LibMiner : le malware qui infectait les conteneurs Redis

Vous souvenez-vous de Graboid ?

Palo Alto Networks avait signalé, en octobre dernier, l'existence de ce ver cryptomineur se propageant par l'intermédiaire de conteneurs.

Qualys vient d'attirer l'attention sur un *malware* de la même espèce : LibMiner.

Comme Graboid, il est destiné à miner du Monero.
Son fonctionnement n'est toutefois pas le même : il s'appuie sur des serveurs Redis mal sécurisés.

Qualys affirme ne pas avoir pu déterminer le mécanisme d'infection initial. Il a cependant identifié plusieurs conteneurs dont le point d'entrée a été paramétré pour exécuter un script.

Ce script planifie l'exécution différée de commandes à travers une tâche Cron. Il réinitialise par ailleurs le contenu du fichier etc/hosts afin de permettre l'accès au serveur qui héberge les autres composantes du *malware*.

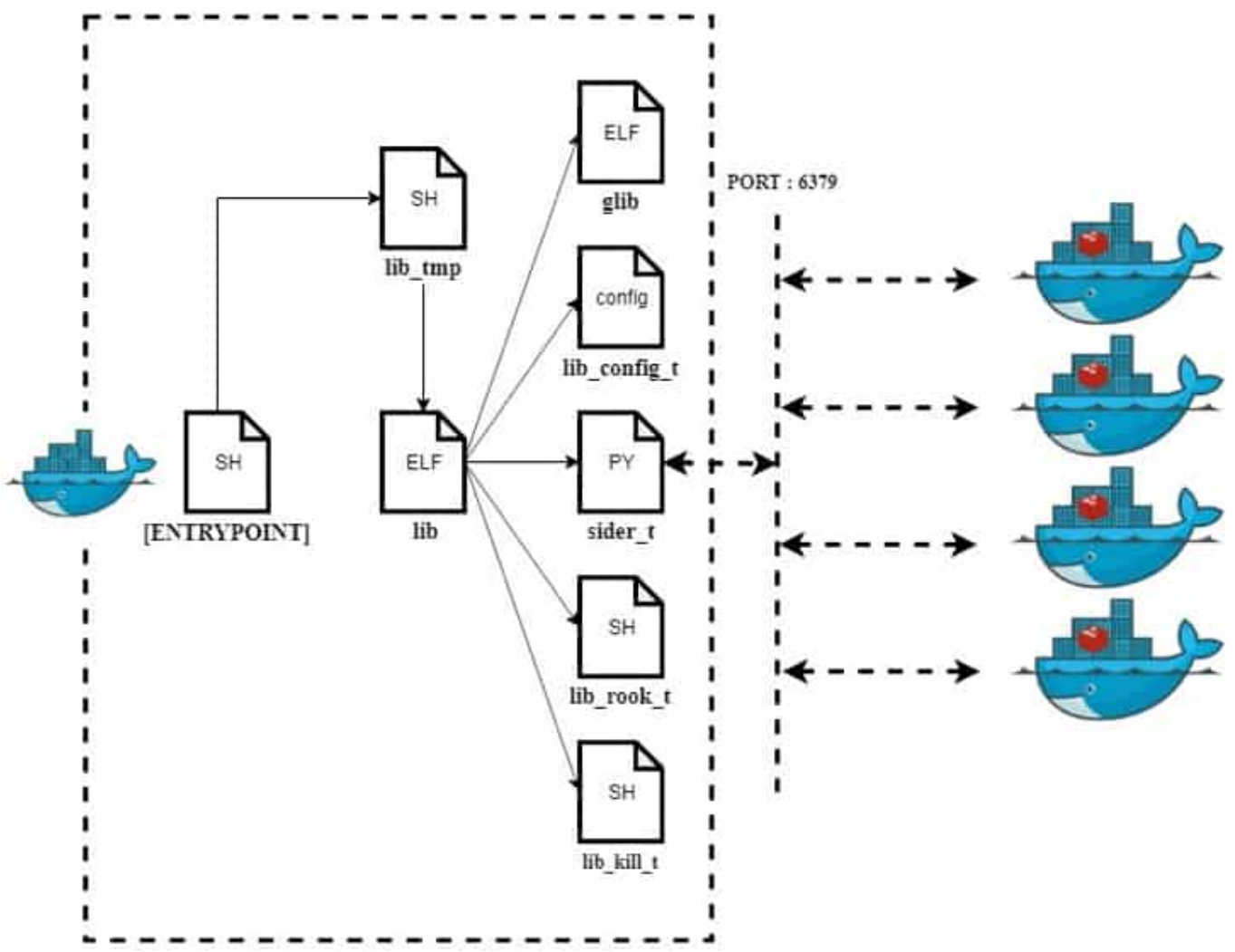
Parmi ces composantes se trouve un autre script : lib_tmp. Il vérifie la présence de certains outils de sécurité et tue les processus associés. Puis met à jour le serveur de nom pour utiliser les DNS publics de Google. Son dernier rôle est de télécharger un fichier ELF (binaire Unix) et de l'enregistrer dans /var/lib sous un nom aléatoire de 4 caractères.

Sus au port 6379

Ce binaire n'est autre que le cœur de LibMiner. Les routines qu'il contient s'exécutent en boucle infinie et téléchargent plusieurs fichiers :

- lib_rook_t et lib_kill_t
  Ces scripts effacent toute trace d'exécution antérieure du *malware*, y compris en fermant les connexions réseau pour une liste d'IP et de ports prédéfinis.
- lib_boot_t
  Ce script récupère la dernière version de LibMiner, la sauvegarde sous un nom aléatoire dans /tmp et l'exécute. Il copie aussi le fichier dans /etc/init.d/symcfget pour assurer une persistance.
- lib_config_t et glib
  Glib permet le minage de Monero. lib_config_t contient ses paramètres, dont l'adresse du portefeuille.
- sider_t
  Ce script sert à infecter les conteneurs exécutant un serveur Redis mal protégé (au niveau du port 6379, utilisé par défaut). Il récupère l'IP des conteneurs et utilise la force brute sur les deux derniers segments de cette IP pour tenter d'étendre l'infection aux systèmes Linux qui exposent leur port 6379.

Une fois la connexion établie, plusieurs fichiers sont placés dans le conteneur et la boucle d'infection recommence.



Plusieurs techniques permettent de rendre LibMiner plus discret et plus résistant :

- la création de processus fils dotés d'un nouveau nom et d'un nouvel identifiant
- un *timeout* très faible pour la console root
- l'invisibilité des commandes entrées dans la commande

Photo d'illustration © Eugène Sergueev – Shutterstock.com