Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

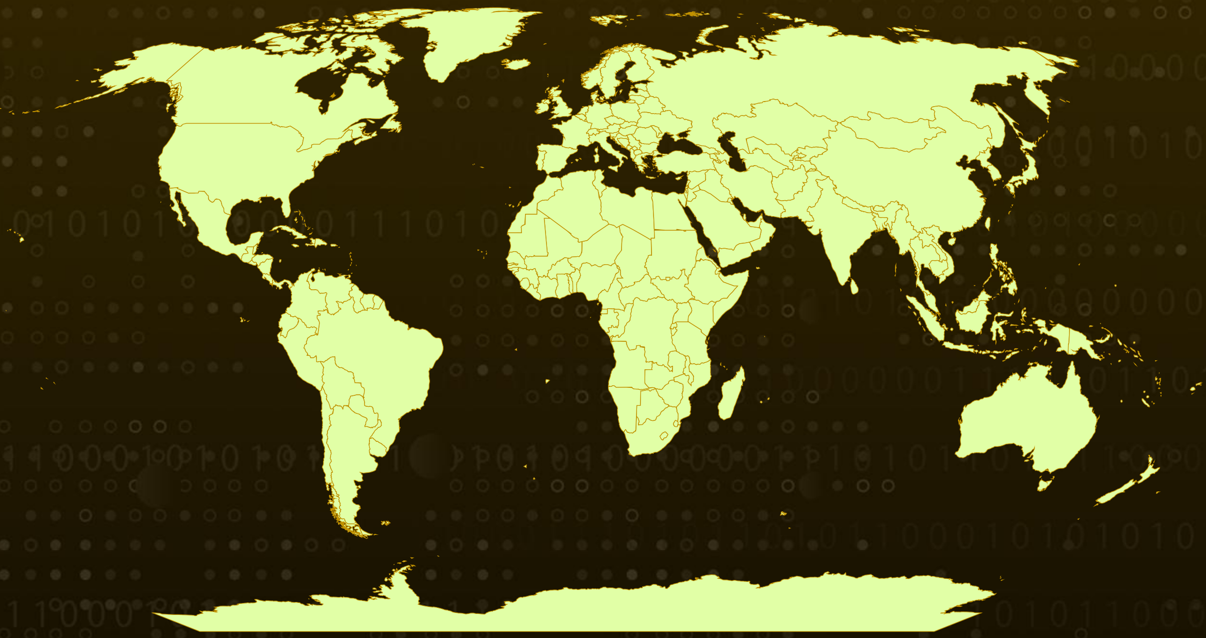
Plague in the Shadows: Unmasking a Silent Linux Backdoor

Date of Publication	Admiralty Code	TA Number
August 6, 2025	A1	TA2025239

Summary

Attack Discovered: July 2024
Targeted Countries: Worldwide
Malware: Plague
Affected Platform: Linux
Attack: The Plague backdoor is a stealthy and well-crafted Linux malware that has silently infiltrated systems by hooking into PAM (Pluggable Authentication Modules), allowing attackers to bypass authentication and maintain persistent SSH access, all while going undetected by antivirus engines. The malware has evolved over time, with threat actors actively developing new variants using increasingly complex string obfuscation and encryption techniques to avoid analysis. Plague also includes anti-debugging features, static credentials, and environment tampering to erase traces of attacker activity from system logs and session histories. Plague remains a quiet yet serious threat to Linux infrastructure, emphasizing the need for proactive behavioral detection, careful PAM auditing, and a greater focus on securing authentication components.

Attack Regions



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

Attack Details

#1 A stealthy Linux backdoor known as Plague has managed to remain undetected, largely due to its ability to completely evade antivirus engines. This malicious implant compromises the Pluggable Authentication Module (PAM), allowing attackers to silently bypass system-level authentication and maintain persistent SSH access, without triggering any alerts.

#2 What makes Plague particularly concerning is its deep integration into core system components like PAM. This level of access grants its remarkable persistence and stealth, making it an ideal tool for long-term espionage or unauthorized access. Its undetected presence serves as a stark reminder of the importance of proactive defense mechanisms, including YARA-based hunting and behavioral monitoring, especially within Linux environments that often lack robust visibility into such silent threats.

#3 Evidence suggests that Plague has undergone continuous development. Multiple samples, compiled over an extended period and in varying environments, include metadata pointing to different compiler versions, indicating active maintenance by its authors. The earliest known variant, named hijack, might offer clues about its origins. This version also reveals a range of stealthy features: anti-debugging techniques, string obfuscation, hardcoded passwords, and artifacts deliberately concealed from session logs, all contributing to its silent and persistent nature. Despite these hints, attribution remains uncertain.

#4 Over time, the threat actor behind Plague has significantly evolved the malware's string obfuscation techniques. Early versions relied on basic XOR-based encryption, while newer iterations adopted routines like the Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA). The most recent samples introduce an additional layer of complexity with a Deterministic Random Bit Generator (DRBG), further complicating both automated detection and manual reverse engineering. These layers obscure not just strings but also their memory references, rendering static analysis largely ineffective.

#5 Further enhancing its stealth, Plague sanitizes the runtime environment to erase any signs of SSH usage. It scrubs evidence of interactive sessions and login metadata from logs, leaving no audit trail and effectively wiping the attacker’s footprints from the system. In sum, Plague represents a highly advanced threat to Linux systems. Its use of sophisticated obfuscation, environment checks, and static credentials combined with deep integration into system authentication mechanisms make it exceptionally hard to detect.

Recommendations

- **Regularly scan for unusual PAM files:** Review your /etc/pam.d/ and related PAM configuration files regularly. Malicious backdoors like Plague often masquerade as legitimate modules.

- **Check for suspicious shared libraries:** Watch out for unusual .so files like libselinux.so.8 in non-standard paths. Verify file integrity using known-good hashes and tools.

- **Monitor SSH activity and login patterns:** Keep an eye out for SSH logins that don’t match expected behavior especially ones without proper log trails or that bypass normal authentication.

- **Isolate and limit PAM module access:** Only trusted users or services should have permissions to modify PAM-related configurations or libraries. Use access controls and monitor changes.

- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0008 Lateral Movement
T1140 Deobfuscate/Decode Files or Information	T1497 Virtualization/Sandbox Evasion	T1070 Indicator Removal	T1562 Impair Defenses
T1562.003 Impair Command History Logging	T1547 Boot or Logon Autostart Execution	T1021 Remote Services	T1021.004 SSH
T1564 Hide Artifacts	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	85c66835657e3ee6a478a2e0b1fd3d87119bebadc43a16814c30eb94c53766bb, 7c3ada3f63a32f4727c62067d13e40bcb9aa9cbec8fb7e99a319931fc5a9332e, 9445da674e59ef27624cd5c8ffa0bd6c837de0d90dd2857cf28b16a08fd7dba6, 5e6041374f5b1e6c05393ea28468a91c41c38dc6b5a5230795a61c2b60ed14bc, 6d2d30d5295ad99018146c8e67ea12f4aaa2ca1a170ad287a579876bf03c2950, e594bca43ade76bbaab2592e9eabeb8dca8a72ed27afd5e26d857659ec173261, 14b0c90a2eff6b94b9c5160875fcf29aff15dcfdfd3402d953441d9b0dca8b39
Filename	libselinux.so.8, libse.so, hijack

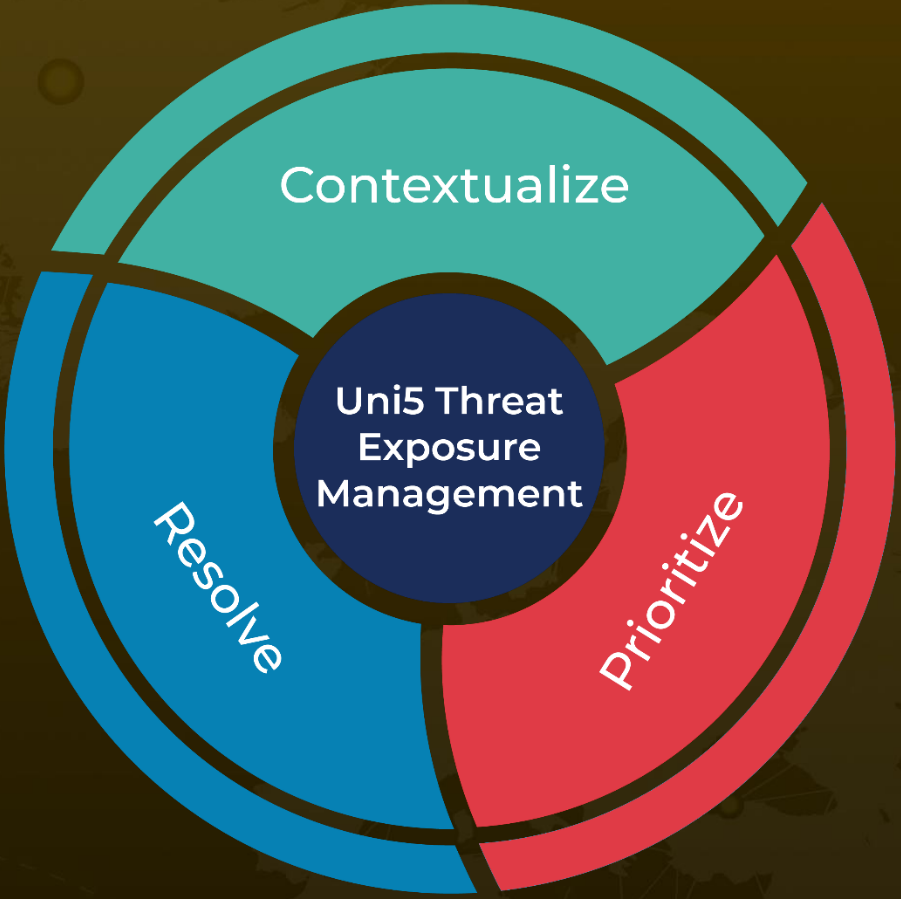
References

https://www.nextron-systems.com/2025/08/01/plague-a-newly-discovered-pam-based-backdoor-for-linux/

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

August 6, 2025 • 6:30 AM

More at www.hivepro.com