ADVISORY FOR ICM SECTORS

TeamTNT Returns with a Docker Gatling Gun Campaign

Original report published on: Oct 25, 2024

Executive Summary

Aqua Security researchers warn of a new campaign by TeamTNT, a threat group targeting cloud-native environments. The campaign, dubbed "Docker Gatling Gun", leverages compromised Docker daemons to deploy malicious payloads. By appending compromised Docker instances to a Docker Swarm, TeamTNT is extending its attack range. Docker Swarm allows for the creation of clusters from multiple Docker engines. This enables attackers to launch attacks on a wider scale.

The attackers are also leveraging Docker Hub, a repository for container images. TeamTNT can store and distribute its malware through Docker Hub, making it readily available to potential victims.

Background

TeamTNT, a known cybercriminal group, has primarily targeted cloud and containerised environments such as Kubernetes (K8s) and Docker. The group has been active since at least October 2019 and mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.

TeamTNT appears to be returning to its roots while preparing for a large-scale attack. The threat actor replaced its traditional Tsunami backdoor with the stealthier "Sliver" malware. "Sliver" is an open-source, cross-platform, adversary emulation, and red-team framework. Its implants support Command and Control (C2) over multiple protocols, and dynamically compiled with per-binary asymmetric encryption keys. It can be used to execute commands and deliver payloads, including in-memory execution.

The campaign gains initial access by exploiting exposed Docker daemons on ports *2375*, *2376*, *4243*, and *4244*. The attack script, which scans for these ports, is known as the Docker Gatling Gun. It targets wide range of IP addresses (approximately ~16.7 million) and deploy container from compromised Docker Hub account. The container will execute an initial script called "TDGGinit.sh" (Short for TeamTNT's Docker Gatling Gun init shell script).

TeamTNT has always experimented with cloud native open-source software (OSS) and offensive security tools. In this campaign, Aqua Security observed use of Docker Hub to store and spread malware, and Sliver for control and exploitation. TeamTNT monetised computational power belonging to victims' systems, in exchange for cryptocurrency and financial gain. This group of images includes the following crypto-mining software; XMRIG, T-Rex miner, CGMiner, BFGMiner, and SGMiner.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Scan for Indicators of Compromise (IOCs) on your network. Validate before adding malicious file hashes to blocklist in antivirus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR) including servers.
- Conduct regular scan of images for vulnerabilities with tool like Docker Scan.
- Run containers with the least privilege necessary to reduce attack surface.
- Verify the authenticity and integrity of images.
- Network segmentation to isolate Docker hosts and containers from other systems to limit the impact of a compromise.
- Only allow necessary network traffic to and from Docker hosts and containers.
- Configure Network Security Groups (NSGs) to control inbound and outbound traffic to Docker hosts.
- Secure SSH access by using strong passwords, two-factor authentication, and SSH key-based authentication.
- Regularly review and monitor system and security logs for signs of intrusion.
- Restrict access to the Docker daemon to authorised users only.
- Harden and disable unused Docker features to reduce attack surface.
- Implement a container runtime security solution to monitor container behaviour and detect anomalies.
- Develop and test an incident response plan to contain and mitigate attacks fast.
- Implement regular backups to recover from data loss or corruption.
- Use a Container Security Platform to manage and secure container environment.

Notable MITRE ATT&CK Tactics and Techniques

Tactic	Technique
Initial Access	T1190 – Exploit Public-Facing Application
Execution	T1059 – Command and Scripting Interpreter
Persistence	T1578.002 – Modify Cloud Compute Infrastructure
Defence Escalation	T1014 – Rootkit
	T1036 – Masquerading
	T1211 – Exploitation for Defence Evasion
Credential Access	T1552.001 – Unsecured Credentials: Credentials in Files
Discovery	T1018 – Remote System Discovery
Command and Control	T1071.004 – Application Layer Protocol: DNS
	T1090 – Proxy
	T1102.001 – Web Service: Dead Drop Resolver
Impact	T1496 – Resource Hijacking

Indicators of Compromise (IOCs)

Type	Value	Comment
IP Address		
IP Address	188[.]114[.]96[.]7	Host download server
IP Address	104[.]21[.]8[.]145	Host download server
IP Address	172[.]67[.]10[.]114	Host download server
IP Address	45[.]154[.]2[.]77	Sliver C2
IP Address	95[.]182[.]101[.]23	Tsunami C2
Domain		
Domain	solscan[.]life	-
Domain	solscan[.]one	-
Domain	solscan[.]online	-
Domain	solscan[.]store	-
Domain	devnull[.]anondns[.]net	-
Domain	teamtnt[.]red	-
Files		
Binary File (MD5)	b62ce36054a7e024376b98df7911a5a7	prochider (xmrig[.]so)
Binary File (MD5)	64c3ac5a0f4318f64f438e78a6b42d40	prochider (systemd[.]so)
Binary File (MD5)	8b553728900ba2e45b784252a1ff6d17	Sliver Malware (SPLENDID_ISLAND)
Binary File (MD5)	9dc2819c176c60e879f28529b1b08da1	Sliver Malware (bioset)
Shell Script (MD5)	a733160e0603207d8328ddb025c43d42	TDGGinit, TDGGinit[.]sh
Shell Script (MD5)	fdf9c2f7221de9f3567fc094d5e759a9	TDGG, TDGG[.]sh
Shell Script (MD5)	0bc189bb53c9c92322e7b2fd6ac68bd7	docker
Perl Script (MD5)	db2fbe4d00b222cab6dd00cdfdd38e31	scan[.]pl
Docker Hub Account		
nmlm99	https://hub[.]docker[.]com/u/nmlm99	Disseminates malware and crypto miners

References

1. “Aqua Nautilus - TeamTNT's Docker Gatling Gun Campaign”
2. “MITRE ATT&CK - TeamTNT [G1039]”