Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

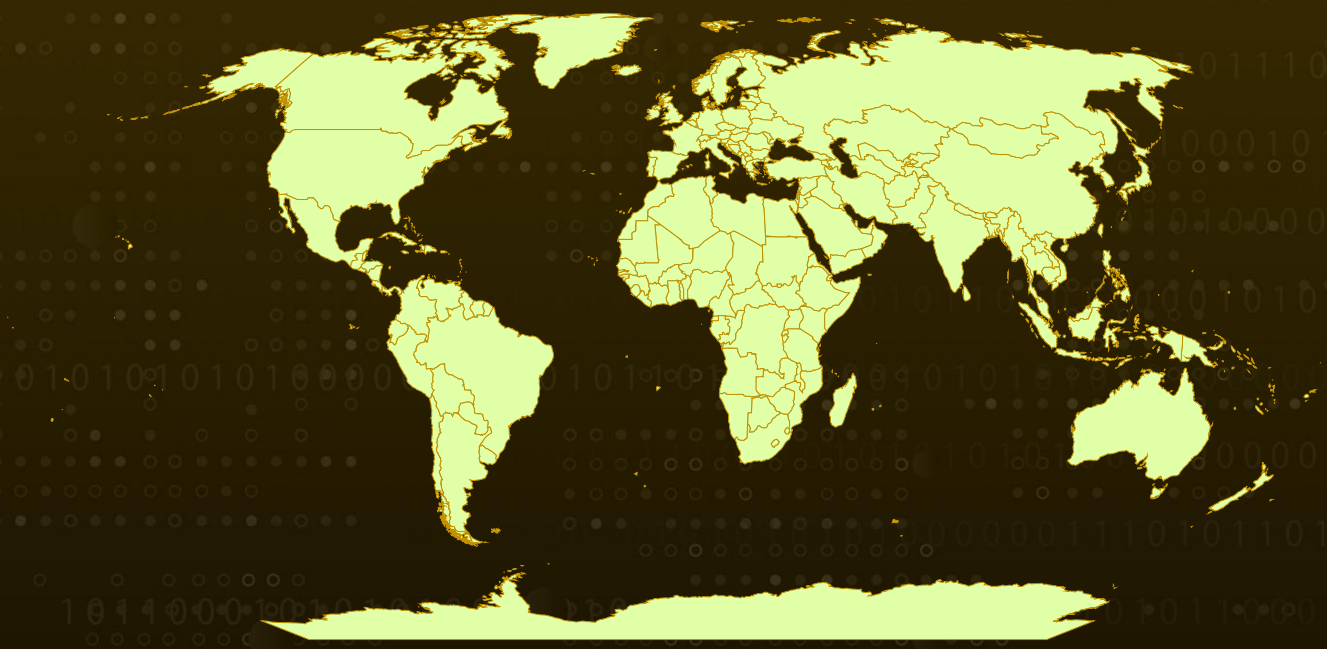
Docker Under Siege: Zombie Containers Fuel Dero Crypto Heist

Date of Publication	Admiralty Code	TA Number
May 28, 2025	A1	TA2025164

Summary

Attack Discovered: 2025
Malware: Dero crypto miner
Targeted Countries: Worldwide
Affected Platform: Windows, Linux
Targeted Industry: Cryptocurrency
Attack: A new Dero cryptocurrency mining campaign is hijacking Docker environments through exposed APIs, turning containers into "zombies" that spread the infection. Using malware disguised as nginx, the attackers automate the creation of malicious containers to mine crypto and scan for more targets. This self-propagating attack compromises resources and expands rapidly, putting any unsecured Docker setup at serious risk.

Attack Regions



Attack Details

#1 A new wave of malicious activity has been observed targeting containerized environments, specifically Docker infrastructures, through a campaign designed to mine Dero cryptocurrency. The attack spreads like a "zombie outbreak," where a single compromised container exploits exposed Docker APIs to both deploy malicious containers and infect existing ones. These compromised containers now turned into "zombies" not only mine cryptocurrency but also seek out and infect other vulnerable systems, creating a self-sustaining cycle of propagation.

#2 This campaign relies on two primary malicious components: a propagation tool disguised as the legitimate nginx web server and a Dero cryptocurrency miner, both written in Golang and compressed using UPX. The "nginx" malware is specifically engineered to maintain persistence and enable further spread, while the "cloud" component acts as the miner. These tools are built for automation, allowing the attack to proceed with minimal human oversight. The use of the name "nginx" helps the malware fly under the radar by masquerading as trusted software, making it harder to detect.

#3 Once deployed, the malware sets up logging activity and checks for the presence of the crypto miner process. If it's not running, the malware automatically restarts it. It then generates random IPv4/16 subnets to search for more exposed Docker APIs, using the port-scanning tool masscan. Once vulnerable targets are found those with Docker's default API port 2375 exposed it attempts to create new containers remotely, installing necessary dependencies and transferring the malicious binaries into them. Persistence is ensured by modifying shell aliases to automatically re-execute the malware on container startup.

#4 The malware specifically targets containers based on Ubuntu 18.04, infecting them and hijacking their resources. It continues to scan and infect other containers, creating an ever-growing network of compromised systems. The Dero miner is embedded with hardcoded configurations, including wallet and node addresses, and uses AES-CTR encryption to hide these details.

#5 Although container-targeted attacks are relatively less frequent than traditional infrastructure breaches, they remain a serious threat especially to organizations using Docker or Kubernetes with misconfigured or publicly exposed APIs. With over 500 publicly exposed Docker APIs detected in April 2025 alone, the risks remain high for unprotected container environments, making monitoring and securing these infrastructures more important than ever.

Recommendations

- **Lock Down Docker APIs:** Never expose the Docker API to the internet without strict authentication. Use firewalls or network policies to limit access.
- **Monitor for Unusual Container Behavior:** Set up alerts for unexpected container launches, resource spikes, or traffic patterns.
- **Restrict Container Privileges:** Use least privilege principles for containers, limiting what they can access and execute.
- **Scan Your Infrastructure:** Proactively check if your APIs or ports (like 2375) are publicly accessible and take them offline if not needed.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0010** Exfiltration	**TA0011** Command and Control	**TA0040** Impact
T1190 Exploit Public-Facing Application	**T1036** Masquerading	**T1036.005** Match Legitimate Resource Name or Location	**T1610** Deploy Container
T1562 Impair Defenses	**T1059** Command and Scripting Interpreter	**T1072** Software Deployment Tools	**T1041** Exfiltration Over C2 Channel

T1571 Non-Standard Port	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1496** Resource Hijacking
T1102 Web Service	**T1552** Unsecured Credentials	**T1552.007** Container API	**T1543** Create or Modify System Process
T1543.005 Container Service			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	094085675570A18A9225399438471CC9, 14E7FB298049A57222254EF0F47464A7
SHA256	BE81A7FB61F9EA26EAF2369988476DD4C952177CE3D3D935AB492B47595AE7E6, E4AA649015B19A3C3350B0D897E23377D0487F9EA265FE94E7161FED09F283CF
File Path	/usr/bin/nginx, /usr/bin/cloud, /var/log/nginx.log, /usr/bin/version.dat
Domain	d[.]windowsupdatesupport[.]link, h[.]wiNdowsupdatesupport[.]link
Dero wallet address	dero1qyy8xjrdjcn2dvr6pwe40jrl3evv9vam6tpx537vux60xxkx6hs7zqgde993y

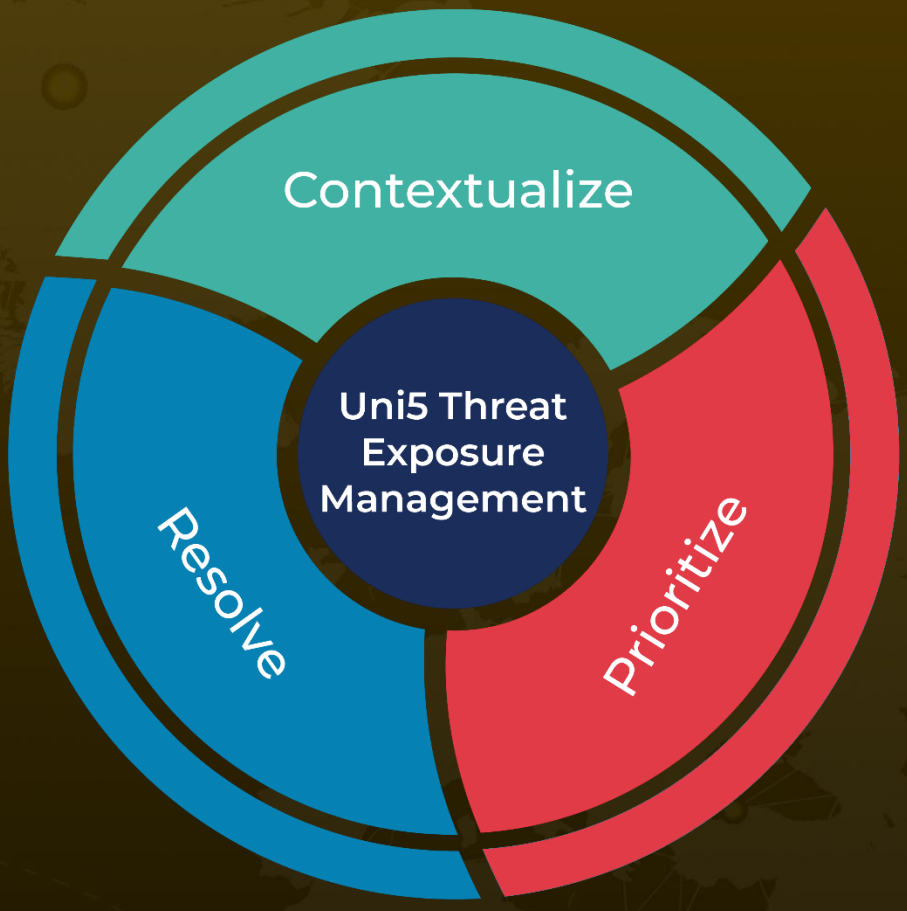
References

https://securelist.com/dero-miner-infects-containers-through-docker-api/116546/

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

May 28, 2025 • 5:50 AM

More at www.hivepro.com