Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

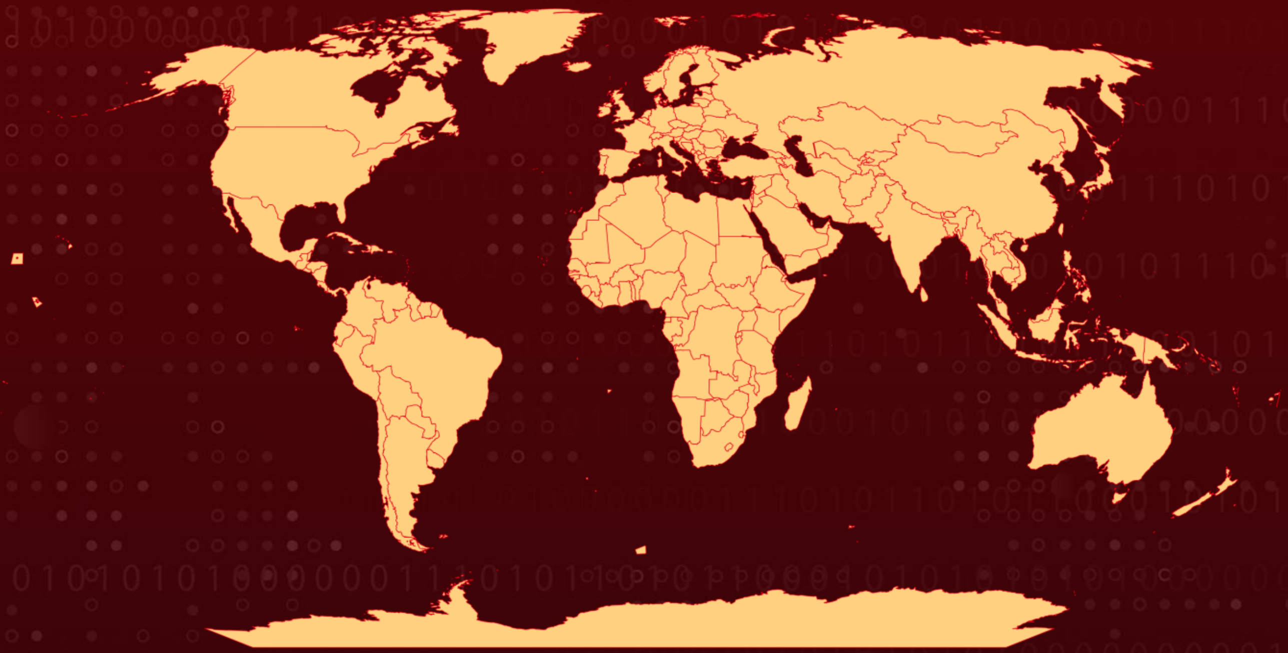
Misconfigured Servers Targeted with New Golang Malwares

Date of Publication	Admiralty Code	TA Number
March 7, 2024	A1	TA2024091

Summary

Attack Discovered: March 2024
Attack Region: Worldwide
Attack: In a newly observed malware campaign, threat actors are targeting misconfigured and vulnerable servers running Apache Hadoop YARN, Docker, Atlassian Confluence, and Redis services. The campaign aims to deliver a cryptocurrency miner and establish a reverse shell for persistent remote access. The attackers utilize new Golang-based malware, which automates the discovery and compromise of these vulnerable hosts.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓

Attack Details

#1 Hackers are using new Golang-based malware in campaign called "Spinning YARN" which aims to deliver a cryptocurrency miner, using various attack vectors to automatically find and compromise misconfigured systems running Apache Hadoop YARN, Docker, Confluence, or Redis. This operation involves hiding malicious processes with user-mode rootkits and exploiting common misconfigurations and vulnerabilities to execute RCE attacks and infect new hosts.

#2 In one attack campaign observed on a Docker Engine API honeypot, attackers created a bind mount for the server's root directory using a Docker command, allowing them to execute base64-encoded shell commands via an executable called vurl. They then established a TCP connection to their C2 infrastructure and retrieved the first-stage payload, resolving to a malicious IP address.

#3 To add more payloads, the cronb.sh script sets the C2 domain and URL, it ensures the chattr function is available and then renames it to zzhcht. The attacker also utilized a comprehensive shell script named "ar.sh." This script, also fetches the Golang-based reverse shell Platypus. Additionally, "ar.sh" adds an SSH key, enabling continued access for the attacker to the compromised machine. It also brings another Golang payload named "fkoths“, tasked with the eradication of Docker images from the Ubuntu or Alpine repositories, effectively eliminating any traces of the initial access.

#4 In order to download and persist further binary payloads on the host, the malware runs a second shell script. The script establishes a directory structure and defines the C2 domain. To perform reconnaissance in the target system and move laterally and further spread the injection, this shell script is in charge of bringing multiple Golang ELF binaries that pose as .sh files and are intended to target services in the Docker Engine API, Apache Hadoop YARN, Confluence, and Redis servers.

#5 It's noteworthy that the shell script payloads employed in this campaign exhibit similarities to those utilized in previous cloud-based attacks, including those attributed to WatchDog, TeamTNT, and the Kiss a Dog campaign. Moreover, the utilization of multiple binaries and shell scripts compounds the complexity of the attack, underscoring the need for robust security measures.

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.

Monitor and Audit Logs: Enable logging for servers and applications and regularly monitor and review logs for signs of unauthorized access or suspicious activities. Implement automated alerts for unusual or malicious events.

Apply Patch: Install the security patch provided by Atlassian to address the CVE-2022-26134 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Configuration Review: Ensure that systems are not operating with default configurations and are instead configured with a focus on security. Conduct continuous configuration reviews and audit checks to identify and rectify configuration gaps.

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
T1496 Resource Hijacking	T1210 Exploitation of Remote Services	T1053 Scheduled Task/Job	T1053.003 Cron
T1036 Masquerading	T1036.008 Masquerade File Type	T1059 Command and Scripting Interpreter	T1059.004 Unix Shell

T1027 Obfuscated Files or Information	**T1525** Implant Internal Image	**T1105** Ingress Tool Transfer	**T1046** Network Service Discovery
T1140 Deobfuscate/Decode Files or Information	**T1570** Lateral Tool Transfer	**T1070** Indicator Removal	**T1562** Impair Defenses
T1562.003 Impair Command History Logging	**T1014** Rootkit	**T1190** Exploit Public-Facing Application	**T1098** Account Manipulation
T1098.004 SSH Authorized Keys			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d4508f8e722f2f3ddd49023e7689d8c65389f65c871ef12e3a6635bbaeb7eb6e, 64d8f887e33781bb814eaefa98dd64368da9a8d38bd9da4a76f04a23b6eb9de5, afddbaec28b040bcbaa13decdc03c1b994d57de244befbdf2de9fe975cae50c4, 251501255693122e818cadc28ced1ddb0e6bf4a720fd36dbb39bc7dedface8e5, 0c7579294124ddc32775d7cf6b28af21b908123e9ea6ec2d6af01a948caf8b87, 0c3fe24490cc86e332095ef66fe455d17f859e070cb41cbe67d2a9efe93d7ce5, d45aca9ee44e1e510e951033f7ac72c137fc90129a7d5cd383296b6bd1e3ddb5, e71975a72f93b134476c8183051fee827ea509b4e888e19d551a8ced6087e15c, 5a816806784f9ae4cb1564a3e07e5b5ef0aa3d568bd3d2af9bc1a0937841d174
Paths	/usr/bin/vurl, /etc/cron.d/zzh, /bin/zzhcht, /usr/bin/zzhcht, /var/tmp/.11/sshd, /var/tmp/.11/bioset,

TYPE	VALUE
Paths	/var/tmp/.11/..lph, /var/tmp/.dog, /etc/systemd/system/sshm.service, /etc/systemd/system/sshb.service, /etc/systemd/system/zzhr.service, /etc/systemd/system/zzhd.service, /etc/systemd/system/zzhw.service, /etc/systemd/system/zzhh.service, /etc/…/.ice-unix/, /etc/…/.ice-unix/.watch, /etc/.httpd/…/httpd, /var/.httpd/…../httpd
IP	47[.]96[.]69[.]71, 107[.]189[.]31[.]172, 209[.]141[.]37[.]110
URLs	http[:]//b[.]9-9-8[.]com, http[:]//b[.]9-9-8[.]com/brysj/cronb.sh, http[:]//b[.]9-9-8[.]com/brysj/d/ar.sh, http[:]//b[.]9-9-8[.]com/brysj/d/c.sh, http[:]//b[.]9-9-8[.]com/brysj/d/h.sh, http[:]//b[.]9-9-8[.]com/brysj/d/d.sh, http[:]//b[.]9-9-8[.]com/brysj/d/enbio.tar

Patch Link

https://jira.atlassian.com/browse/CONFSERVER-79016

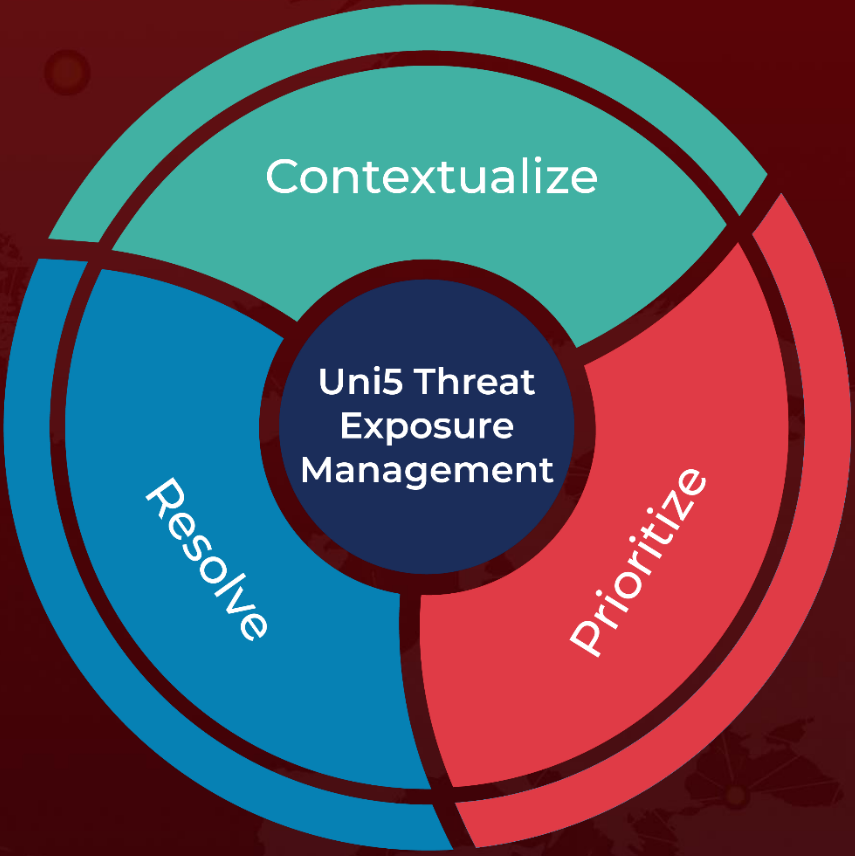
References

https://www.cadosecurity.com/spinning-yarn-a-new-linux-malware-campaign-targets-docker-apache-hadoop-redis-and-confluence/

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

March 7, 2024 • 7:30 AM

More at www.hivepro.com