20 Million Miners: Finding Malicious Cryptojacking Images in Docker Hub

unit42.paloaltonetworks.com/malicious-cryptojacking-images/

Aviv Sasson

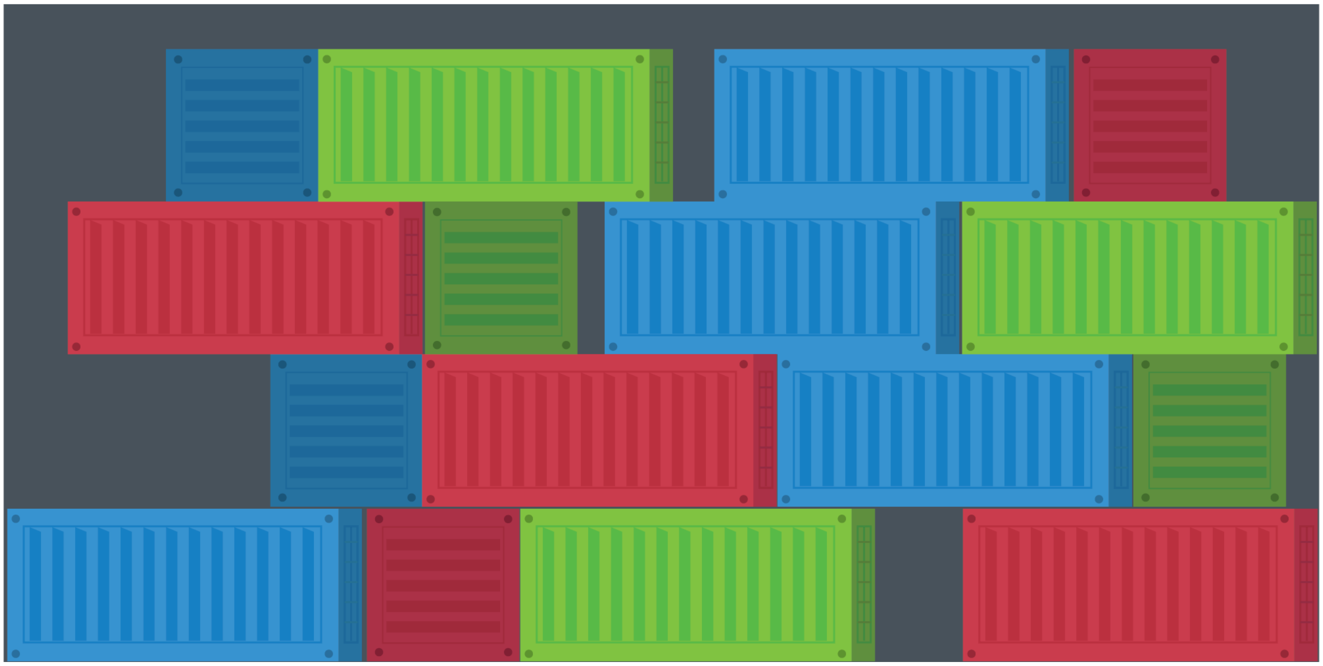
March 26, 2021

By Aviv Sasson

March 26, 2021 at 6:00 AM

Category: Cloud, Malware, Unit 42

Tags: cryptojacking, Cryptominers, Docker, Docker Hub, Monero



This post is also available in: 日本語 (Japanese)

Executive Summary

As a cybercriminal, there are many ways to make a profit. One of the easiest ways is cryptojacking – the illegal use of someone else’s computing resources to mine cryptocurrencies. Container images are known as a simple way to distribute software, yet malicious cryptojacking images are also a simple way for attackers to distribute their cryptominers.

I decided to take an extensive look into Docker Hub and discovered 30 malicious images with a total number of 20 million pulls (which means the images were downloaded 20 million times), together accounting for cryptojacking operations worth US$200,000. In this post, I will elaborate on my findings and why it is reasonable to assume that there are many other undiscovered malicious images on Docker Hub and other public registries.

Palo Alto Networks Prisma Cloud customers are protected from these threats through the Cryptominers Runtime Detection feature and the Trusted Images feature. In addition, Palo Alto Networks Next-Generation Firewall customers with the Threat Prevention security subscription are protected against the delivery of these images.

Finding Malicious Cryptojacking Images

In the last several years, Unit 42 researchers have been witnessing cloud-based cryptojacking attacks in which miners are deployed using an image in Docker Hub.

The cloud is popular for cryptojacking attacks due to two main reasons:

- The cloud consists of many instances for each target (e.g. lots of CPUs, lots of containers, lots of virtual machines), which can translate to big mining profits.
- The cloud is hard to monitor. Miners can run undetected for a long time, and without any detection mechanisms in place, they may run until the user finds an inflated cloud usage bill and realizes that something is wrong.

Modern cloud technology is largely based on containers, and in some environments, Docker Hub is the default container registry. Attackers can take advantage of it to deploy miners on compromised clouds.

Because of all of the facts mentioned above, I wanted to see if I could find malicious cryptojacking images in Docker Hub. In my research, I found 30 images from 10 different Docker Hub accounts that account for over 20 million pulls.

Individuals improve their mining efficiency by using mining pools, and so do adversaries.

It is possible to check how many cryptocurrencies were mined to a mining pool account by inspecting the mining pool. Half of the images I found used a mining pool that shares this information, and by extrapolating from that half I estimated that, in total, in all of the attacks, US$200,000 worth of cryptocurrencies were mined.

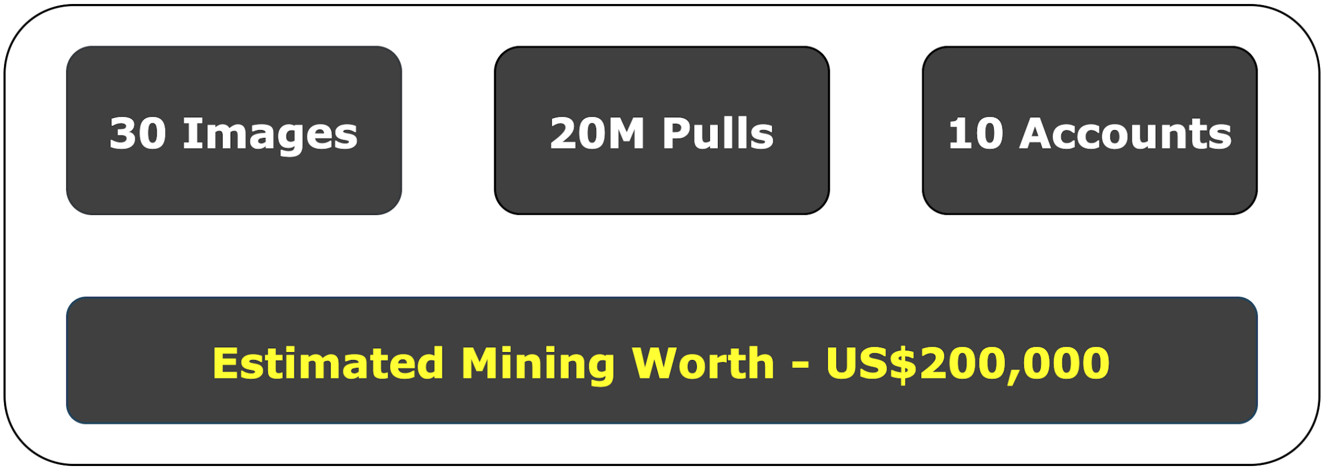


Figure 1. Research findings.

In order to better understand the findings, I began classifying the results. With the help of public mining pools, I checked which cryptocurrency is mined, which cryptominer is used and how many coins have been mined.

Coin Distribution

My first discovery, perhaps not surprising to our returning readers, is that the most popular cryptocurrency for attackers to mine is Monero, just as we saw with Pro-Ocean, Cetus and many more.

Attackers favor Monero for three reasons:

- Monero provides maximum anonymity. One of its features is that, unlike for other coins, Monero transitions are hidden. This privacy is perfect for cybercriminals because it means their activity is hidden. Hence, they won't get banned from exchanges and it is easier for them to evade attempts to track their funds.
- The Monero mining algorithm favors CPU mining, unlike many other cryptos that require ASICs or GPU for mining. This is convenient because all computers have CPUs. Thus, the miner can run effectively on any machine. This is even more suitable for containers, of which the vast majority run without a GPU.
- Monero is a popular coin, and its exchange volume is around US$100 million a day, making it easy for the attackers to sell their coins.

The figure below demonstrates the cryptocurrency distribution of the cryptojacking images found on Docker Hub.

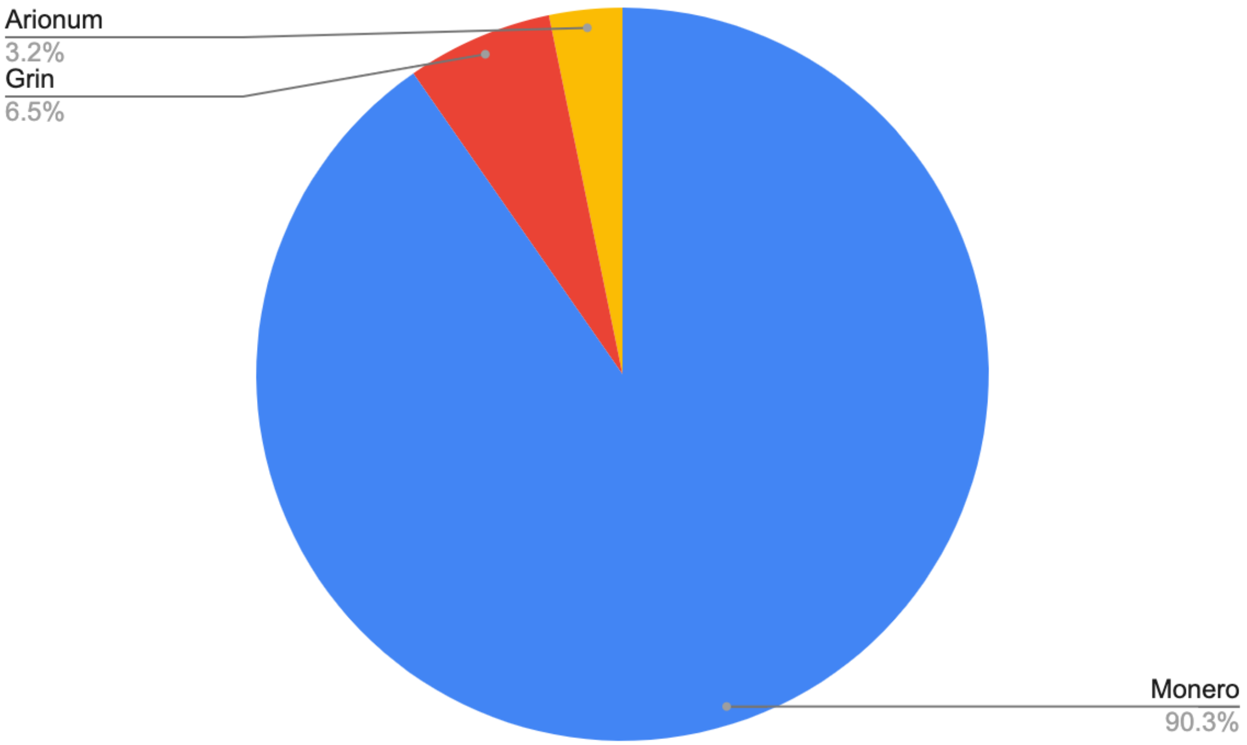


Figure 2. Cryptocurrency distribution.

Cryptominer Distribution

In most attacks that mine Monero, the attackers used XMRig, just as we saw with Hildegard and Graboid. XMRig is a popular Monero miner and is preferred by attackers because it's easy to use, efficient and, most importantly, open source. Hence, attackers can modify its code.

For example, most Monero cryptominers forcibly donate some percentage of their mining time to the miner's developers. One common modification attackers make is to change the donation percentage to 0.

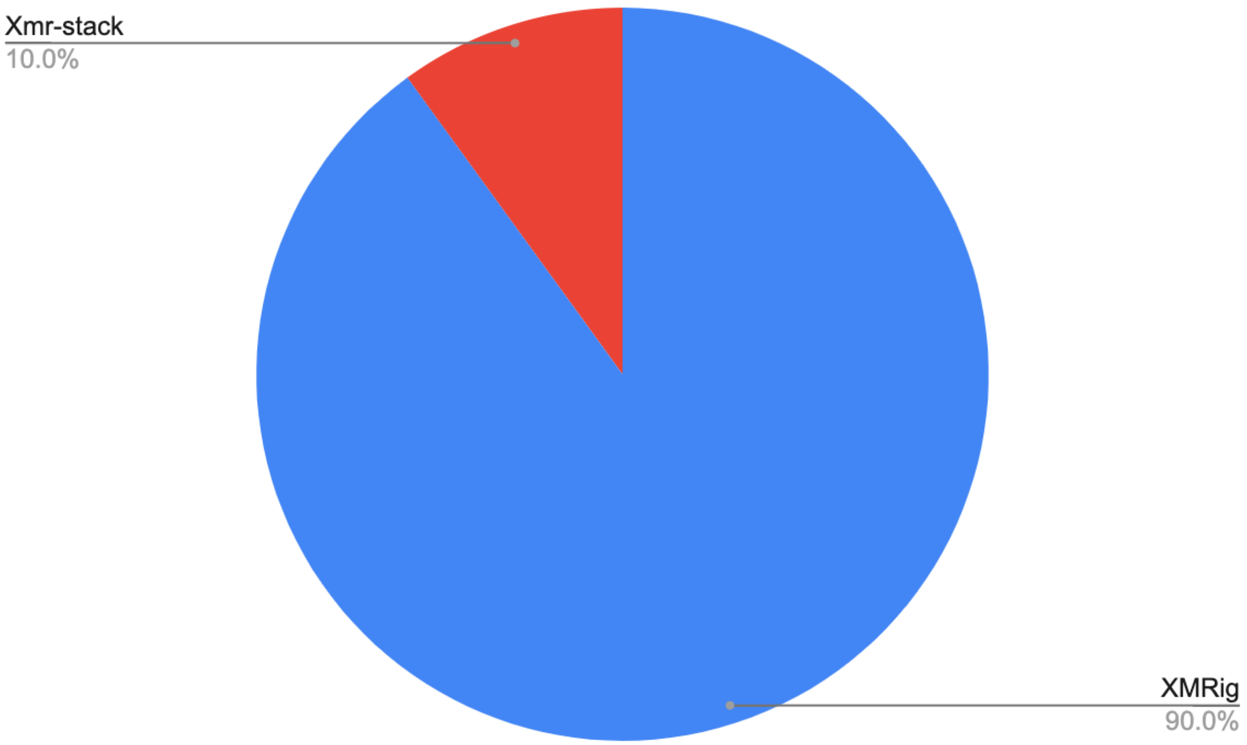


Figure 3. Cryptominer distribution.

Image Tags

Container registries allow users to upgrade their images and in that process upload a new tag to the registry. Tags are a way to reference different versions of the same image.

When examining the tags of the images, I found that some images have different tags for different CPU architectures or operating systems. It seems like some attackers are versatile and add these tags in order to fit a broad range of potential victims that includes a number of operating systems (OS) and CPU architectures.

In some images, there are even tags with different types of cryptominers. This way, the attacker can choose the best cryptominer for the victim's hardware.

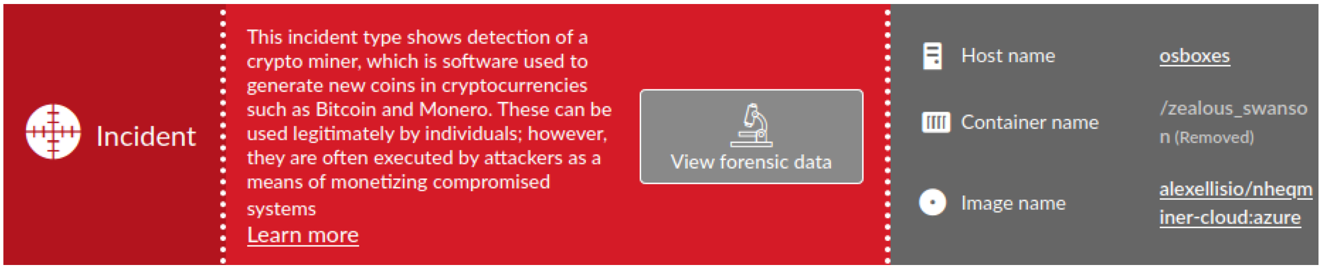
The only thing that is common for all the tags in a certain image is the wallet address or the mining pool credentials. With the help of these identifiers, I could classify each campaign. After digging deeper, in some cases, I could see that there are numerous Docker Hub accounts that belong to the same campaign. For example, in previous research, Unit 42 found the malicious account azurenql. Now, we discovered that the campaign is broader and includes the accounts 021982, dockerxmrig, ggcloud1 and ggcloud2.

In my research, I was able to find additional images mining Monero for the same campaign described in recent Unit 42 findings on azurenql, adding over 10 million more pulls under the attacker's name.

Conclusion

The cloud presents big opportunities for cryptojacking attacks. In my research, I used a cryptomining scanner that only detects simple cryptomining payloads. I also made sure any identified image was malicious by correlating the wallet address to previous attacks. Even with these simple tools, I was able to discover tens of images with millions of pulls. I suspect that this phenomenon may be bigger than what I found, with many instances in which the payload is not easily detectable.

Palo Alto Networks Prisma Cloud customers are protected from these threats through the Cryptominers Runtime Detection feature and the Trusted Images feature. In addition, Palo Alto Networks Next-Generation Firewall customers with the Threat Prevention security subscription are protected against the delivery of these images.



This incident type shows detection of a crypto miner, which is software used to generate new coins in cryptocurrencies such as Bitcoin and Monero. These can be used legitimately by individuals; however, they are often executed by attackers as a means of monetizing compromised systems

Host name osboxes

Container name /zealous_swanson (Removed)

Image name alexellisio/nheqminer-cloud:azure

Figure 4. Prisma Cloud container incident notification.

Indicators of Compromise

Docker Images

021982/155_138

021982/66_42_53_57

021982/66_42_93_164

021982/xmrig

021982/xmrig1

021982/xmrig2

021982/xmrig3

021982/xmrig4

021982/xmrig5

021982/xmrig6

021982/xmrig7

avfinder/gmdr

avfinder/mdadmd

docheck/ax

docheck/health

dockerxmrig/proxy1

dockerxmrig/proxy2

ggcloud1/ggcloud

ggcloud2/ggcloud

kblockdkblockd/kblockd

osekugatty/picture124

osekugatty/picture128

tempsbro/tempsbro

tempsbro/tempsbro1

toradmanfrom/toradmanfrom

toradmanfrom/toradmanfrom1

xmrigdocker/docker2

xmrigdocker/docker3

xmrigdocker/xmrig

xmrigdocker/xmrig

zenidine/nizadam