Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

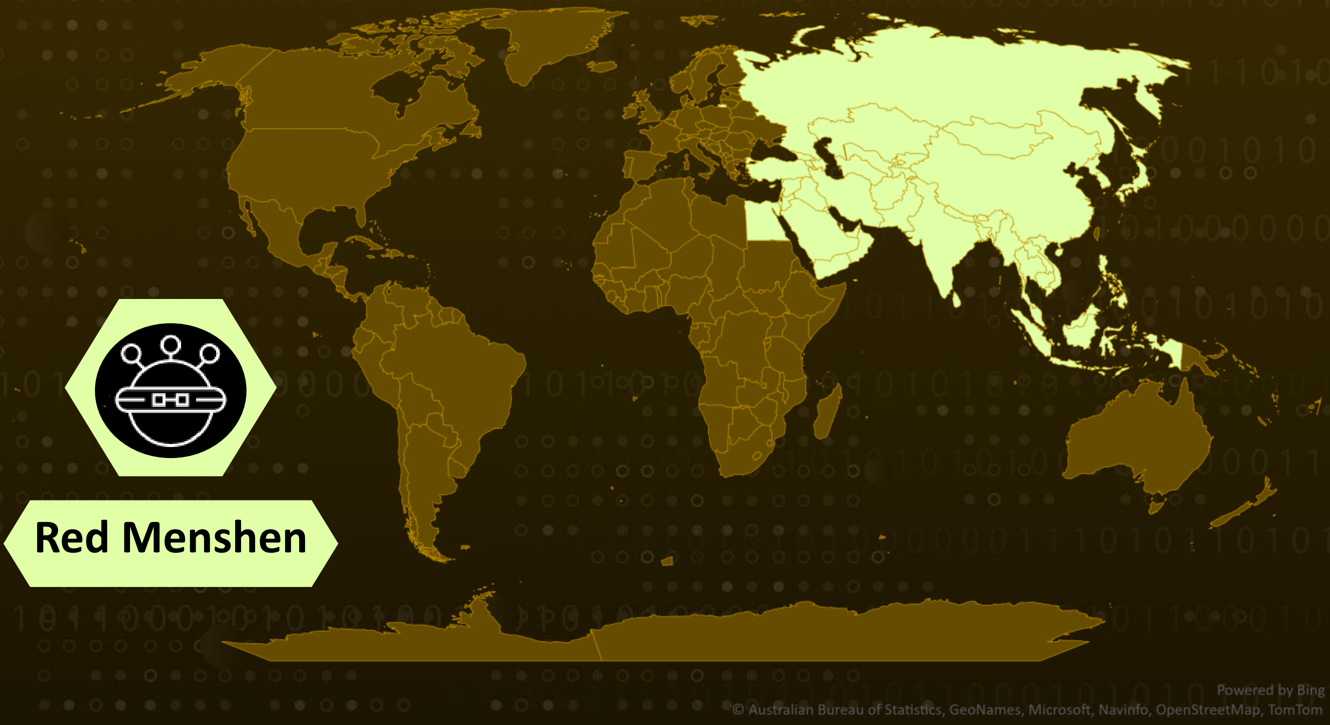
New Variant of BPFDoor Linux Malware Features Enhanced Encryption and Stealthy Communication

Date of Publication	Admiralty Code	TA Number
May 12, 2023	A1	TA2023226

Summary

First appeared: 2017
Attack Region: Middle East and Asia
Actor name: Red Menshen (AKA Red Dev 18)
Malware: BPFDoor
Affected Platform: Linux
Targeted Sector: Telecommunications
Attack: A new variant of the Linux malware BPFDoor has been discovered, featuring more robust encryption and reverse shell communication. It uses the BPF to bypass firewall restrictions, allowing threat actors to maintain persistence and remain undetected on breached Linux systems.

Attack Regions



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

Attack Details

#1

A new variant of the Linux malware called BPFDoor, which has been active since at least 2017, has been discovered. The malware is associated with a Chinese threat actor, Red Menshen (AKA Red Dev 18), which has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors since 2021.

#2

The new variant of the malware features more robust encryption and reverse shell communication, making it stealthier and harder to detect. It uses the Berkeley Packet Filter (BPF) for receiving instructions while bypassing incoming traffic firewall restrictions, allowing threat actors to maintain lengthy persistence on breached Linux systems and remain undetected for extended periods.

#3

Upon execution, BPFDoor creates and locks a runtime file and then sets itself to ignore various OS signals that could interrupt it. The malware allocates a memory buffer and creates a packet sniffing socket that it uses for monitoring incoming traffic for a "magic" byte sequence.

#4

When it finds a packet containing its "magic" bytes in the filtered traffic, it treats it as a message from its operator and parses out two fields and then forks itself. The parent process continues and monitors the filtered traffic coming through the socket while the child treats the previously parsed fields as a Command & Control IP-Port combination and attempts to contact it. After establishing a connection with the C2, the malware sets up a reverse shell and waits for a command from the server.

Recommendations

Monitoring network traffic and logs for any unusual activity, especially on ports that may be associated with BPFDoor malware communication. Regular network traffic analysis can help detect any outgoing traffic that may be indicative of BPFDoor malware communication with its Command & Control server.

Having robust endpoint protection can help detect and prevent the execution of BPFDoor malware on endpoints. Organizations should ensure that they have up-to-date antivirus software and endpoint detection and response (EDR) solutions in place to detect and respond to any malicious activities.

BPFDoor creates and locks a runtime file on "/var/run/initd.lock" upon execution. Monitoring this file's integrity can help detect any changes made by the malware and help prevent it from maintaining persistence on the system. Organizations should implement file integrity monitoring tools to monitor this file and other critical system files for any unauthorized changes.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0006 Credential Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1071 Application Layer Protocol
T1205 Traffic Signaling	T1573 Encrypted Channel	T1562 Impair Defenses	T1059 Command and Scripting Interpreter
T1562.004 Disable or Modify System Firewall	T1040 Network Sniffing	T1572 Protocol Tunneling	T1205.002 Socket Filters
T1106 Native API	T1083 File and Directory Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7
Mutex	/var/run/initd[.]lock

References

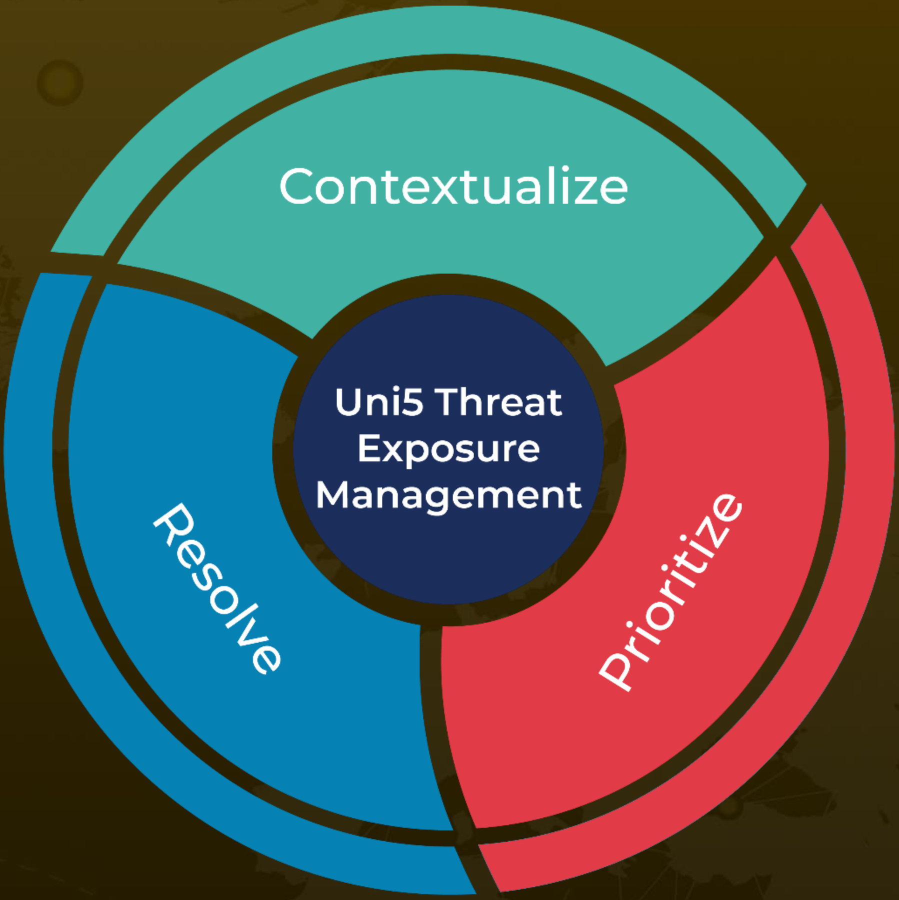
https://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game

https://www.bleepingcomputer.com/news/security/stealthier-version-of-linux-bpfdoor-malware-spotted-in-the-wild/

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

May 12, 2023 • 3:30 AM

More at www.hivepro.com