Cryptomining attacks on Docker systems

Threat Memo - Date: 08/04/2020 - Version: 1.0
TLP:WHITE

	Category	Type	Domain(s)	Sector(s)	Confidence
FOR INFORMATION	Cybercrime	Unauthorised access, API abuse, Cryptomining	World	Cloud, IT services	A1

Key Points

- Insecure instances of the popular Docker virtualisation platform are being targeted in a wide spread campaign aiming to abuse them for cryptomining.
- The methodology of the campaign exposes unsecured Docker installations and may also endanger other hosted applications, the hosting server, and adjacent systems.
- The case underlines the dangers of inadequate security configurations resulting in publicly exposed systems.

Summary

On April 3, 2020 the cloud security company AquaSec published information[1] on a widespread campaign targeting the software platform Docker. The goal of the attackers is to install and operate cryptomining malware. Docker is a suite of software residing on the Linux host operating system that allows software packages (called containers) to make use of a complete OS environment independent of other software also operating on the same machine. In this respect, it offers a ready operating system environment acting as a platform-as-a-service cloud service solution. The containers are highly transportable and can be installed in different Docker environments including single hosts and cloud hosting. The Docker Engine provides an API to accommodate the installation, operation, and management of Containers.

As any other piece of software, Docker installations require careful configuration concerning what resources they may expose to third parties. The cyber-crime campaign referenced particularly abuses inadequately secured Docker Engine instances that expose their API to the Internet. The attackers transfer and install a Container that, after ensuring detection evasion and persistence, operates a piece of malware called Kinsing. The Kinsing malware:

- Connects to a Command and Control (C2) infrastructure.
- Attempts to move laterally in the organisation, targeting other containers as well as hosts (using ssh connections based on information passively gathered from its host system).
- Downloads and operates a cryptominer called kdevtmpfsi.

The AquaSec researchers reported that the campaign has been active for several months (since at least March 2019), with “thousands of attempts taking place nearly on a daily basis”. This indicates a threat actor with the intention, persistence, and resources to continuously follow it up. The popularity and wide deployment of the Docker platform offers numerous opportunities to abuse vulnerable and misconfigured installations both in host as well as in cloud environments.

The case underlines the dangers of misconfigured multi-tenant cloud installations as weaknesses in the hosting software can result in exposure of the host, other installed tenants, and adjacent systems. It is also a warning call for potential data exposure threats using similar techniques.

Comments

As previously pointed in CERT-EU Threat Memos, misconfigured and open to the internet software installations expose the systems and data of an organisation to various sorts of threats (please also see recent reporting on insecure Elasticseach databases in TM 20-038). In this specific case, cryptomining malware steals the resources of exposed machines, significantly affecting their performance.

CERT-EU monitors this as well as other similar threats and will continue to update the EU-I on them.

[1] https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability