Sophisticated Supply Chain Attacks on Container Infrastructure

CISO Executive Brief

Executive Summary

Over the past year we observed numerous attacks targeting container environments, leveraging innocuous-looking container images to plant sophisticated, multi-stage malware that evades static scanning and signature-based tools. These attacks are well-organized and conducted on a large scale. Most attacks were launched with the aim of abusing their targets' cloud resources to mine for cryptocurrency, but the techniques used enable attackers to run arbitrary code in containers, opening the door to a variety of attack objectives.

The full results of our research are available in our Threat Report »

Threat Report Highlights

- Container images in public registries are being poisoned with Potentially Unwanted Applications (PUAs) that cannot be detected using static scanning. It springs into action only when the container is running.
- New and sophisticated evasion techniques are being used to hide attacks and make them more persistent. This includes the use of "vanilla" images that seem innocuous, disabling other malware, delaying before downloading payloads into the container, using 64-bit encoding to obfuscate malware, and more.
- Since the beginning of 2020, the volume of attacks has dramatically increased. Further analysis indicates that there are organized infrastructure and systematic targeting behind these attacks, we observed 16,371 attacks that we tracked back to multiple locations across the globe.
- The main motivation of the malicious actors has been to hijack the targets' cloud compute resources to mine for cryptocurrency, but we have seen evidence that other objectives, such as establishing DDoS infrastructure, were achieved in this manner.

Observed Attacks in the Wild

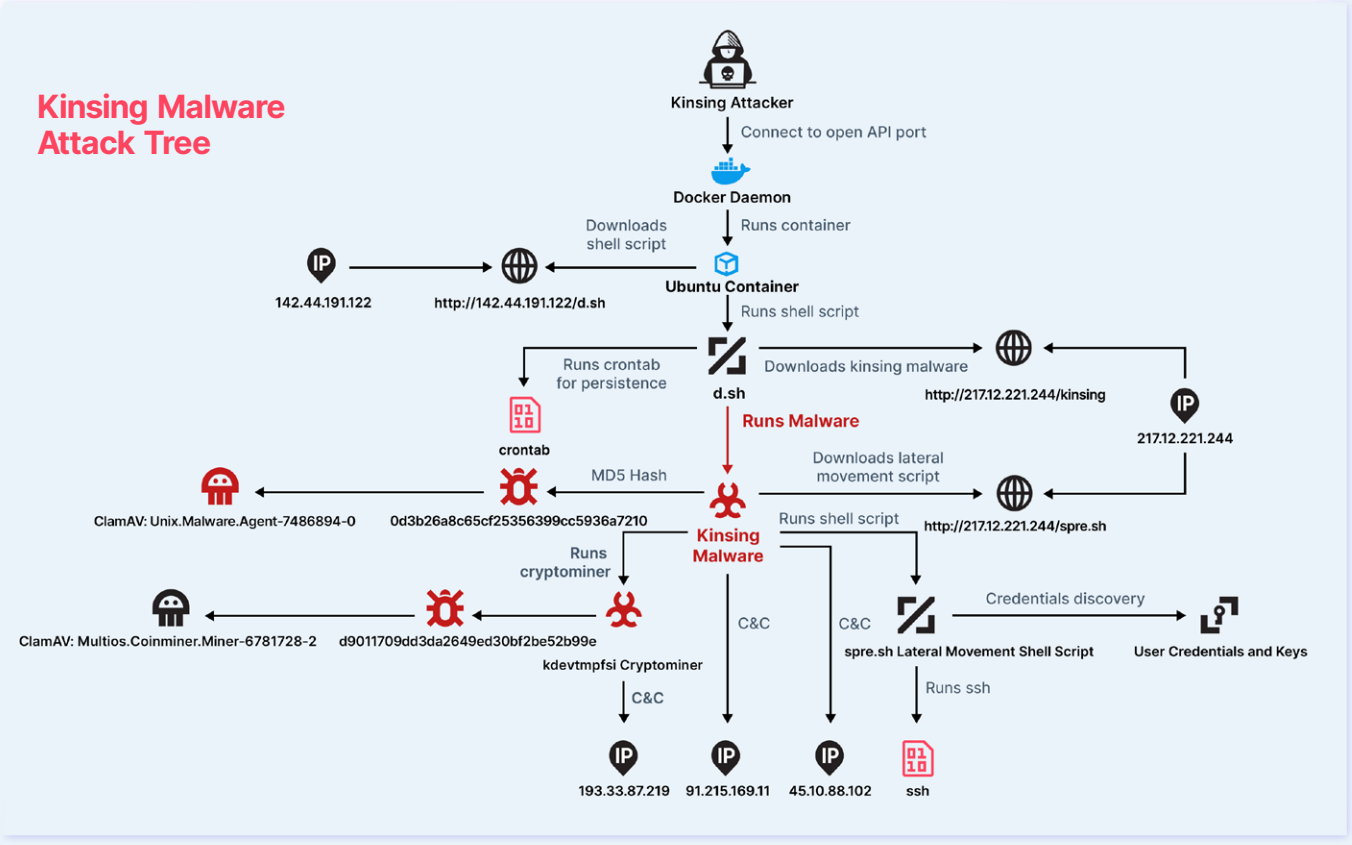
Anatomy of the attacks

70.7% of the attacks were built to mislead and conceal their malicious nature:

- Images might seem as novel, innocuous-looking and the adversaries embed their code, which is often encrypted or deployed as polymorphic malware to avoid detection. Because some organizations only permit the usage of official images, for instance 'alpine: latest', from a predetermined, explicitly allowed list, this increases the chances that the attack will be executed as planned since that these images will be pre-approved for use.

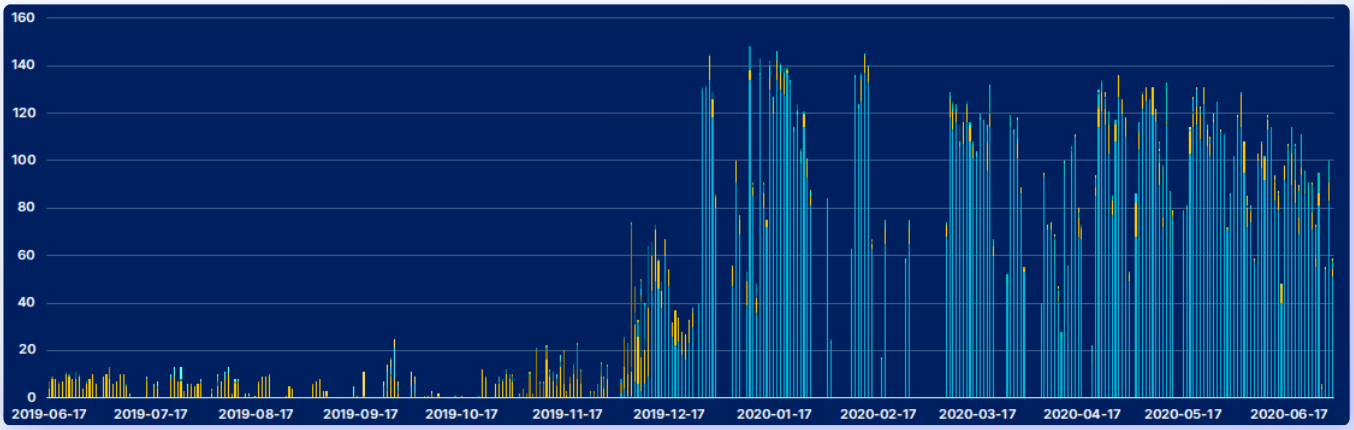
- Dedicated obscure malicious images executed scripts aimed to download malicious components from an external remote source.

The attack tree of one such observed attack, deploying the Kinsing malware



Scale and trending

Between June 2019 and July 2020, we observed thousands of attacks **against our honeypots**. Between June 2019 and January 2020, the average number of attacks per day increased 50%, but since January 2020 and until the end of June 2020, the number of attacks per day exploded, increasing by more than 250%.



Our analysis suggests that the threat landscape shifted towards organized cybercrime, which is investing in infrastructure that allows them to find exposed/vulnerable hosts and systematically target cloud native infrastructure.

Origin of the Attacks

The attackers' IP addresses mainly originated from the US and China, using the following hosting service providers: Aliyun (Alibaba), Digital Ocean, and Chinanet.

Impact and Risk

- 95% of the images were designed to hijack resources for the sole purpose of cryptocurrency mining and 5% of the images were set to launch a Distributed Denial-of-Service attack.
- With the rising threat of image-based malware, adversaries can inject code to an image and leverage more advanced APTs.

How Can You Reduce Exposure?

With the increase in cloud native technology adoption, organizations need to be prepared with a strong cloud native security strategy. The increased velocity of modern pipelines, extensive use of open-source packages and images from different sources have created new security risks and malicious actors have been paying attention and adjusting their strategies accordingly. The increasingly sophisticated attacks we have witnessed require the use of new dynamic analysis techniques to detect them and thwart them in time.

We recommend that security organizations work to methodically close the strategic gaps in their security posture by addressing these three areas:

Protect the supply chain - shift-left security

- Limit access to public image registries, control who can access and download container images and other open source artifacts within your organization, and create a trusted private registry for approved base images.
- Incorporate image vulnerability scanning into your CI pipeline in order to detect issues early and allow for quick remediation.
- Use Aqua Dynamic Threat Analysis to discover and assess sophisticated malware hidden in container images, intercepting them before they are run in production environments.

Control what you deploy

- Add Assurance policies to your CI/CD pipeline and ensure that non-compliant images are blocked from progressing through the CI/CD pipelines.
- Review authorization and authentication policies, basic security policies, and adjust them according to the principle of least privilege

Define a clear cloud native security strategy

- Be sure to cover your entire stack and full application lifecycle.
- Implement automation and manage the security posture of your cloud environments across all cloud providers.

Get the Full Cloud Native Threat Report »

aquasec.com
@AquaSecTeam
@Aqua Security
contact@aquasec.com
in/Aqua Security
@AquaSecTeam