Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

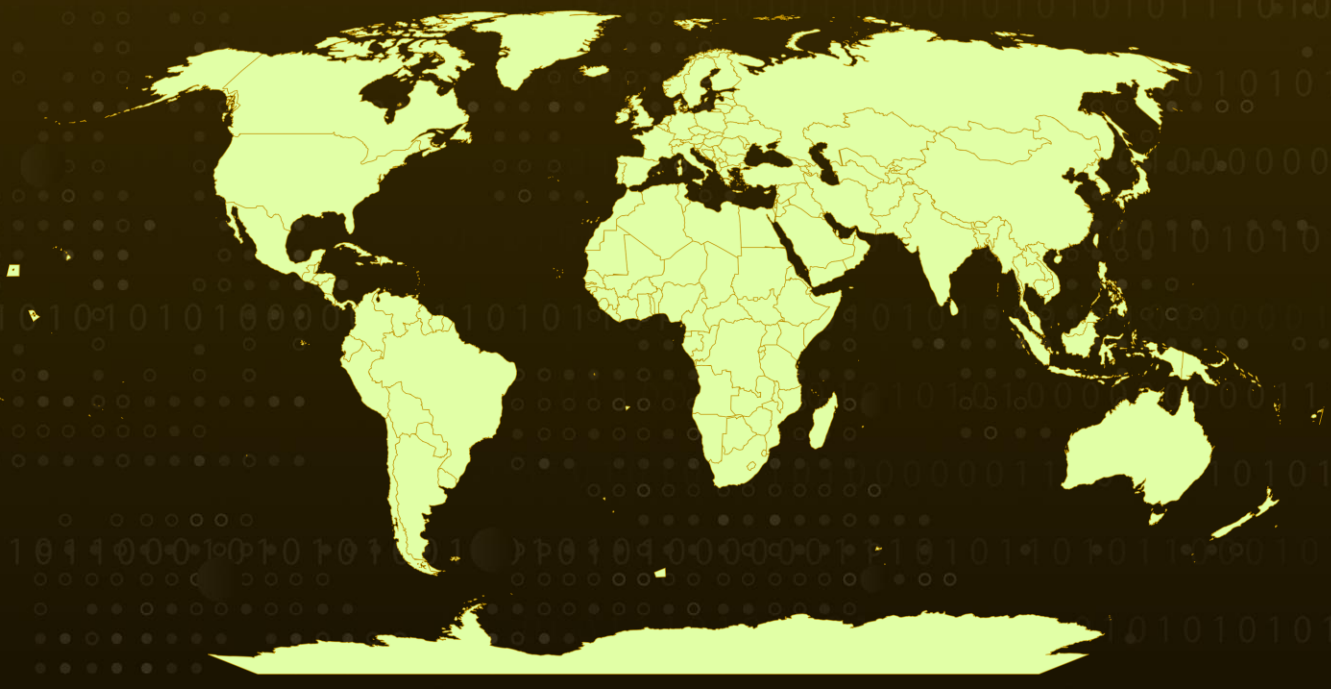
Attackers Exploit 8-Year-Old Redis Servers to Deploy Metasploit Meterpreter

Date of Publication	Admiralty Code	TA Number
April 12, 2024	A1	TA2024144

Summary

Attack Discovered: April 2024
Attack Region: Worldwide
Malware: Meterpreter, PrintSpoofer, Stager
Attack: Hackers are utilizing the Redis services to install the Metasploit Meterpreter backdoor highlights a concerning security vulnerability within organizations. Exploiting outdated versions of Redis, such as the one developed in 2016, provides threat actors with a gateway to infiltrate systems and potentially compromise the entire internal network.

Attack Regions



Attack Details

#1 Hackers deploying the Metasploit Meterpreter backdoor via the Redis service, particularly targeting the 2016 version, represents a method used by threat actors to infiltrate systems. With Metasploit in place, attackers can exploit vulnerabilities to gain control over the organization's internal network, effectively compromising the targeted server.

#2 Redis is an open-source, in-memory database and data structure storage system. In this case, threat actors likely utilized vulnerability exploits to execute commands or took advantage of improper settings within the Redis system. The specific version being exploited, version 3.x released in 2016, suggests that attackers may have exploited known vulnerabilities or misconfigurations due to its outdated status.

#3 Initially threat actor deployed PrintSpoofer, a tool for privilege escalation, leveraging PowerShell's "invoke-webrequest" command. This tool exploits the SeImpersonatePrivilege to escalate user privileges and is employed in attacks targeting vulnerable services like web servers or database service providers. The threat actor modified a string within PrintSpoofer to evade detection. There has been a shift in the installation method, with the CertUtil tool now being used instead of PowerShell which was used previously.

#4 Following the installation of PrintSpoofer, the threat actor proceeded to install Metasploit's Stager malware. Metasploit is a penetration testing framework used for assessing security vulnerabilities in networks and systems. Meterpreter serves as a backdoor for executing malicious actions and can be categorized into two types: staged and stageless.

#5 In the stageless approach, Meterpreter is directly included in the payload, leading to an increase in its size. Conversely, the staged method involves using a malware called "Stager" to download Meterpreter from a C&C server, resulting in a smaller payload size. The threat actor typically creates the Stager using a reverse TCP method and then executes it by establishing a connection to the C&C server to fetch the Meterpreter backdoor. Once Meterpreter is downloaded and executed in memory, the threat actor gains control over the compromised system.

#6 With Metasploit installed, a threat actor can utilize the malware's functionalities to take over not only the compromised system but also an organization's internal network. Security administrators must ensure that servers are patched to the most recent version and take precautions to prevent known vulnerabilities from being exploited.

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.

Regular Patch Management: Implement a robust patch management process. This involves regularly scanning for vulnerabilities and applying patches promptly. Automated patch management tools can streamline this process.

Continuous Monitoring: Implement continuous monitoring solutions to detect any unauthorized changes or suspicious activities on your servers. This allows you to respond quickly to any security incidents.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	TA0006 Credential Access
TA0008 Lateral Movement	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1584 Compromise Infrastructure	T1584.004 Server	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1105 Ingress Tool Transfer	T1068 Exploitation for Privilege Escalation	T1570 Lateral Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	cff64cc3e82aebd7a7e81f1633b5040e, dbdcbacbc74b139d914747690ebe0e1c, b26b57b28e61f9320cc42d97428f3806
IPv4:Port	34.124.148[.]215:9070
URLs	hxxp://35.185.187[.]24/PrintSpoofer.exe, hxxp://35.185.187[.]24/ps.exe, hxxp://35.185.187[.]24/meteran.exe

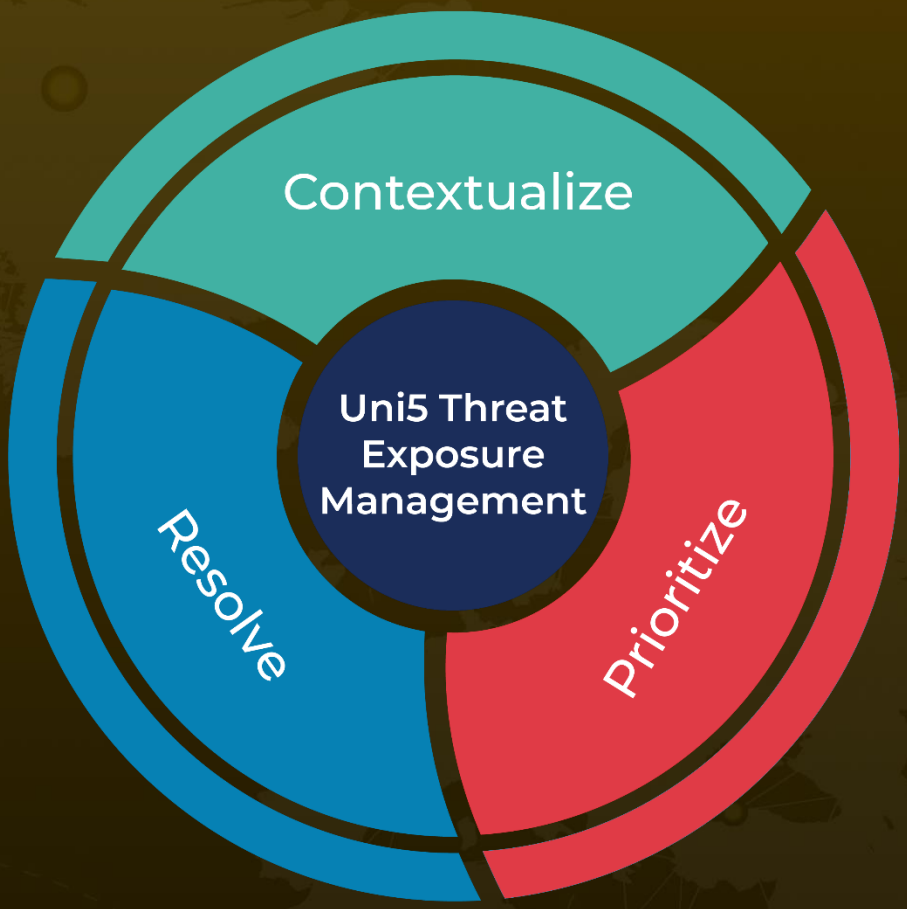
References

https://asec.ahnlab.com/en/64034/

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

April 12, 2024 • 5:50 AM

More at www.hivepro.com