Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

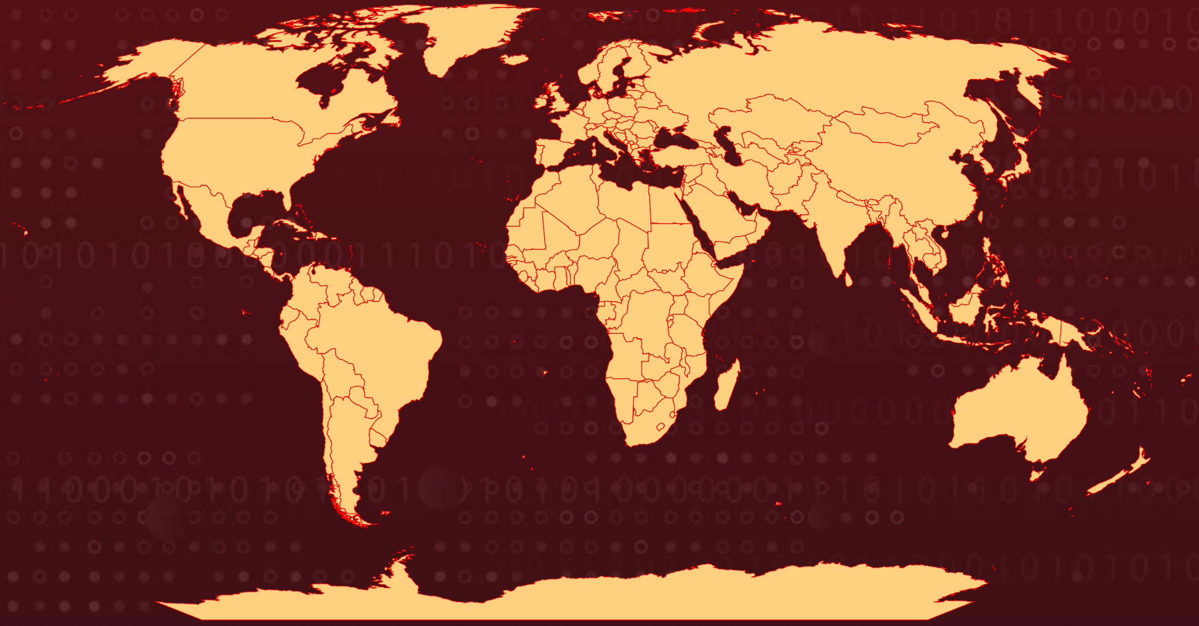
PUMAKIT Unveiled: A Stealthy Malware Redefining Linux Threats

Date of Publication	Admiralty Code	TA Number
December 13, 2024	A1	TA2024462

Summary

Attack Discovered: September 2024
Targeted Countries: Worldwide
Affected Platform: Linux
Malware: PUMAKIT
Attack: A newly discovered Linux rootkit malware, named Pumakit, employs sophisticated stealth techniques and advanced privilege escalation methods to remain undetected on compromised systems. This malware is a multi-faceted threat, consisting of several components: a dropper, memory-resident executables, a kernel module rootkit, and a shared object (SO) userland rootkit. This multi-layered design makes Pumakit a particularly complex and dangerous threat.

Attack Regions



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

Attack Details

#1 PUMAKIT is an advanced malware characterized by its intricate multi-stage architecture. It comprises a dropper, memory-resident executables, a loadable kernel module (LKM) rootkit, and a shared object (SO) userland rootkit. Its core component, named "PUMA," leverages an internal Linux function tracer to manipulate core system operations and employs techniques like privilege escalation and command execution for system interaction. The LKM rootkit activates only under specific conditions validated by kernel scans, enabling functionalities such as privilege escalation, file hiding, and communication with C2 servers.

#2 PUMAKIT's execution begins with a dropper in the form of a "cron" binary. This binary spawns two memory-resident executables /memfd:tgt and /memfd:wpn which verify system conditions, run a temporary script, and deploy the LKM rootkit containing the Kitsune component. This layered design enhances stealth by leveraging memory-resident files and performing precise environmental checks, significantly reducing detection risk.

#3 The "cron" binary functions as a dropper, embedding payloads directly into memory to avoid filesystem detection. It checks for the keyword "Huinder" in command-line arguments and executes ELF binaries entirely in memory if present. Using writeToMemfd(...) for fileless execution and execveat() to run binaries via file descriptors, PUMAKIT mimics legitimate system processes. The /memfd:tgt file replicates the Ubuntu Cron binary, while /memfd:wpn initiates the LKM rootkit.

#4 A supporting shell script, "script.sh," inspects and decompresses files using utilities like gunzip and bunzip2 to verify ELF binaries. The rootkit loads only when prerequisites like secure boot validation and kernel symbol resolution are met, reflecting its highly targeted deployment.

#5 The LKM rootkit, relies on kallsyms_lookup_name() for symbol resolution. It bypasses restrictions using tactics like fake GPL licenses to access non-exported kernel functions. The rootkit hooks system calls through ftrace mechanisms, particularly intercepting rmdir() for executing specialized commands. These include initialization confirmation, version retrieval, and temporary root privilege escalation.

#6 A key component, Kitsune responsible for persistence and user-space interactions. It includes strings indicating its role in coordinating these activities. PUMAKIT's advanced architecture, combining syscall hooking, memory-resident execution, and privilege escalation, poses significant challenges to detection and mitigation.

Recommendations

Implement Comprehensive Log Monitoring: Regularly monitor system logs such as /var/log/messages and /var/log/syslog for unusual events, such as the appearance of processes with executable stacks.

Monitor for Suspicious Command Execution: Track and analyze system calls and processes associated with privilege escalation, such as the rmdir command, especially when unusual UID/GID changes occur. Customize queries to detect abnormal command executions, particularly those linked to the creation of new kernel threads or attempts to escalate privileges.

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

TA0002 Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**T1036** Masquerading
T1140 Deobfuscate/Decode Files or Information	**T1218** System Binary Proxy Execution	**T1070** Indicator Removal	**T1014** Rootkit
T1564 Hide Artifacts	**T1564.001** Hidden Files and Directories	**T1053** Scheduled Task/Job	**T1053.003** Cron
T1068 Exploitation for Privilege Escalation	**T1059** Command and Scripting Interpreter	**T1059.004** Unix Shell	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f, cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe, 934955f0411538eebb24694982f546907f3c6df8534d6019b7ff165c4d104136, 8ef63f9333104ab293eef5f34701669322f1c07c0e44973d688be39c94986e27, 8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03, bbf0fd636195d51fb5f21596d406b92f9e3d05cd85f7cd663221d7d3da8af804, bc9193c2a8ee47801f5f44beae51ab37a652fda02cd32d01f8e88bb793172491, 1aab475fb8ad4a7f94a7aa2b17c769d6ae04b977d984c4e842a61fb12ea99f58
Domains	sec[.]opsecurity1[.]art, rhel[.]opsecurity1[.]art
IPv4	89[.]23[.]113[.]204

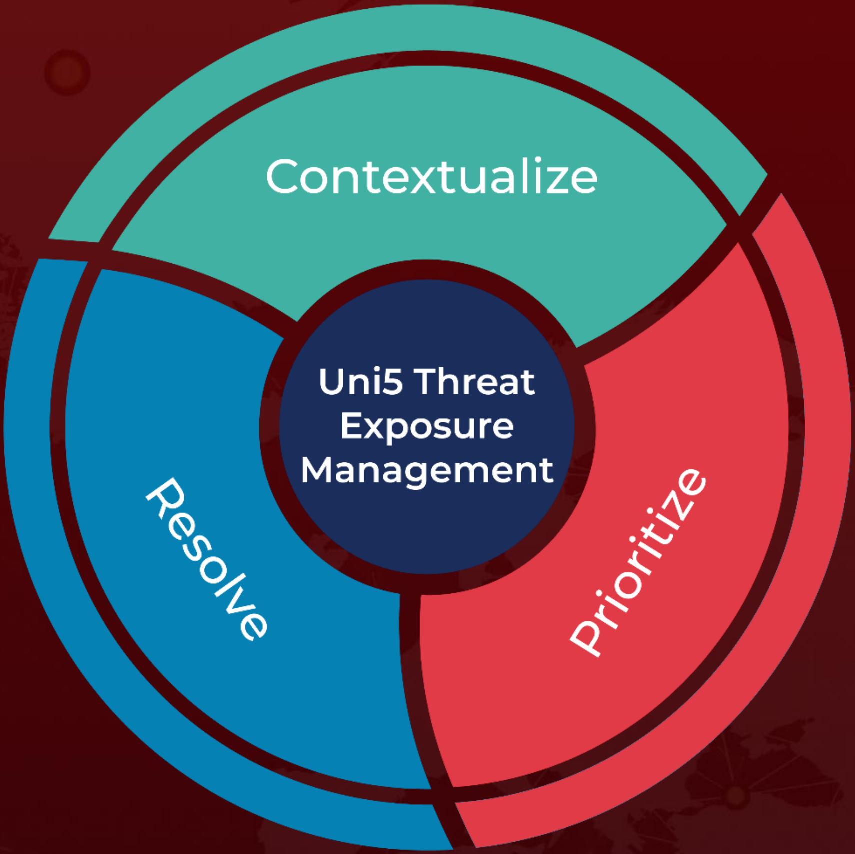
References

https://www.elastic.co/security-labs/declawing-pumakit

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 13, 2024 • 6:00 AM

More at www.hivepro.com