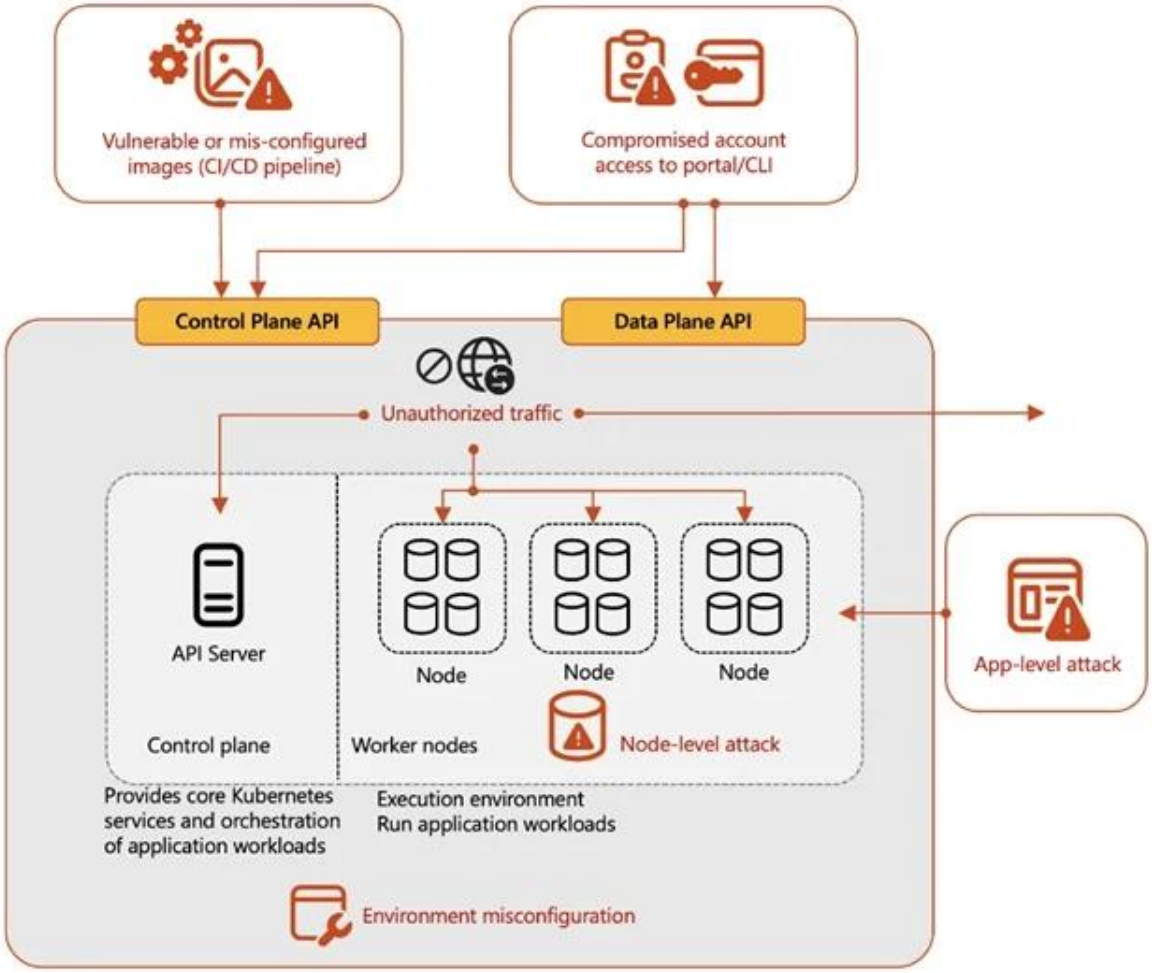
Microsoft ha informado que un actor de amenazas, identificado como Storm-1977, ha llevado a cabo ataques de password spraying contra inquilinos en la nube del sector educativo durante el último año.

«El ataque emplea una herramienta llamada AzureChecker.exe, una interfaz de línea de comandos (CLI) que ha sido utilizada por diversos grupos de amenazas,» explicó el equipo de Inteligencia de Amenazas de Microsoft en su análisis.

La compañía tecnológica indicó que observó que este archivo ejecutable se conecta a un servidor externo llamado «sac-auth.nodefunction[.]vip» para descargar datos cifrados con AES que contienen una lista de los objetivos del ataque de password spraying.

Además, la herramienta acepta como entrada un archivo de texto llamado «accounts.txt«, que incluye combinaciones de nombres de usuario y contraseñas que serán utilizadas durante el ataque.



«El actor de amenazas combinó la información de ambos archivos y luego intentó validar las credenciales contra los inquilinos objetivo,» añadió Microsoft.

En uno de los incidentes exitosos documentados por Microsoft, el atacante aprovechó una cuenta de invitado comprometida para crear un grupo de recursos dentro de la suscripción afectada.

Posteriormente, los atacantes crearon más de 200 contenedores dentro de ese grupo de recursos, con el objetivo de realizar minería de criptomonedas de manera ilegal.

Microsoft advirtió que los recursos basados en contenedores, como los clústeres de Kubernetes, registros de contenedores y imágenes, son vulnerables a varios tipos de ataques, entre ellos:

- Uso de credenciales en la nube comprometidas para tomar control del clúster.
- Aprovechamiento de imágenes de contenedores con vulnerabilidades o configuraciones incorrectas para realizar acciones maliciosas.
- Explotación de interfaces de gestión mal configuradas para acceder a la API de Kubernetes y desplegar contenedores maliciosos o incluso tomar el control total del clúster.
- Ataques a nodos que ejecutan software o código vulnerable.

Para reducir el riesgo de estos ataques, Microsoft recomienda a las organizaciones:

- Proteger la implementación y la ejecución de contenedores.
- Supervisar solicitudes inusuales a la API de Kubernetes.
- Configurar políticas que impidan desplegar contenedores desde registros no confiables.
- Asegurarse de que las imágenes utilizadas en los contenedores estén libres de vulnerabilidades.