Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

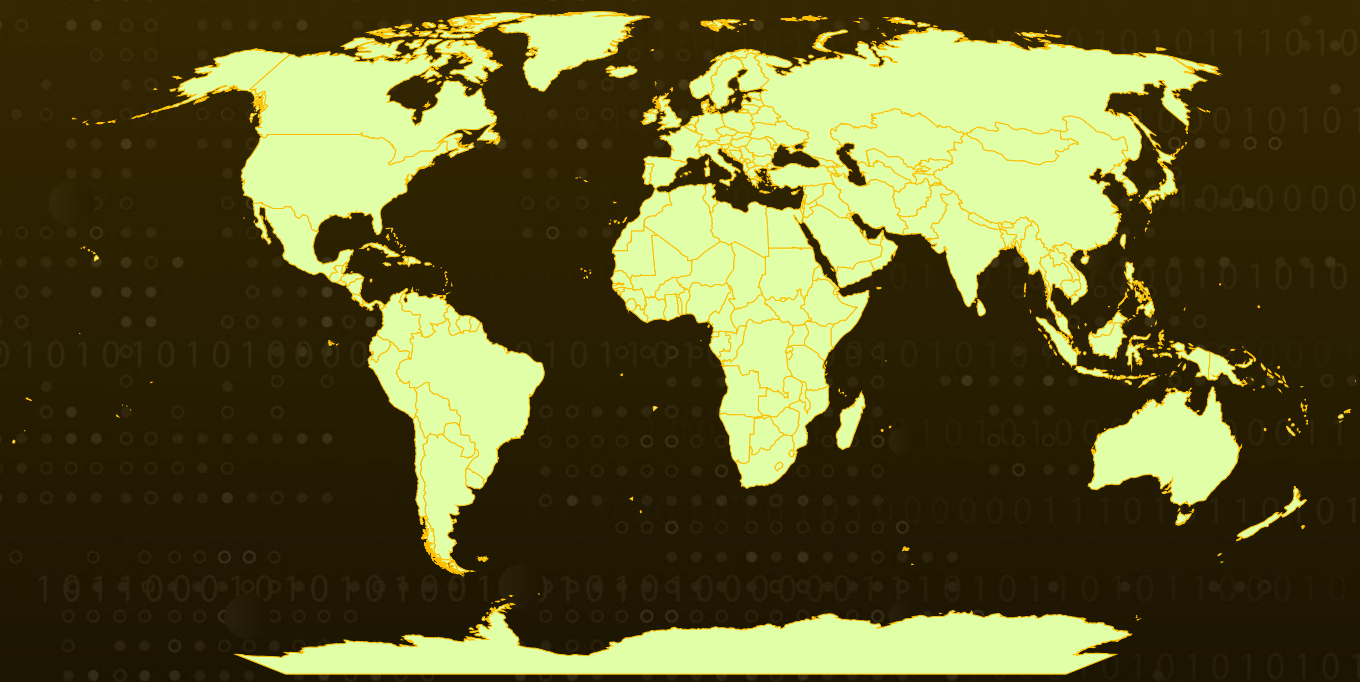
Exposed Docker APIs Fuel Illicit Cryptomining Surge

Date of Publication	Admiralty Code	TA Number
October 23, 2024	A1	TA2024407

Summary

Attack Discovered: 2024
Targeted Countries: Worldwide
Malware: SRBMiner
Attack: Threat actors have been observed targeting Docker remote API servers to install the SRBMiner cryptocurrency miner. Utilizing the gRPC protocol over h2c, they effectively bypassed security defenses to conduct their cryptomining operations on the Docker host. The attackers obtained the miner from GitHub and swiftly executed it, directing the mining process to their own cryptocurrency wallet and public IP address.

Attack Regions



Attack Details

#1 A recent cyberattack has targeted Docker remote API servers, exploiting their vulnerabilities for cryptomining purposes. This poses a considerable security threat when these servers are inadequately configured and publicly accessible. Docker’s remote API provides developers the ability to manage containers, images, and volumes remotely; however, this convenience can be leveraged by malicious actors if proper safeguards are not implemented.

#2 In this particular instance, the attacker utilized the gRPC protocol over h2c, effectively bypassing conventional security measures to install the SRBMiner cryptominer on the Docker host, focusing on mining XRP, a cryptocurrency created by Ripple Labs.

#3 The attacker's initial step involves probing the Docker API to determine its status and version. Following this reconnaissance, they request an upgrade to the gRPC/h2c protocol, allowing them to access various gRPC methods that support essential Docker operations, such as health checks, file synchronization, authentication, secrets management, and SSH forwarding. After successfully executing the protocol upgrade, the attacker sends a gRPC request to create a Docker image using a specific Dockerfile named Dockerfile.srb, which is built upon the legitimate debian:bookworm-slim image.

#4 Once this stage is complete, the adversary downloads the SRBMiner from GitHub, and installs it into the /usr/sbin directory, and activates the mining operation. They provide their cryptocurrency wallet address along with the cryptominer's public IP address to facilitate the illicit activity. This sequence of actions is designed to disrupt the integrity and security of Docker-based environments.

#5 While containerization platforms such as Docker are vital to contemporary application development, their security is often compromised if not effectively protected. Cybercriminals are adept at exploiting remote management APIs like the gRPC protocol to engage in unauthorized cryptocurrency mining. This incident serves as a stark reminder of the imperative to enhance security protocols and protect these vital infrastructure components.

Recommendations

Regularly Update Docker: Ensure that Docker and all its associated components are consistently updated to safeguard against known vulnerabilities. Regular updates help mitigate potential security risks and enhance system stability. Additionally, ensure that containers and APIs are properly configured to minimize the risk of exploitative attacks.

Restrict Network Access: To enhance the security of Docker API servers, restrict access by configuring firewalls to permit only trusted IP addresses. Additionally, ensure that running containers do not operate with root privileges; instead, run them as dedicated application users. This practice limits the potential damage in the event of a compromise and promotes better security hygiene within your containerized environment.

Monitor and Log Activity: Implement logging for API access and actively monitor these logs for any suspicious activities. Utilize advanced tools capable of analyzing logs for anomalies, which can alert administrators to potential threats in real time. Conduct regular security audits to assess the integrity of containers and images, ensuring that any suspicious or unauthorized elements are promptly identified and addressed. This proactive approach to monitoring and logging is vital for maintaining a secure Docker environment.

Limit Access to the Docker Daemon: Avoid exposing the Docker socket (/var/run/docker.sock) to unauthorized users or containers. This socket provides root access to the host system and should not be shared. Disable TCP access to the Docker daemon unless absolutely necessary. If TCP is required, use TLS for secure communication.

Use Non-Root Users: Configure your containers to run as non-root users to limit potential damage from a compromised container. This can be done in your Dockerfile or at runtime using the -u option.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access
TA0007 Discovery	TA0011 Command and Control	TA0040 Impact	T1190 Exploit Public-Facing Application

T1133 External Remote Services	**T1610** Deploy Container	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1496** Resource Hijacking	**T1016** System Network Configuration Discovery	**T1016.001** Internet Connection Discovery
T1592 Gather Victim Host Information	**T1592.002** Software	**T1552** Unsecured Credentials	**T1552.007** Container API

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0d4eb69b551cb538a9a4c46f7b57906a47bcabb8ef8a5d245584fbba09fc5084
URL	hxxps[:]//github[.]com/doktor83/SRBMiner-Multi/releases/download/2.5.8/SRBMiner-Multi-2-5-8-Linux[.]tar[.]g
IPv4:Port	167[.]71[.]194[.]227:3333
IPv4	59[.]93[.]45[.]16

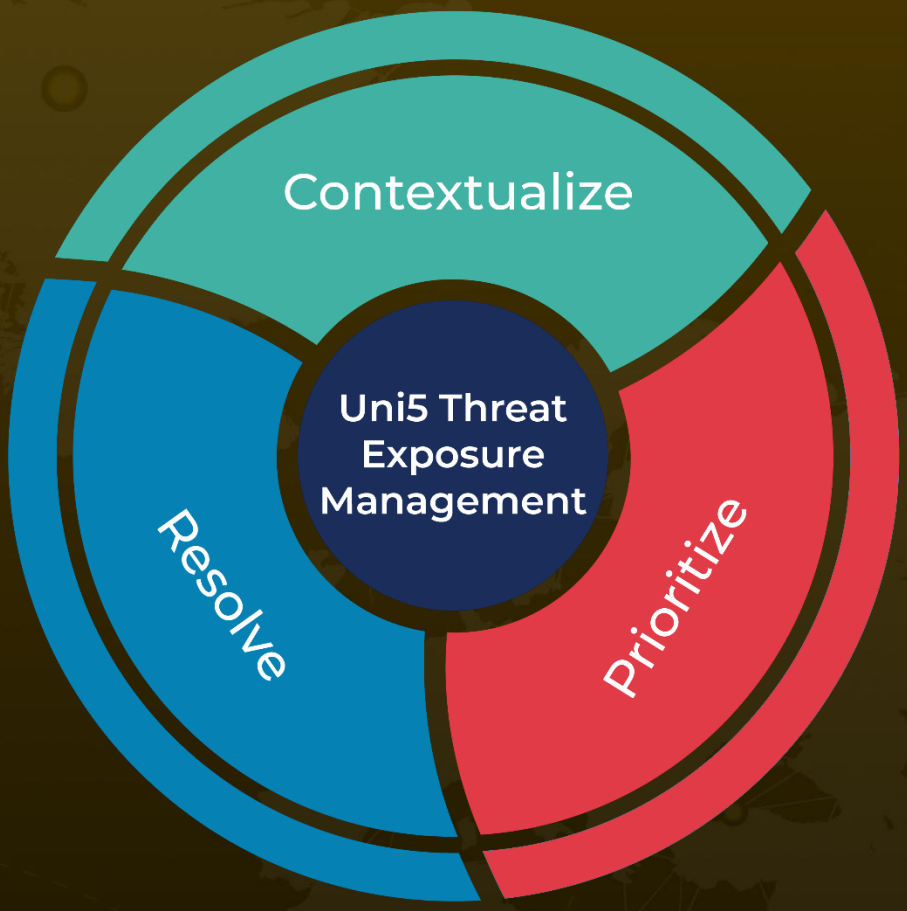
References

https://www.trendmicro.com/en_us/research/24/j/using-grpc-http-2-for-cryptominer-deployment.html

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 23, 2024 • 6:00 AM

More at www.hivepro.com