Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

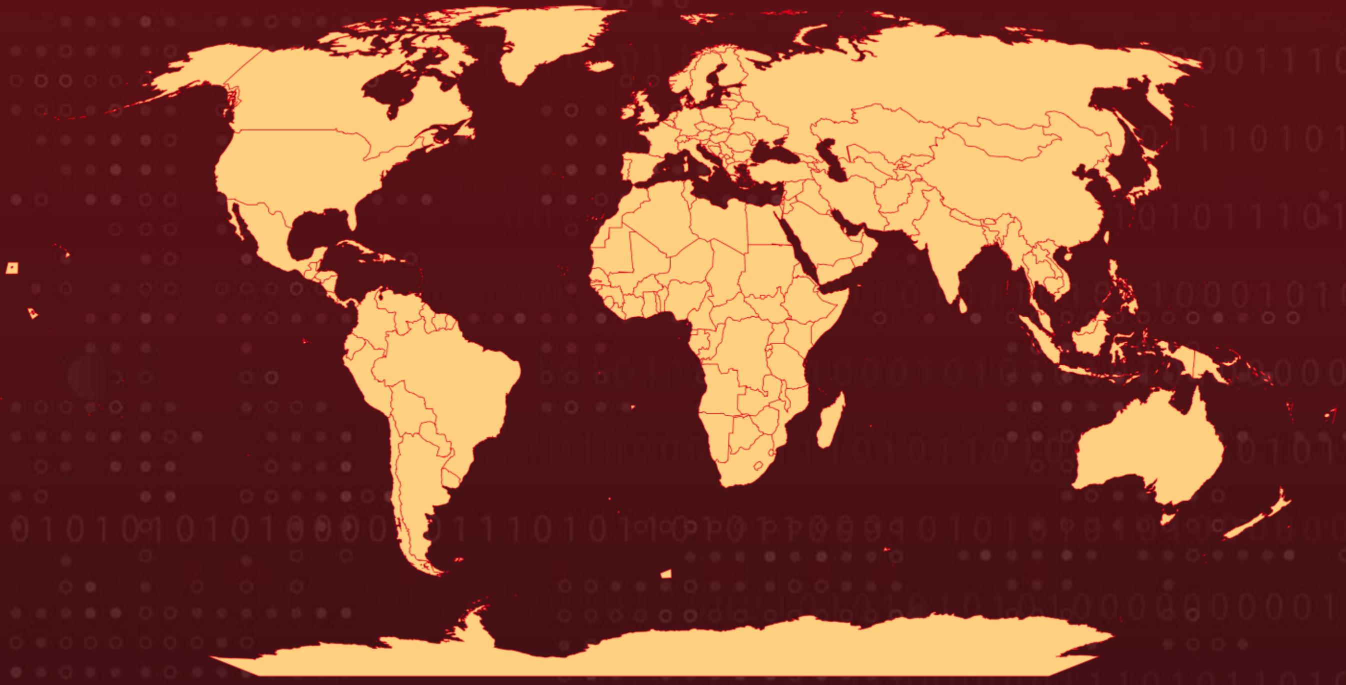
Muhstik Botnet Exploits Apache RocketMQ Flaw in Latest Operations

Date of Publication	Admiralty Code	TA Number
June 7, 2024	A1	TA2024221

Summary

Attack Discovered: June 2024
Attack Region: Worldwide
Malware: Muhstik
Attack: A new campaign of Muhstik malware has been discovered targeting message queuing service applications, specifically the Apache RocketMQ platform. The attackers exploited a known vulnerability in the platform to download the Muhstik malware onto compromised instances. By doing so, they were able to co-opt susceptible servers and expand the scale of their attack.

Attack Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	RocketMQ	✗	✓	✓

Attack Details

#1 The Muhstik botnet has been exploiting a vulnerability in Apache RocketMQ to commandeer vulnerable servers, leveraging its capabilities to propagate further. RocketMQ, esteemed for its performance and scalability, was discovered to have a remote code execution vulnerability (CVE-2023-33246) affecting versions 5.1.0 and below.

#2 Attackers capitalize on this vulnerability by accessing RocketMQ elements without permission checks, enabling them to execute commands through the update configuration function. This flaw empowers them to operate with the same privileges as RocketMQ users, facilitating the download of the Muhstik malware.

#3 Muhstik, a notorious threat targeting IoT devices and Linux-based servers, is infamous for its cryptocurrency mining and DDoS attacks. Part of the Kaiten family, it operates via IRC channels, sharing similarities with the Mirai malware.

#4 The attack sequence involves exploiting RocketMQ's broker configuration to execute malicious commands. By updating the `filterServerNums` variable, attackers trigger the execution of a shell command, enabling them to download the shell script. This script retrieves multiple binaries, including the Muhstik malware.

#5 Upon execution on a compromised machine, Muhstik employs persistence techniques, manipulating system files like `inittab` and employing DNS requests to communicate with malicious domains, establishing a command-and-control (C2) server for communication with compromised machines.

#6 The malware checks for network tools and endeavors to access other machines via SSH, indicating its sophisticated evasion techniques. In previous campaigns, cryptomining activity was detected following the malware's execution, indicating that the attackers aim to infect more machines for cryptocurrency mining. This highlights the complex and multifaceted nature of contemporary cyber threats.

Recommendations

Update: It is strongly advised to upgrade to version 5.1.1 or higher when utilizing RocketMQ 5.x, or version 4.9.6 or higher when utilizing RocketMQ 4.x. This ensures access to the latest security patches and reduces the risk of exploitation from known vulnerabilities.

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.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control	TA0040 Impact
T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1059.004 Unix Shell	T1037 Boot or Logon Initialization Scripts
T1037.005 Startup Items	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information

T1027.002 Software Packing	**T1620** Reflective Code Loading	**T1036** Masquerading	**T1036.005** Match Legitimate Name or Location
T1082 System Information Discovery	**T1021** Remote Services	**T1021.004** SSH	**T1071** Application Layer Protocol
T1071.004 DNS	**T1496** Resource Hijacking	**T1498** Network Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	94[.]224[.]82[.]40, 91[.]148[.]224[.]34, 89[.]36[.]76[.]42, 89[.]36[.]76[.]38, 51[.]79[.]19[.]53, 54[.]36[.]49[.]151, 51[.]79[.]19[.]53, 139[.]159[.]192[.]50, 194[.]59[.]165[.]52, 138[.]197[.]78[.]18, 91[.]200[.]43[.]22, 139[.]180[.]185[.]248, 161[.]35[.]219[.]184
Domain	p[.]de-zahlung[.]eu, p[.]shadow-mods[.]net, p[.]findmeatthe[.]top, p[.]deutschland-zahlung[.]eu
SHA256	9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572, 1f9cda58cea6c8dd07879df3e985499b18523747482e8f7acd6b4b3a82116957, 176c57e3fa7da2fb2afcd18242b79e5881c2244f5ab836897d4846885f1bd993, a7bf3c031ab66265ce724fc26c8f7565442a098b06b01ea8871f13179d168713, 6730eb04edf45d590939d7ba36ca0d4f1d2f28a2692151e3c631e9f2d3612893, 86947b00a3d61b82b6f752876404953ff3c39952f2b261988baf63fbbbd6d6ae

Patch Link

https://rocketmq.apache.org/download

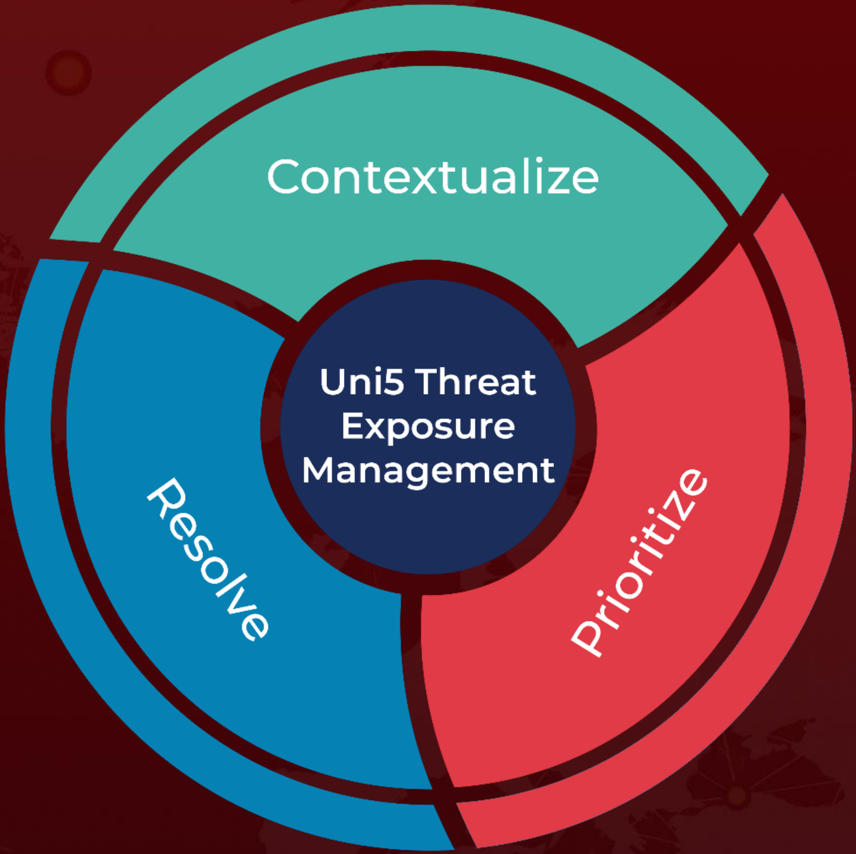
References

https://www.aquasec.com/blog/muhstik-malware-targets-message-queuing-services-applications/

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

June 7, 2024 • 6:30 AM

More at www.hivepro.com