Kubeflow : une arme de gros calibre pour les cybercriminels ?

Les clusters Kubeflow, cibles de choix pour le minage de cryptomonnaies ?

L'équipe Azure Security Center le constate dans la théorie, mais aussi dans la pratique.

Sur le volet théorique, la logique est simple. Ces clusters permettent d'exécuter des tâches d'apprentissage automatique. Ils disposent ainsi généralement de grandes capacités de calcul.

Sur le volet pratique, « des dizaines » d'entre eux auraient subi des attaques ces dernières semaines.
Plusieurs images Docker malveillantes* issues d'un dépôt GitHub public y ont été installées. Elles contenaient le cryptomineur XMrig, sous différentes configurations.

Parmi les services qui composent Kubeflow figure un tableau de bord, exécuté dans son propre conteneur.
La connexion à cet outil repose sur Istio Gateway. Par défaut, elle ne peut se faire depuis l'extérieur sans router le trafic *via* le serveur API Kubernetes.

Il peut être tentant de modifier le paramétrage de sorte à exposer Istio Gateway sur le réseau Internet. Mais cela comporte des risques d'accès indésirables par des tiers qui pourraient notamment :

- Créer un serveur de *notebooks* Jupyter et lui greffer une image Docker malveillante
- Déployer un conteneur malicieux depuis un *notebook* Jupyter (existant ou créé pour l'occasion) et envisager une latéralisation grâce au compte de service associé

Azure Security Center s'était déjà fait l'écho d'une campagne cyber visant des tableaux de bord vulnérables dans l'écosystème Kubernetes. Mais c'est la première fois qu'elle en découvre une visiblement spécifique à Kubeflow.

** Pour contrôler la présence de la principale de ces charges malveillantes, une commande :* kubectl get pods –all-namespaces -o jsonpath="{.items[*].spec.containers[*].image}" | grep -i ddsfdfsaadfs.
Pour vérifier l'état d'Istio Gateway : kubectl get service istio-ingressgateway -n istio-system.

Illustration principale © projet Kubeflow