Graboid : un ver cryptomineur qui se propage via Docker

Si vous accédez à vos instances Docker Engine par le réseau Internet, assurez-vous d'implémenter un dispositif d'authentification adéquat.

Les équipes de Palo Alto Networks donnent ce conseil eu égard à un *malware* qu'elles ont baptisé Graboid.

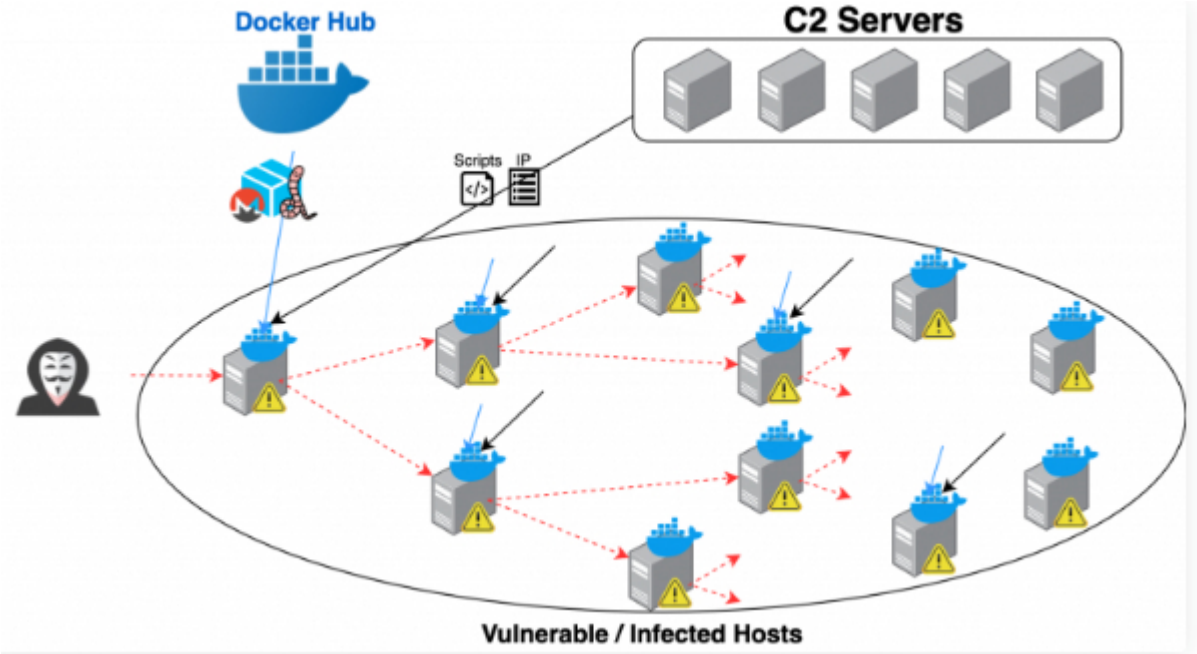
Ce ver mineur de cryptomonnaie a la particularité de se propager par l'intermédiaire de conteneurs.

Des instances non sécurisées du moteur Docker ont servi de point d'entrée. Elles ont permis de télécharger et de déployer un conteneur malveillant (pocosow/centos:7.6.1810).

Minage P2P

Ce conteneur contient un client Docker. Il inclut aussi un script (/var/sbin/hash) qui se connecte à un serveur distant pour y récupérer quatre autres scripts :

- live.sh
  Transmission au serveur du nombre de processeurs disponibles sur l'hôte infecté.
- worm.sh
  Téléchargement d'une liste d'IP correspondant à des hôtes dont les points de terminaison API sont vulnérables. Une adresse est choisie au hasard pour y déployer le conteneur malveillant, assurant ainsi la réplication du *malware*.
- xmr.sh et cleanxmr.sh
  Le premier sélectionne une IP sur la même liste et y déploie un autre conteneur (gakeaws/nginx) qui lance le minage de cryptomonnaie Monero.
  Le second stoppe l'activité sur un autre hôte là aussi choisi au hasard. Se crée alors une sorte de système P2P de contrôle du minage.



Des cibles en France

Cette séquence se répète périodiquement (dernier intervalle constaté : toutes les 100 secondes) sur chaque machine infectée.

Sur les 2 034 IP que comprend la liste, une vingtaine (0,9 %) sont situées en France. Plus de la moitié (57 %) se trouvent aux États-Unis. Une quinzaine d'entre ces hôtes ont fait office de postes de commande. Un serveur web y a probablement été installé, là aussi par l'intermédiaire d'un conteneur.

Au 16 octobre 2019, pocosow/centos comptait plus de 10 000 téléchargements ; gakeaws/nginx, plus de 6 500.

Difficile de détecter le caractère malveillant du premier de ces deux conteneurs aussi longtemps que les quatre scripts ne sont pas téléchargés.

Pour le second, c'est plus évident. Ne serait-ce que de par l'inscription de l'adresse du porte-monnaie électronique « en dur », dans une variable d'environnement.

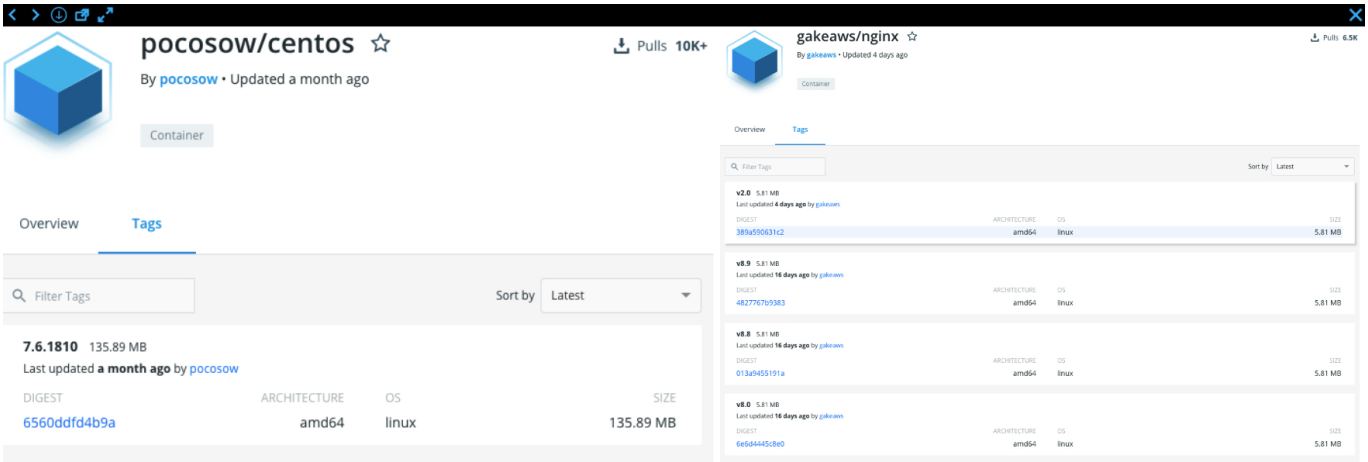


Photo d'illustration © Eugène Sergueev – Shutterstock.com