 21 abril). First-Ever Attack Leveraging Kubernetes RBAC to Backdoor Clusters. https://blog.aquasec.com/. https://blog.aquasec.com/leveraging-kubernetes-rbac-to-backdoor-clusters

Robinson, D. (2018). The Risks and Benefits of Cryptocurrency Mining. Digital Guardian. Recuperado de https://digitalguardian.com/blog/risks-and-benefits-cryptocurrency-mining

Sharma, S. (2018). Understanding Monero Mining Malware and Its Impact. Security Boulevard. Recuperado de https://securityboulevard.com/2018/06/understanding-monero-mining-malware-and-its-impact/