Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

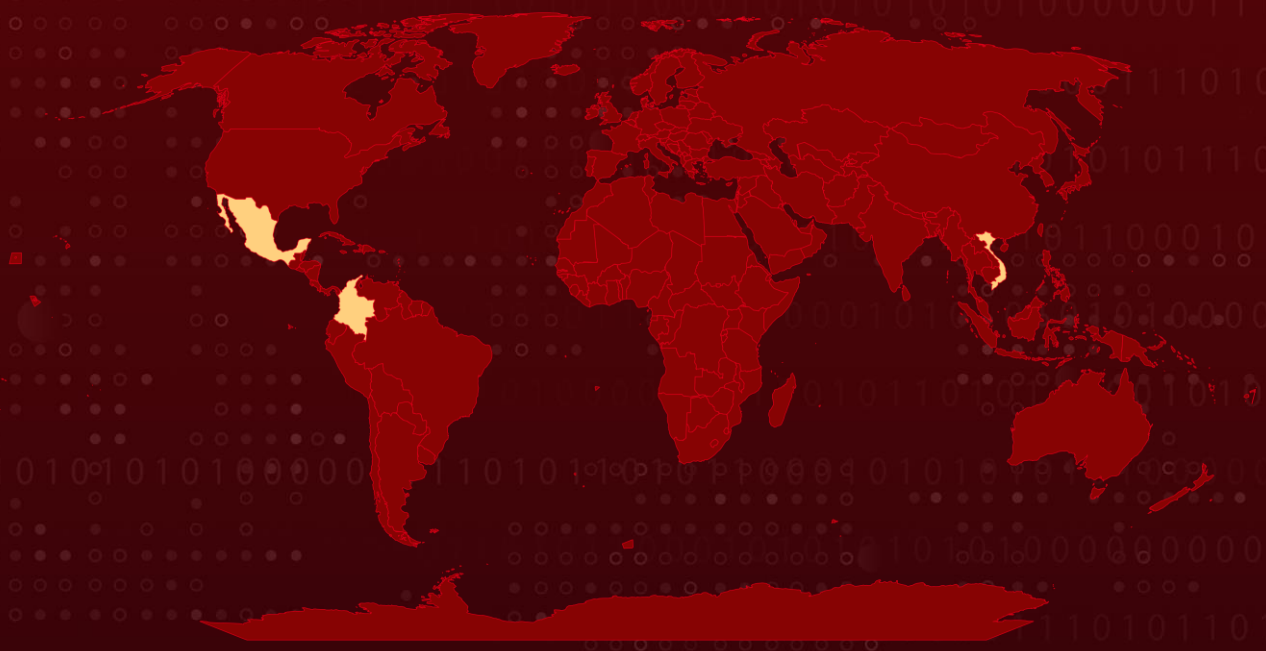
NKAbuse: A New Multiplatform Threat Exploiting the Blockchain Protocol

Date of Publication	Admiralty Code	TA Number
December 18, 2023	A1	TA2023508

Summary

First appeared: December 2023
Affected Platform: Linux, IoT devices
Attack Region: Mexico, Colombia, and Vietnam
Target Industry: Financial
Malware: NKAbuse
Attack: A novel malware called 'NKAbuse' stands out as a new, Go-based, multi-platform threat. What makes this malware distinctive is its pioneering use of the peer-to-peer network connectivity protocol NKN (New Kind of Network) technology for data exchange. This utilization of NKN technology makes NKAbuse a stealthy threat, emphasizing its ability to operate discreetly and potentially evade traditional detection methods.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-5638	Apache Struts Remote Code Execution Vulnerability	Apache Struts	✓	✓	✓

Attack Details

#1 A newly discovered multi-platform threat, NKAbuse, has been found using the decentralized, peer-to-peer network connectivity protocol NKN (New Kind of Network) for communication. NKN, a network protocol incorporating blockchain technology for resource management, offers a secure and transparent model for network operations. While NKAbuse primarily targets Linux desktops, its ability to infect MISP and ARM systems also poses a threat to IoT devices.

#2 The NKN network protocol, with over 60,000 official nodes, is designed to optimize data transmission through various routing algorithms. Unfortunately, this efficiency has made NKN a target for exploitation by malware operators. NKAbuse utilizes the NKN public blockchain protocol to execute flooding attacks and act as a backdoor within Linux systems. To infiltrate systems, the malware uploads an implant to the victim host, establishes persistence through a cron job, and installs itself in the host's home folder.

#3 NKAbuse takes advantage of an obsolete Apache Struts vulnerability, CVE-2017-5638, to target a financial company. Using the NKN public blockchain protocol, NKAbuse executes DDoS attacks that are challenging to trace back due to the novel protocol's lack of active monitoring by security tools. The malware client communicates with the bot master through NKN, facilitating data exchange using various protocols.

#4 NKAbuse also acts as a potent RAT equipped with capabilities for persistence, command execution, and information gathering. Using the "Heartbeat" framework, it engages in regular communication with the bot master, storing essential information about the infected host. Additionally, NKAbuse can capture screenshots of the infected machine through an open-source project.

#5 This multifaceted functionality makes NKAbuse a powerful tool for remote control and extensive information acquisition. The use of blockchain technology adds an extra layer of complexity, making defense against this threat exceptionally challenging.

Recommendations

Apply Patch: Install the security patch provided by Apache to address the CVE-2017-5638 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

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.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of malware and prevent it from accessing critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0007 Discovery	TA0011 Command and Control
TA0040 Impact	T1104 Multi-Stage Channels	T1083 File and Directory Discovery	T1498 Network Denial of Service
T1033 System Owner/User Discovery	T1059 Command and Scripting Interpreter	T1057 Process Discovery	T1053 Scheduled Task/Job
T1053.003 Cron			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	11e2d7a8d678cd72e6e5286ccfb4c833
Files Created	/root/.config/StoreService, /root/.config/StoreService/app_linux_amd64, /root/.config/StoreService/files, /root/.config/StoreService/.cache

Patch Details

Upgrade to Struts version 2.3.32, 2.5.10.1 or the latest version

Link:
https://struts.apache.org/download.cgi#struts-ga

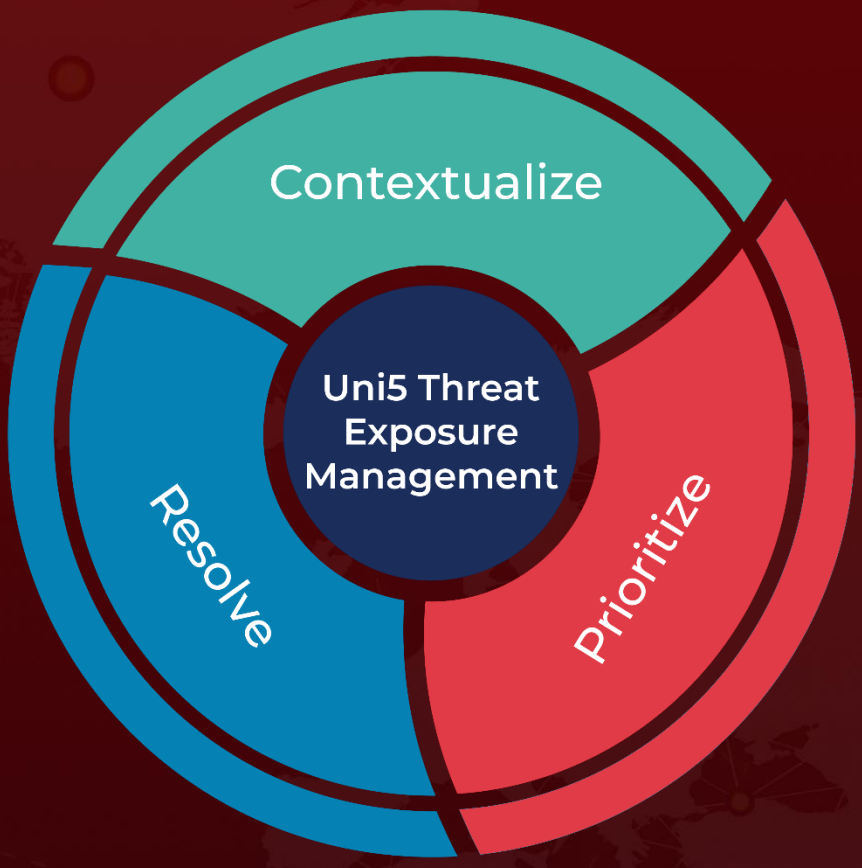
References

https://securelist.com/unveiling-nkabuse/111512/

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

December 18, 2023 . 2:30 AM

More at www.hivepro.com