Les conteneurs Docker, une planque pour les malwares

Dans les différentes annonces faites lors de la conférence à la Black Hat, les exploits concernant les conteneurs Docker sont un peu passés inaperçus. Et pourtant, cette technologie prend de l'ampleur et la sécurité est souvent mise en avant comme un frein pour un développement plus large.

Des chercheurs d'Aqua Security, Michael Cherny et Sagie Dulce, ont démontré que les conteneurs Docker sont une cachette idéale pour des malwares. Le POC fonctionne sur l'ensemble des installations Docker exposant son API via TCP. « *Le but ultime de l'attaque est l'exécution du code à distance au sein du réseau de l'entreprise* », explique Sagie Dulce. En ajoutant, « *la persistance sur la machine hôte est pratiquement indécelable par les solutions de sécurité* ».

L'attaque démontrée par les spécialistes comprend plusieurs étapes. En premier lieu, il faut attirer le développeur utilisant Docker sur Windows vers une page web hébergeant un programme en JavaScript. Ce dernier a la capacité entre autres d'éviter les politiques de sécurité de type Same Origin Policy (SOP) présentes sur les navigateurs. « *Plusieurs commandes n'outrepassent pas le SOP à travers des requêtes GET, HEAD et POST* », précise Sagie Dulce en donnant une liste exhaustive dans le document présenté à la conférence. Les chercheurs ont utilisé l'API Docker sans être bloqués par SOP. Ils ont même réussi à créer un conteneur sur le PC hôte en s'appuyant sur un référentiel Git pour les commandes et contrôles et embarquant le code de l'attaque.

Host rebinding attack et shadow conteneur

Le conteneur ainsi créé est limité et sert principalement à bénéficier des accès privilégiés de l'API. Pour cela, les chercheurs ont élaboré une technique nommée « Host rebinding attack » (attaque par rappel de l'hôte). Elle s'apparente un procédé similaire, « DNS rebinding attack » permettant à un attaquant d'utiliser des DNS pour tromper le SOP d'un navigateur. Dans le cadre du rappel d'hôte, l'attaque a permis de berner les protocoles de résolution de nommage, NetBIOS et LLMNR. Le résultat est la réalisation d'un conteneur sur une VM tournant sur Hyper-V, partageant le réseau local de son hôte et pouvant exécuter du code à distance. Sur l'aspect persistance, les chercheurs ont créé un « shadow conteneur » pour que les fonctionnalités de contournement intégrées dans le conteneur restent après le démarrage de la VM.

Docker a été informé du problème et a indiqué le problème provenait de l'accès à distance du daemon Docker via http/TCP sur d'anciennes versions de Docker pour Windows. Aujourd'hui, l'éditeur Open Source précise que le port HTTP a été fermé pour éviter ce problème.

A lire aussi :

Microservices, Docker, Kubernetes : des compétences que les entreprises s'arrachent

Docker part à la conquête de la Chine

Crédit Photo : Donvitorio-Shutterstock