Threat Alert: TeamTNT Pwn Campaign Against Docker and K8s Environments

blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment

Assaf Morag

Assaf Morag

February 17, 2021

Last week, TeamTNT launched a new campaign against Docker and Kubernetes environments. Using a collection of container images that are hosted in Docker Hub, the attackers are targeting misconfigured docker daemons, Kubeflow dashboards, and Weave Scope, exploiting these environments in order to steal cloud credentials, open backdoors, mine cryptocurrency, and launch a worm that is looking for the next victim. In this blog, I will explore these container images and what they were designed to do.

The Docker Hub account 'heavy0x0james' was created on June 3rd, 2019. In February 2021, the adversaries uploaded six malicious container images that have been observed to perform attacks in the wild. All six container images initially run a shell file named init.sh, but in each image it does something different. Then the attackers leverage a binary named zgrab (MD5= 7691c55732fded10fca0d6ccc64e41dc) in order to scan the internet for more victims.

Below is the list of these malicious container images and their capabilities:

Container images	Capabilities
Wescopwn	• Run a cryptominer • Execute a worm • Scan ports 80, 443, 8080, 8888 • Look for vulnerable weave scope applications • Execute Tsunami malware
Tornadopwn	• Execute a worm • Scan AWS IP ranges • Scan ports 80, 443, 8080, 8888 • Look for vulnerable Kubeflow and Jupyter notebooks
Jaganod	• Execute a trojan (/usr/local/lib/dockerd.so) • Execute a worm • Scan ports 80, 2375, 2376, 4243, 4040, 8888 • Look for vulnerable Docker daemons, vulnerable weave scope applications and vulnerable Kubeflow and Jupyter notebooks
Awspwner	• Execute a worm • Scan AWS IP ranges • Scan ports 2375, 2376, 2377, 4244, 4243 • Execute AWS keys grabber
Tornadorangepwn	• Execute a worm • Scan ports 80, 443, 8080, 8888 • Execute AWS keys grabber

Conclusion

Over the last few years, we at Team Nautilus have detected many kinds of attacks against Docker and Kubernetes environments, but this is the first time that we see a campaign designed to massively and systematically scan the internet, search for specific misconfigurations or outdated software, and attack the potential victims. Some of these images deploy a cryptominer, some open backdoors, and others are looking to steal AWS keys. These findings should alert security practitioners that even the smallest misconfiguration even for a fraction of time matters as it can result in a cyberattack.

When working with Docker and

1. **Regularly update your cloud software, specifically Docker and Kubernetes projects**. Previous versions typically have more known vulnerabilities.
2. If possible, **avoid exposing unnecessary APIs to the internet.** Additionally, try limiting APIs inbound and outbound traffic to your organization's network range.
3. **Review authorization and authentication policies, basic security policies**, and adjust them according to the principle of least privilege.
4. **Regularly monitor the runtime environment.** This includes monitoring the running containers, their images, and the processes that they run. Investigate logs, mostly around user actions, look for actions you can't account for regular anomalies or outliers.
5. Implement a security strategy where you can easily enforce runtime policies, as well as consider using cloud security tools that will widen your scope and reach within your cloud resources.

Indication of Compromise (IOCs)

heavy0x0james/dockgeddon:latest

- root/dockerd (MD5= 091efbe14d22ecb8a39dd1da593f03f4)
- root/TNTfeatB0RG (MD5= 624e902dd14a9064d6126378f1e8fc73)
- C2= 45[.]9[.]148[.]85

heavy0x0james/wescopwn:latest

- root/dockerd (MD5= 091efbe14d22ecb8a39dd1da593f03f4)
- root/TNTfeatB0RG (MD5= 624e902dd14a9064d6126378f1e8fc73)
- C2= 45[.]9[.]148[.]85, borg[.]wtf

heavy0x0james/tornadopwn:latest

C2= 45[.]9[.]148[.]85

heavy0x0james/jaganod:latest

- usr/local/lib/dockerd.so (MD5= e8b1dc73a3299325f5c9a8aed41ba352)
- root/dockerd (MD5= 091efbe14d22ecb8a39dd1da593f03f4)
- C2= 45[.]9[.]148[.]85

heavy0x0james/awspwner:latest

- aws.sh
- C2= borg[.]wtf

heavy0x0james/tornadorangepwn:latest

- aws.sh
- C2= borg[.]wtf

Assaf Morag

Assaf is a Lead Data Analyst at Aqua. As part of Team Nautilus, Aqua's research team, he focuses on supporting the data needs of the team, obtaining threat intelligence and helping Aqua and the industry stay on the forefront of new threats and methodologies for protection. His work has been published in leading info security publications and journals across the globe, and most recently he contributed to the new MITRE ATT&CK Container Framework.

Security Threats, Dynamic Container Analysis

- Tweet
-