Docker Hub is used by hackers to spread Cryptojacking malware

Malicious software is installed by the hacker into Docker Images and spreads through the Docker Hub itself.

Docker is becoming increasingly popular with developers as packaging services and deploying software applications. Therefore, black-hat hackers focused their attacks on exposed Dock end APIs to create infected Docker Images. From there, hackers can deploy DDoS attacks and run unauthorized cryptocurrency mining applications on the victim's system.

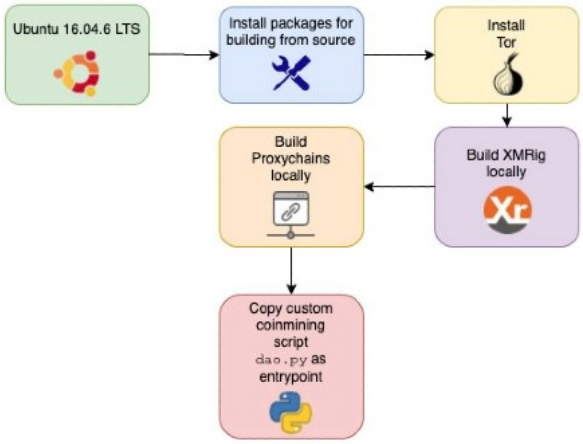
As reported by Palo Alto Networks Unit 42, a cyber security threat researcher, hackers make a profit by deploying cryptocurrency mining software using Docker Containers. Moreover, they take advantage of the Docker Hub repository itself to spread malicious Docker Images.

Docker Hub is used by hackers to spread malware

Unit 42 reports: *"The Docker Container is a convenient method, which makes it easier for programmers to package the software, so more and more programmers use it. Therefore, hackers easily distribute exploit software. mining cryptocurrency to machines with Docker software. Immediately, the victim's system will be used to illegally mine cryptocurrency* .

Docker is a well-known solution platform (PaaS) for Linux and Windows, allowing developers to deploy, test and package their applications in virtualized environments. This helps applications operate separately from the server system that contains it.

In the "azurenql" account, which has now been removed from the Docker Hub, researchers discovered 8 Docker Images containing malicious code capable of mining Moreno cryptocurrency. The author of this malicious code uses a Python script to activate the virtual currency mining malware and use anonymous internet access tools like ProxyChains and Tor to avoid being detected.



The process of attack and illegal mining of virtual money on the victim's system
Since its launch in October 2019, the Docker Images of "azurenql" accounts have been conducting virtual currency mining more than 2 million times. In one of the e-wallets associated with this campaign, researchers found virtual money worth $ 36,000 (838 million).

DDoS attack

Not only that, in a recent scan, Trend Micro researchers discovered that Docker's unprotected servers are being attacked by at least two malicious code, XOR DDoS and Kaiji. These malware will collect the victim's system information and perform DDoS attacks.

The researchers stated: *"Hackers often use botnets to perform brute-force after scanning the Secure Shell (SSH) and Telnet left open. Now, hackers are still looking for the machine Docker host with port 2375 unprotected ".*

Although there are different methods of DDoS attack, both XOR DDoS and Kanji collect data such as domain name, network speed, identification of running processes and information about the system's CPU. These are all necessary information for DDoS campaigns.

Experts recommend that users and businesses using Docker should immediately check if their API endpoints are exposed on the internet. In addition, you need to close all ports on the Docker server as well as enforce the highest level of security measures for the entire system.

You finished reading the article "**Docker Hub is used by hackers to spread Cryptojacking malware**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com