Malware Protection on Containers

Author: Stefan Alfeis, stefan.alfeis@quant-x-sec.com

Malware – a quick view

When thinking about malware protection, we need to bring to mind what exactly malware is. At its core, malware is nothing but a program – one with malicious intent. With that in mind, it should be clear that potentially every existing operating system can be infected by malware. Containers are no exception. In the following paragraphs, we are going to have a look at how we can protect our container environment against malware.

Basic configurations

The first thing we need to remember when securing a system is to set up the basic configurations (according to the the so-called security baselines) for our operating system. System specific security baseline recommendations by official instances such as the Center for Internet Security (CIS) are available publicly[1]. For Linux OS, you should take a close look at SE Linux and App Armor. See our whitepaper *"platform_security_app_armor_SE_linux.pdf"* for more background information. These two security applications take some time to set up, but, in the end, the overall system security will be improved considerably.

The next step is to keep your system up to date. This requirement is fulfilled by establishing good patch management processes on each affected technical component. Many backdoors and exploits are fixed by regular updates. Always take your time to view the update notes to make sure that all affected technical components are covered. For complex infrastructures, it makes sense to set up a patch management tool. E. g. Bitdefender[2] offers this feature in addition to malware protection.

An example for a threat through misconfiguration occurred around May 2020[3]. Back then, there was an attack on Docker systems which had some open ports in their daemons. Attackers used this to set up malicious cryptocurrency miners and Distributed Denial of Service (DDoS) bots. This example should make it clear that, even though it takes some time to set up a secure system, it is worth the effort – even if you are not controlled by regulatory instances, as some critical infrastructure providers are. You should regularly take some time to review your security baselines and their implementation on the system (configuration) to ensure everything is up to date and that there are no wrong configurations.

1 https://www.cisecurity.org/benchmark/
2 https://www.bitdefender.com/
3 https://www.trendmicro.com/vinfo/hk-en/security/news/virtualization-and-cloud/malicious-docker-hub-container-images-cryptocurrency-mining

One more thing you should never miss out on is protecting your network. Always remember to set up everything necessary to secure your network, like firewalls, VPNs, DMZ's etc. With a secure network, you can minimize potential threats, especially from experienced cybercrime organizations with massive attack resources[4].

Malware protection for containers

Due to the ongoing growth in container usage, many security companies have also started creating malware protection for containers[5]. Some of these security programs start scanning the container images during the creation of the container image itself, which is really helpful to get the right setup from the start. The container images are monitored for malware, vulnerabilities and for acting towards the compliance-guidelines. Other programs offer protection of the container runtime environment and even gather forensic data from this. During the build of the environment, these systems search for vulnerabilities and monitor the configuration. The active environment is monitored for events, metrics are gathered and security policies are monitored as well. To get the fastest response to any incident, these systems can be connected to SIEM solutions. Furthermore, with some programs, you can create maps of your existing containers, showing all of the connections and behavior.

Conclusion

There are several ways to enforce security and, in particular, malware protection in your container environment. Always keep the basic system configurations of all involved components up to date and take your time to get everything that is needed to assure the highest possible level of security covered. As time goes on, there will be more and more possibilities to add security programs to your existing systems. As for the system configuration, take your time to see what best fits your needs apart from the official recommendations. But be aware of risks when you deviate.

BiNome platform managed container images are built and managed on our own platform and therefore subject to strict malware protection measures.

4 https://containerjournal.com/topics/container-security/protecting-containers-against-doki-malware/
5 https://www.computerwoche.de/a/7-security-tools-fuer-docker-und-kubernetes,3546931