Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

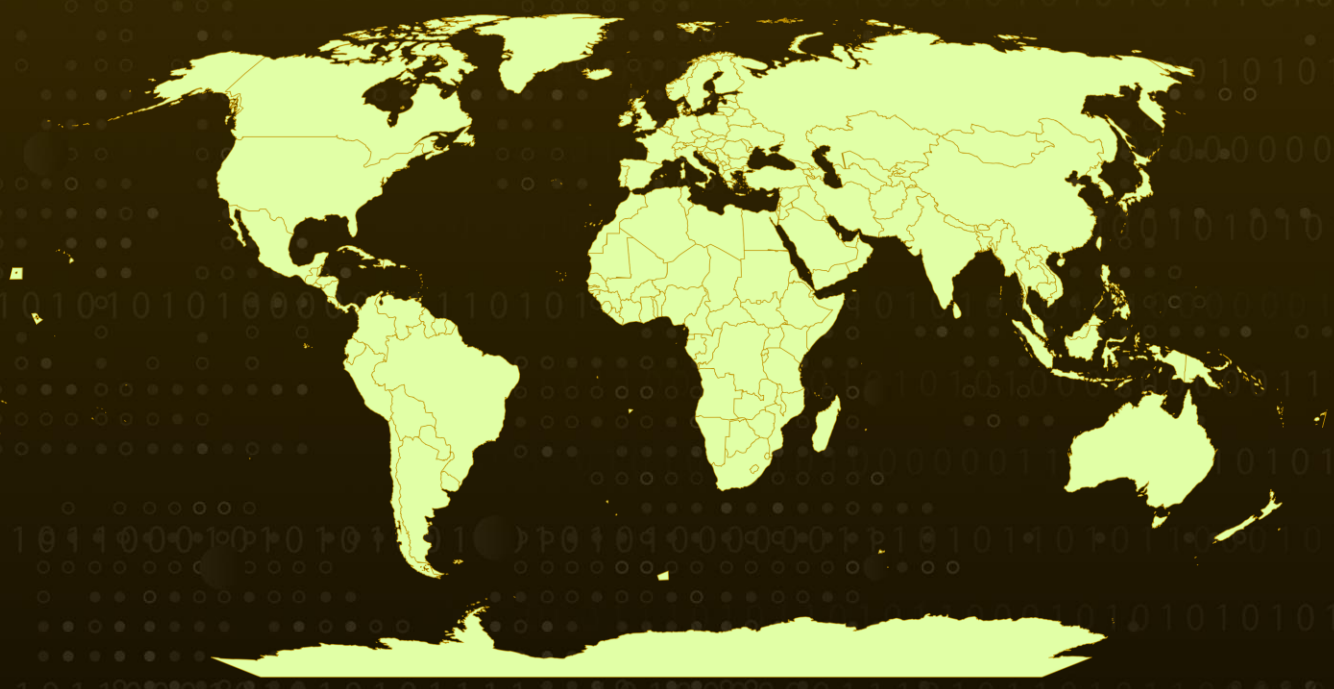
Migo Targets Redis Servers for Cryptojacking Attacks

Date of Publication	Admiralty Code	TA Number
February 23, 2024	A1	TA2024074

Summary

Attack Began: February 2024
Attack Region: Worldwide
Malware: Migo
Attack: A new campaign has been uncovered that mines cryptocurrencies on Redis servers running Linux hosts by means of a malicious programme known as "Migo." Migo is distributed as a Golang ELF binary that can persist on Linux hosts and is obfuscated at compile time. The malware uses a variety of commands to leverage Redis and initiate a cryptojacking attack.

Attack Regions



Attack Details

#1 The recently discovered malware, Migo, has been designed to infiltrate Redis servers with the primary objective of utilizing the underlying Linux host for cryptocurrency mining. Redis, a versatile in-memory data structure store, serves various purposes such as acting as a message broker, database, and cache.

#2 The attackers initiated the Migo campaign by exploiting Redis servers, which came to light when a malicious node connected to a Redis honeypot and utilized the `config set` function of the Redis CLI to disable specific security settings on the system. Attackers have been observed leveraging the Redis replica-read-only feature to deliver malicious payloads. This method echoes previous Redis cryptominer campaigns, which also utilized the same feature as an attack vector.

#3 To execute its core payload, Migo installs a customized XMRig miner on compromised endpoints by configuring a cron job to run silently in the background. Migo's architecture consists of an ELF file that has been stripped and packed with UPX, compiled from Go code for the x86_64 architecture. The attacker used compiled-time obfuscation to hinder and complicate reverse engineering attempts, effectively bypassing the "Program Counter Line Table" (pclntab) feature. This feature had allowed security researchers to infer malware capabilities from stack traces.

#4 In addition to exploiting Redis servers, Migo employs various tactics to evade detection and maintain persistence. It scans files and directories under /etc using passive file reading techniques, potentially to avoid dynamic analysis and sandbox solutions. It utilizes systemd timers for persistence, disable SELinux, run a cryptocurrency miner, configure iptables, remove competing miners, and search for specific items in the target environment.

#5 Persistence is ensured through a systemd service and timer, allowing Migo's payload to execute every 5 seconds and contribute to the mining pool. The attack methodology employed by Migo underscores the threat actor's profound understanding of the Redis environment and its functionalities. By operating stealthily and avoiding disruptions or data corruption, the threat actor can exploit this access to potentially deploy more malicious payloads.

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.

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	TA0009 Collection	T1049 System Network Connections Discovery	T1053 Scheduled Task/Job
T1053.003 Cron	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1560 Archive Collected Data
T1497 Virtualization/Sandbox Evasion	T1543 Create or Modify System Process	T1543.002 Systemd Service	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1014 Rootkit
T1574 Hijack Execution Flow	T1574.006 Dynamic Linker Hijacking	T1082 System Information Discovery	T1562 Impair Defenses
T1562.004 Disable or Modify System Firewall			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8cce669c8f9c5304b43d6e91e6332b1cf1113c81f355877dabd25198c3c3f208, c5dc12dbb9bb51ea8acf93d6349d5bc7fe5ee11b68d6371c1bbb098e21d0f685, 2b03943244871ca75e44513e4d20470b8f3e0f209d185395de82b447022437ec, 364a7f8e3701a340400d77795512c18f680ee67e178880e1bb1fcda36ddbc12c, 5dc4a48ebd4f4be7ffcf3d2c1e1ae4f2640e41ca137a58dbb33b0b249b68759e, 76ecd546374b24443d76c450cb8ed7226db84681ee725482d5b9ff4ce3273c7f, 32d32bf0be126e685e898d0ac21d93618f95f405c6400e1c8b0a8a72aa753933
IP	103[.]79[.]118[.]221

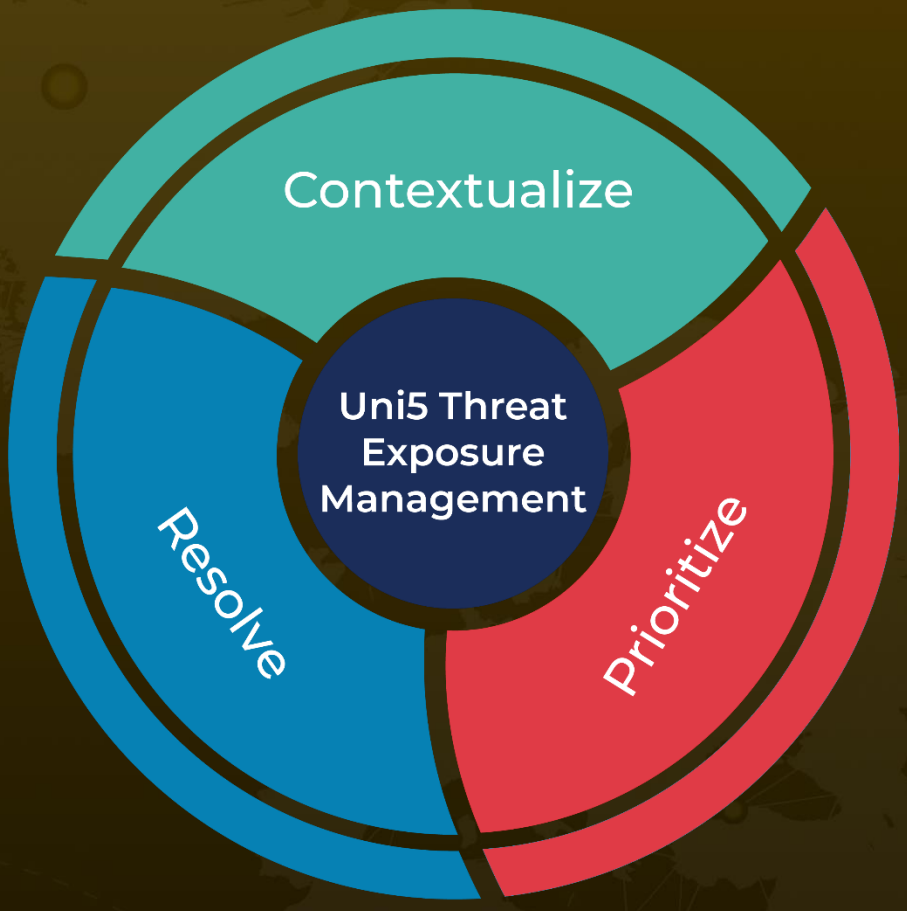
References

https://www.cadosecurity.com/migo-a-redis-miner-with-novel-system-weakening-techniques/

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

February 23, 2024 • 5:55 AM

More at www.hivepro.com