Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

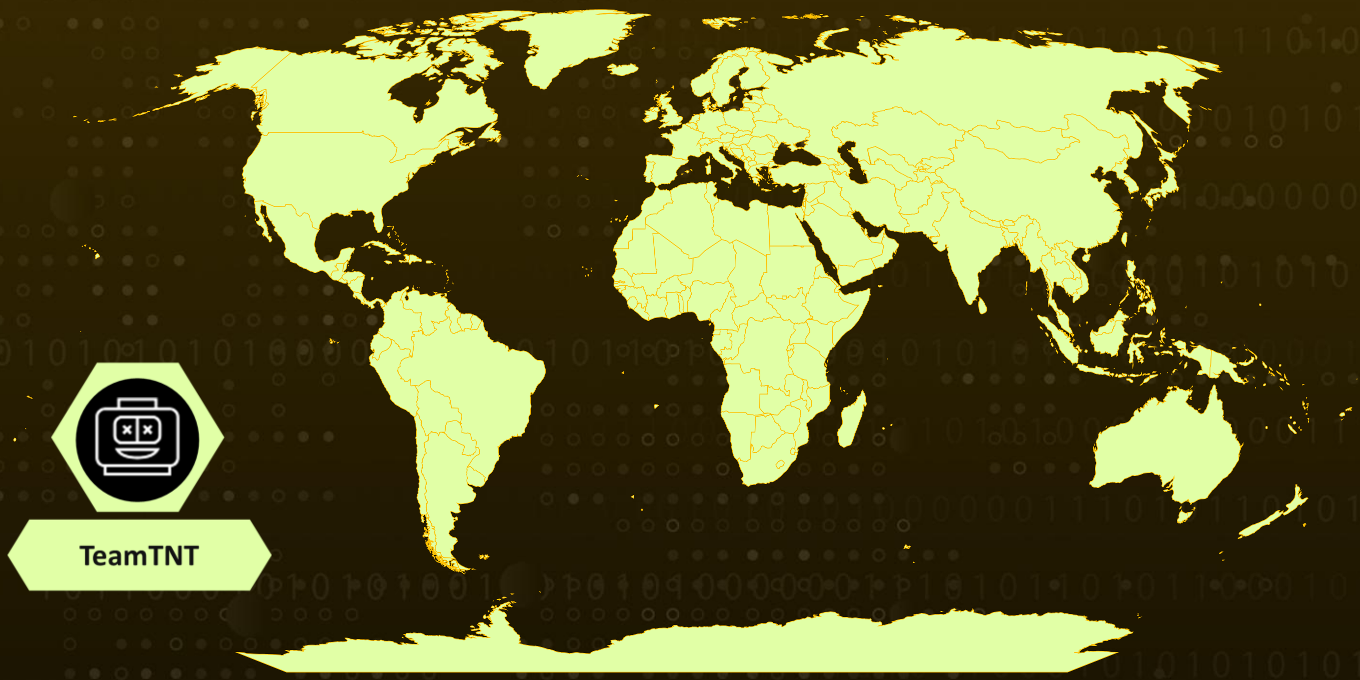
TeamTNT Taps Docker to Unleash Sliver Malware in Major Cloud Assault

Date of Publication	Admiralty Code	TA Number
October 28, 2024	A1	TA2024413

Summary

Attack Discovered: 2024
Targeted Countries: Worldwide
Malware: Sliver, Tsunami
Actor: TeamTNT (aka Adept Libra)
Attack: TeamTNT, a notorious hacking group, is preparing a large-scale campaign targeting cloud-native environments, marking a return to their original methods. The group is leveraging exposed Docker daemons as a critical entry point, allowing them to infiltrate and exploit vulnerable cloud infrastructures. Through these entry points, TeamTNT aims to deploy the Sliver malware, and a cyber worm alongside cryptominers, using compromised servers and Docker Hub as pillars of their malicious ecosystem. This approach highlights the group's adaptability and emphasizes the critical need for vigilant cloud security to thwart resource hijacking and malware spread.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 TeamTNT, a persistent hacking group, is advancing a large-scale campaign targeting cloud-native environments, with a primary focus on exposed Docker daemons. The group initiates the attack by exploiting Docker instances with publicly accessible API ports, gaining initial access through open Docker daemons on ports such as 2375, 2376, 4243, and 4244. After compromising these Docker environments, TeamTNT uses Docker Hub to host and distribute its malware, leveraging it as both a storage and propagation platform. Their payloads include the stealthier Sliver malware, cryptominers, and a cyber worm designed to maintain persistence and resource hijacking capabilities.

#2 Once inside a network, TeamTNT deploys its “Docker Gatling Gun,” an automated attack script that aggressively scans vast IP ranges for vulnerable instances. This script deploys malicious containers from a compromised Docker Hub account, triggering an Alpine Linux image that executes a secondary script which runs various malicious commands to further the infection.

#3 Following this, TeamTNT integrates compromised instances into a Docker Swarm, utilizing Docker’s clustering capabilities to manage these infected containers as a cohesive group. This setup allows TeamTNT to scale its control across the infected infrastructure efficiently. For communication, TeamTNT has shifted from using the Tsunami backdoor to the more adaptive Sliver malware, which facilitates multi-protocol command and control (C2) communications. This upgrade provides enhanced stealth and resilience, making it harder for defenders to detect and disrupt their operations.

#4 To maintain anonymity, TeamTNT uses services like anondns and deploys domains, such as devnull.anondns.net, to mask traffic directed toward their command servers. The group’s technique of outsourcing victims’ computational power to third parties for cryptomining allows them to profit indirectly without managing the cryptomining infrastructure themselves, further obfuscating their involvement.

#5 This campaign highlights TeamTNT’s growing sophistication and strategic evolution in their malware distribution and resource hijacking tactics. Organizations can protect against these attacks by enforcing strict security configurations on Docker instances and actively monitoring for any unusual activity indicative of such intrusions.

Recommendations

Update and Patch Regularly: Keep Docker software, operating systems, and associated components up to date with the latest security patches.

Implement DNS Filtering: Block or monitor access to known malicious domains, like those used in anondns or other anonymous DNS services, which attackers use to obfuscate C2 channels.

Use Official Images: Always source Docker images from trusted, official repositories to reduce the risk of malware-laden or vulnerable software. Official images are regularly reviewed and updated for security, ensuring a more reliable foundation for your containers. Avoid using unverified or custom images from public registries unless thoroughly inspected.

Restrict Docker Access: Configure your Docker daemons to bind only to localhost or internal IP addresses, preventing direct access from external networks. Restrict API access to specific, trusted IP ranges. This minimizes the risk of unauthorized connections from unknown sources.

Run Containers as Non-Root User: Configure containers to operate as non-root users to minimize the impact of potential security breaches. Running with non-root privileges limits access to host resources and reduces the risk of privilege escalation. Ensure each container specifies a user with only the permissions necessary for its functions, following the principle of least privilege.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0040 Impact	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1578 Modify Cloud Compute Infrastructure
T1578.002 Create Cloud Instance	T1211 Exploitation for Defense Evasion	T1036 Masquerading	T1552 Unsecured Credentials

T1552.001 Credentials In Files	**T1552.007** Container API	**T1586** Compromise Accounts	**T1586.003** Cloud Accounts
T1014 Rootkit	**T1018** Remote System Discovery	**T1102** Web Service	**T1102.001** Dead Drop Resolver
T1071 Application Layer Protocol	**T1071.004** DNS	**T1090** Proxy	**T1496** Resource Hijacking
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	188[.]114[.]96[.]7, 188[.]114[.]96[.]7, 104[.]21[.]8[.]145, 172[.]67[.]130[.]114, 45[.]154[.]2[.]77, 95[.]182[.]101[.]23
Domains	solscan[.]life, solscan[.]one, solscan[.]online, solscan[.]store, devnull[.]anondns[.]net, teamtnt[.]red
MD5	b62ce36054a7e024376b98df7911a5a7, 64c3ac5a0f4318f64f438e78a6b42d40, 8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1, a733160e0603207d8328ddb025c43d42, fdf9c2f7221de9f3567fc094d5e759a9, 0bc189bb53c9c92322e7b2fd6ac68bd7, db2fbe4d00b222cab6dd00cdfdd38e31
URL	hxxps[:]//hub[.]docker[.]com/u/nmlm99

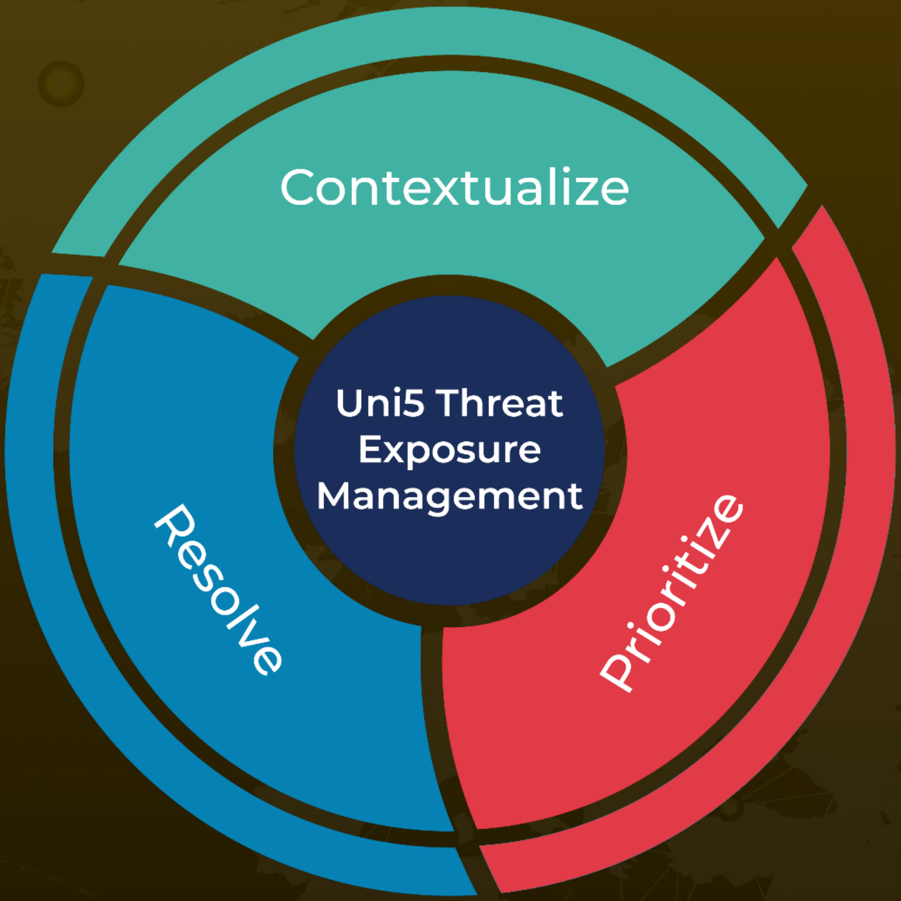
References

https://www.aquasec.com/blog/threat-alert-teamtnts-docker-gatling-gun-campaign/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 28, 2024 • 6:10 AM

More at www.hivepro.com