Fresh Crypto Attacks Targeting Kubernetes Clusters

Microsoft has warned about an ongoing series of attacks targeting Kubernetes clusters running Kubeflow ML instances. These attacks are deploying malicious containers mining Monero and Ethereum. According to Microsoft, these attacks started at the end of May.

What's the threat?

At the end of May, security researchers observed a sudden increase in TensorFlow ML pod deployments. Attackers were proactively scanning clusters and had a list of potential targets.

The pods were genuine, however, the attackers tampered with them to mine cryptocurrency on targeted Kubernetes clusters by deploying ML pipelines, leveraging the Kubeflow Pipelines platform.

The attackers used internet-exposed Kubeflow dashboards to gain initial access to the clusters. This was followed by the deployment of cryptocurrency miners.

Subsequently, they deployed two separate pods on each of the targeted clusters: one was used for GPU mining (Ethminer), and the other one used for CPU mining (XMRig).

Similar campaign

The current campaign seems to be very similar to another campaign that was first observed in April 2020. That campaign had also compromised powerful Kubernetes clusters by targeting Kubeflow using some other components.

- In the April 2020 attacks, the attackers had exploited Jupyter notebooks instead of Kubeflow Pipelines.
- The April 2020 campaign was one of the first to specifically target Kubeflow environments.
- After that Microsoft spotted several other campaigns targeting Kubernetes.

Recommendation

The recent attacks show how cybercriminals are increasingly targeting Kubernetes clusters and their surrounding ecosystem. Therefore, admins are recommended to enable authentication on Kubeflow dashboards when exposing them to the internet, disable anonymous access, implement Role-based Access Control (RBAC) and encrypt secrets at rest. Additionally, always monitor the environments using reliable tools and perform frequent audits for all containers and images.

References:

https://cyware.com/news/fresh-crypto-attacks-targeting-kubernetes-clusters-d182d04e

https://chaslescorp.com/fresh-crypto-attacks-targeting-kubernetes-clusters/

https://thehackernews.com/2021/06/crypto-mining-attacks-targeting.html

https://www.computerweekly.com/news/252495806/Crypto-malware-targets-Kubernetes-clusters-say-researchers