Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

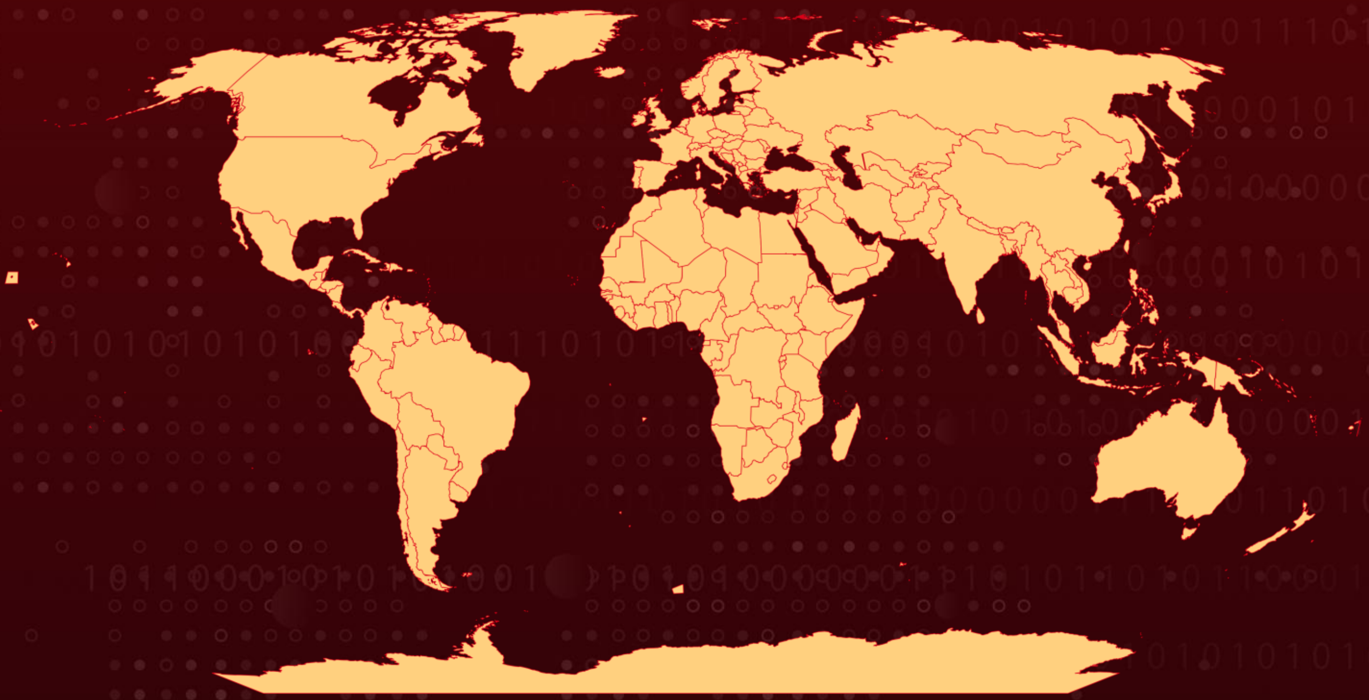
New Attacks Target Misconfigured Apache Applications with Monero Miner

Date of Publication	Admiralty Code	TA Number
January 16, 2024	A1	TA2024016

Summary

Attack Discovered: 2023
Attack Region: Worldwide
Malware: Monero cryptominer
Attack: A recently identified attack exploits misconfigurations in Apache Hadoop and Flink to deploy cryptocurrency miners within targeted environments. This attack stands out due to the attacker's utilization of packers and rootkits to conceal the malware, adding an extra layer of complexity and stealth to the operation.

Attack Regions



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

Attack Details

#1 The attack is specifically aimed at Apache Flink, an open-source unified stream-processing and batch-processing framework, and Apache Hadoop, an open-source framework for distributed storage and processing. The attacker exploits system misconfigurations to achieve code execution and ultimately deploys a Monero cryptocurrency miner. Noteworthy is the use of packers and rootkits in the attack to stealthy deploy the cryptocurrency mining malware within the targeted environments.

#2 In one of the attacks directed at Apache Hadoop, the initial access point exploits a misconfiguration in the ResourceManager of YARN. The attacker commences exploitation by submitting an unauthenticated request to deploy a new application. Subsequently, through another POST request, they activate the newly created app containing malicious shell commands.

#3 The executed command has a specific objective: to clear the /tmp directory, retrieve a file named "dca" from a remote server, and execute it. After this operation, the attacker clears the /tmp directory once again. The executed payload is a compressed ELF binary, acting as a downloader responsible for fetching two rootkits and a Monero cryptocurrency miner binary. To maintain persistence, a cron job is created to download and execute a shell script that deploys the "dca" binary.

#4 Upon delving into the threat actor's infrastructure, it was uncovered that the staging server used to retrieve the downloader was registered on October 31, 2023. An agent-based runtime solution assumes a pivotal role in safeguarding customers from diverse threats, encompassing cryptominers, rootkits, obfuscated binaries, and container drift. This is accomplished through the detection of suspicious behavior within their infrastructure.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

- **Strict Authentication Mechanisms:** Enforce robust authentication mechanisms to prevent unauthorized access to API endpoints and enable positive security model to critical API access.

- **Configuration Review:** Conduct a thorough review of application configurations to identify and rectify any misconfigurations in order to mitigate similar attacks.

- **Zero Trust Network Access (ZTNA):** Implement ZTNA solutions to ensure that users and devices are authenticated and authorized before accessing applications or data, regardless of their location.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0040 Impact	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1059.004 Unix Shell	T1053 Scheduled Task/Job	T1053.003 Cron	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1027.008 Stripped Payloads	T1027.009 Embedded Payloads	T1222 File and Directory Permissions Modification
T1222.002 Linux and Mac File and Directory Permissions Modification	T1014 Rootkit	T1082 System Information Discovery	T1496 Resource Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
IP	20[.]150[.]209[.]84, 185[.]196[.]9[.]181, 185[.]196[.]9[.]190, 185[.]196[.]9[.]200, 185[.]196[.]9[.]5, 185[.]196[.]9[.]7, 185[.]196[.]9[.]8
Domain	ns1[.]disponibletogether[.]com
MD5	58794e43c039fe20281bf0777721c8ce, 94e0f679758facf683a217774e29c2b2, 901ac649b47e0261d88f568f02c90412, cebadcafee4ed6a69c64ab08496163d7, 0a100f6a07e7fd611553ef7c42f37f5a, 38d898459a3f530e2db083e1bb1e1524

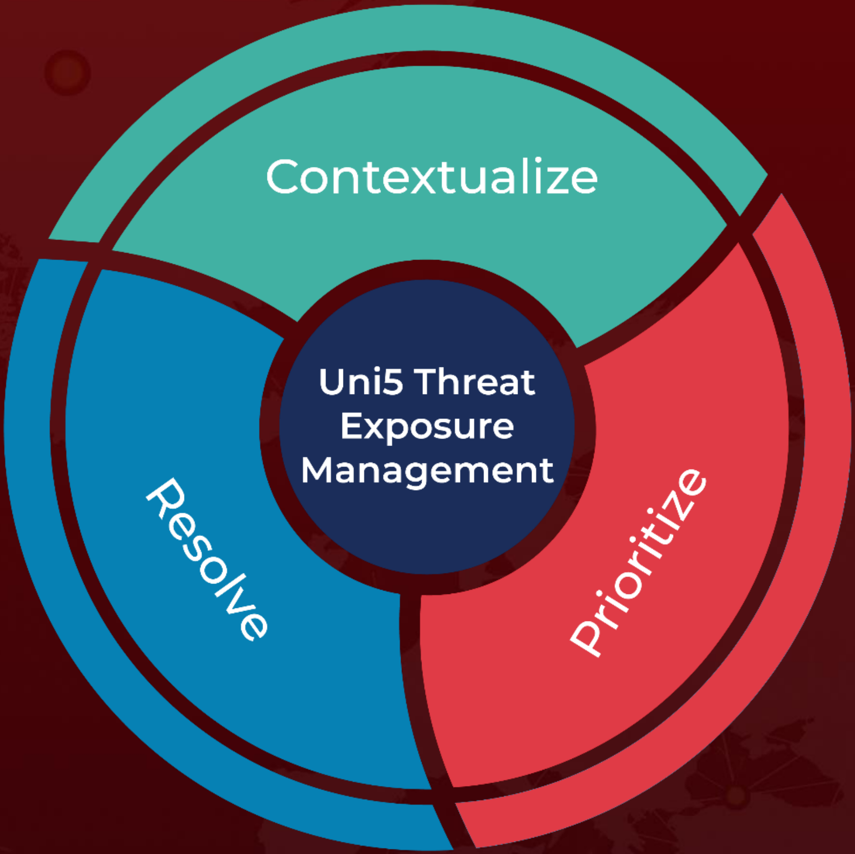
References

https://blog.aquasec.com/threat-alert-apache-applications-targeted-by-stealthy-attacker

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

January 16, 2024 • 4:15 AM

More at www.hivepro.com