Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

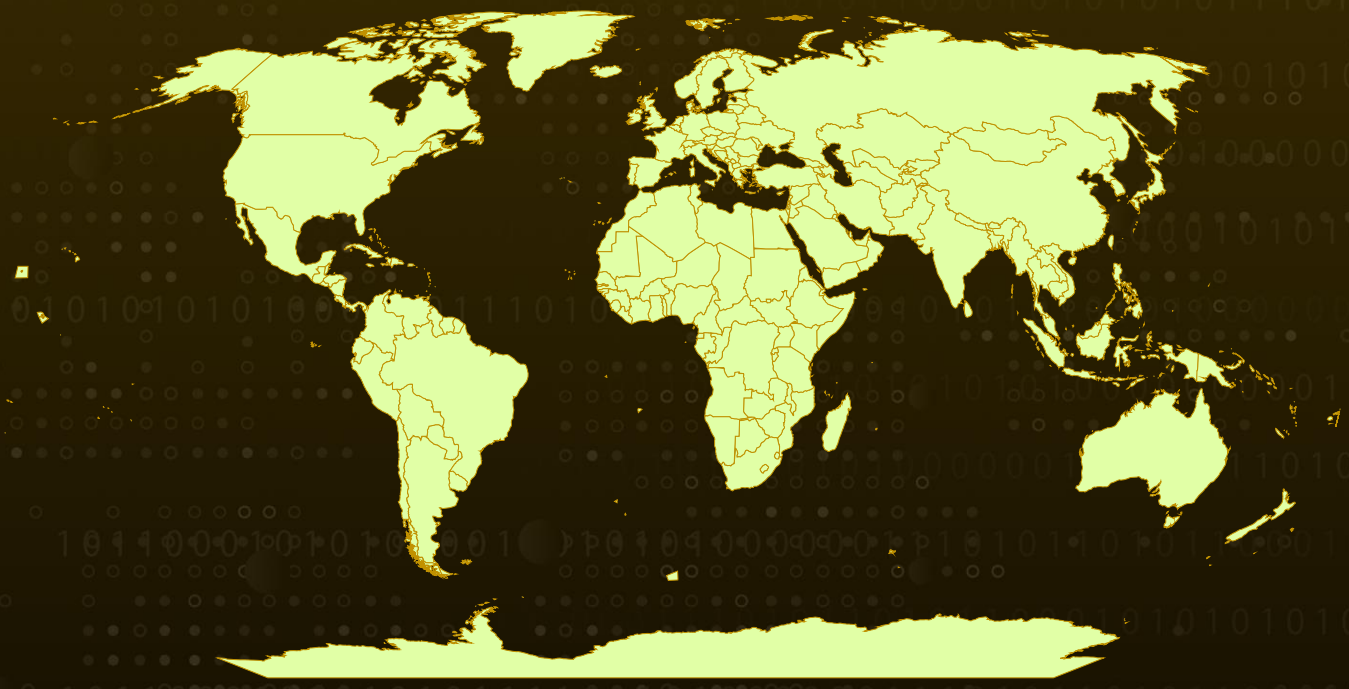
Threat Actors Exploit Docker and Kubernetes for Crypto Mining

Date of Publication	Admiralty Code	TA Number
October 3, 2024	A1	TA2024376

Summary

First Seen: September 2024
Targeted Countries: Worldwide
Malware: XMRig
Affected Platforms: Docker Swarm and Kubernetes
Attack: A new cryptojacking campaign that exploits Docker and Kubernetes environments to mine cryptocurrency by accessing exposed Docker API endpoints without authentication. The attack enables lateral movement within cloud infrastructures, allowing threat actors to compromise multiple systems by leveraging malicious Docker images and scripts. This campaign highlights the urgent need for enhanced security measures in containerized infrastructures to prevent exploitation.

Attack Regions



Attack Details

#1

In recent times, attackers have been increasingly exploiting container orchestration platforms like Docker Swarm and Kubernetes to mine cryptocurrency. A new cryptojacking campaign targets the Docker Engine API and can move laterally to Docker Swarm, Kubernetes, and SSH servers. The campaign begins with the threat actor accessing exposed Docker API endpoints without authentication, a common vulnerability in cloud environments.

#2

Threat actors utilize tools like masscan and zgrab to identify these vulnerable endpoints across the internet. Once a target is found, the malware leverages the Docker API to create an Alpine container, which mounts the host's file system and executes a malicious shell command to download an initialization script that kicks off the infection process.

#3

One of the key features of this attack is its ability to enable lateral movement within cloud infrastructures, allowing it to spread from one compromised container to others running Docker or Kubernetes. The threat actor operates a command and control (C2) server that hosts malicious payloads and manages infected hosts through a controlled Docker Swarm cluster. The campaign involves using Docker Hub to distribute malicious images, specifically from a user account named nmlmweb3, which remains active and has several repositories.

#4

The attack initiates with a command that retrieves an initialization script (init.sh) from a remote server. This script prepares the container for further exploitation by ensuring essential data transfer tools are installed and then downloading a cryptocurrency miner (XMRig) to execute within the container. The script employs dynamic linker hijacking techniques to conceal the mining process from system monitoring tools by modifying system files to hide the miner's presence. This multi-faceted approach underscores the need for robust security measures in containerized environments.

#5

The malware employs various strategies for lateral movement, including targeting Kubernetes environments by scanning local networks for open Kubelet APIs (port 10250) and attempting to execute commands within discovered pods. It also scans for Docker Engine ports and uses found endpoints to deploy additional malicious containers. Furthermore, the malware looks for SSH servers within the local network and attempts to exploit them for further access.

Recommendations

Secure API Endpoints: Ensure that all Docker and Kubernetes API endpoints are secured with strong authentication mechanisms. Disable unauthenticated access to the Docker Engine API and configure Kubernetes to require authentication for all requests. Use role-based access control (RBAC) to limit permissions based on user roles.

Regularly Update and Patch Systems: Keep Docker, Kubernetes, and all related software up to date with the latest security patches. Regularly review and update container images to ensure they do not contain known vulnerabilities. Utilize automated tools to scan for outdated components and apply updates promptly.

Implement Network Segmentation: Segment your network to limit the exposure of sensitive systems. Use firewalls to restrict access to Docker and Kubernetes APIs from untrusted networks. Implement network policies within Kubernetes to control traffic flow between pods and limit lateral movement.

Monitor for Anomalous Activity: Deploy monitoring solutions that can detect unusual behavior within your containerized environments. Set up alerts for suspicious activities, such as unexpected container creation or unusual resource consumption patterns indicative of cryptojacking attempts.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
TA0011 Command and Control	TA0008 Lateral Movement	TA0040 Impact	TA0003 Persistence
T1021.004 SSH	T1021 Remote Services	T1574 Hijack Execution Flow	T1059 Command and Scripting Interpreter
T1027.004 Compile After Delivery	T1027 Obfuscated Files or Information	T1496 Resource Hijacking	T1562.004 Disable or Modify System Firewall

T1562 Impair Defenses	T1574.006 Dynamic Linker Hijacking	T1552.007 Container API	T1552 Unsecured Credentials
T1609 Container Administration Command	T1613 Container and Resource Discovery	T1525 Implant Internal Image	T1564.012 File/Path Exclusions
T1564 Hide Artifacts	T1078 Valid Accounts		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9d02707b895728b4229abd863aa6967d67cd8ce302b30dbcd946959e719842ad, 700635abe402248ccf3ca339195b53701d989adb6e34c014b92909a2a1d5a0ff, 2514e5233c512803eff99d4e16821ecc3b80cd5983e743fb25aa1bcc17c77c79, 6157a74926cfd66b959d036b1725a63c704b76af33f59591c15fbf85917f76fa, 6f426065e502e40da89bbc8295e9ca039f28b50e531b33293cee1928fd971936, 78ebc26741fc6bba0781c6743c0a3d3d296613cc8a2bce56ef46d9bf603c7264, e6985878b938bd1fba3e9ddf097ba1419ff6d77c3026abdd621504f5c4186441, d99bd3a62188213894684d8f9b4f39dbf1453cc7707bac7f7b8f484d113534b0, 505237e566b9e8f4a83edbe45986bbe0e893c1ca4c5837c97c6c4700cfa0930a, e4c4400a4317a193f49c0c53888ec2f27e20b276c2e6ee1a5fd6eacf3f2a0214, c5391314ce789ff28195858a126c8a10a4f9216e8bd1a8ef71d11c85c4f5175c, 0af1b8cd042b6e2972c8ef43d98c0a0642047ec89493d315909629bcf185dffd

TYPE	VALUE
Domains	solscan[.]live, x[.]solscan[.]live
IPv4	164[.]68[.]106[.]96
URLs	hxxp[://]192[.]155[.]94[.]199/sh/xmr[.]sh[.]sh, hxxp[://]45[.]9[.]148[.]35/aws, hxxp[://]solscan[.]live/aws[.]sh, hxxp[://]solscan[.]live/bin/64bit/xmrig, hxxp[://]solscan[.]live/bin/pnscan_1[.]12+git20180612[.]orig[.]tar[.]gz, hxxp[://]solscan[.]live/bin/xmr/x86_64, hxxp[://]solscan[.]live/bin/xmrig, hxxp[://]solscan[.]live/data/docker[.]container[.]local[.]spread[.]txt, hxxp[://]solscan[.]live/input/kube_in[.]php?target=<IP Address>, hxxp[://]solscan[.]live/scan_threads[.]dat, hxxp[://]solscan[.]live/sh/init[.]sh, hxxp[://]solscan[.]live/sh/kube[.]lateral[.]sh, hxxp[://]solscan[.]live/sh/search[.]sh, hxxp[://]solscan[.]live/sh/setup_xmr[.]sh, hxxp[://]solscan[.]live/sh/spread_docker_local[.]sh, hxxp[://]solscan[.]live/sh/spread_kube_loop[.]sh, hxxp[://]solscan[.]live/sh/spread_ssh[.]sh, hxxp[://]solscan[.]live/sh/xmr[.]sh[.]sh, hxxp[://]solscan[.]live/so/xmrig[.]so, hxxp[://]solscan[.]live/up/kube_in[.]php?target=<IP Address>, hxxp[://]solscan[.]live/upload[.]php,

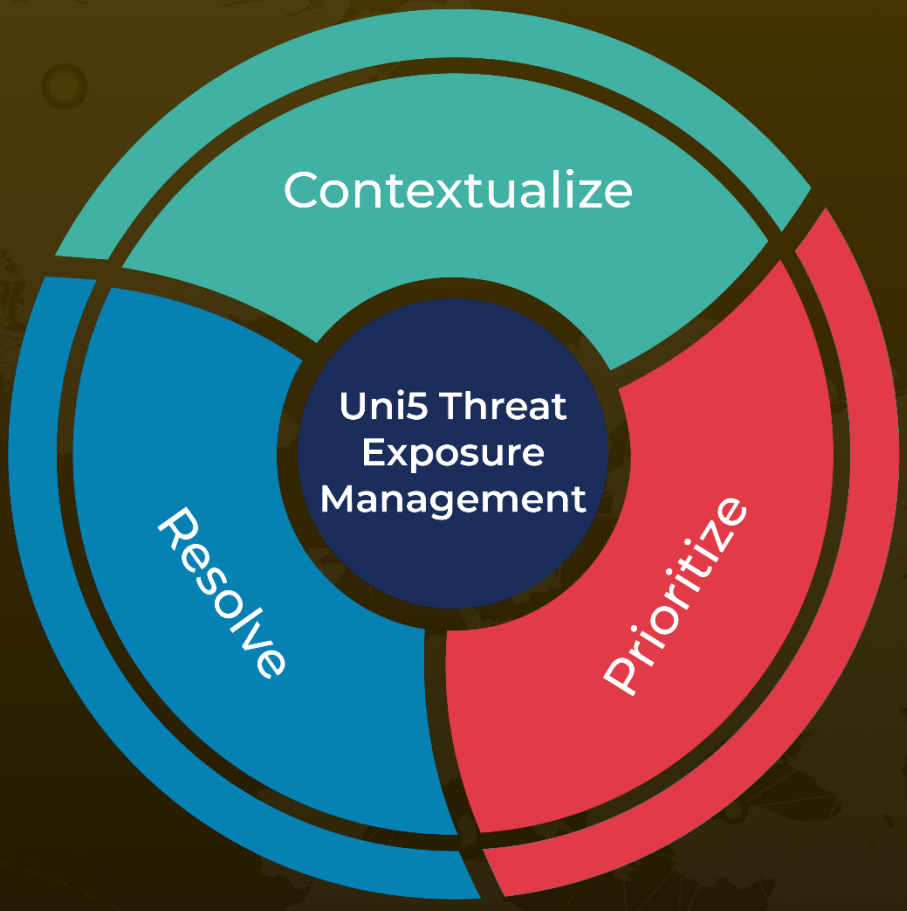
References

https://securitylabs.datadoghq.com/articles/threat-actors-leveraging-docker-swarm-kubernetes-mine-cryptocurrency/

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 3, 2024 • 5:30 AM

More at www.hivepro.com