Hive Pro

Threat Level

Amber

HiveForce Labs

# THREAT ADVISORY

ATTACK REPORT

# WolfsBane and FireWood: Gelsemium’s Expanding Arsenal Targets Linux Systems

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| November 25, 2024 | A1 | TA2024442 |

# Summary

**Attack Discovered:** 2023
**Targeted Countries:** Worldwide
**Actor:** Gelsemium
**Malware:** WolfsBane, FireWood
**Attack:** A novel malware WolfsBane is linked to the Gelsemium APT group, as the Linux counterpart to their Windows-based Gelsevirine malware. Alongside this, a second backdoor called FireWood, tied to Project Wood, has also been identified, with its Windows variant previously deployed in Gelsemium's Operation TooHash. Both backdoors demonstrate the group's expanding cross-platform capabilities and sophisticated cyber-espionage strategies, underscoring the need for robust security measures to counter such advanced threats.

## Attack Regions

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

# Attack Details

#1 Two sophisticated Linux backdoors are dicovered, WolfsBane and FireWood, both intricately tied to the Gelsemium APT group, a known player in cyberespionage. WolfsBane, a Linux variant of the Gelsevirine backdoor, and FireWood, an extension of the Project Wood backdoor. This shift towards Linux-focused malware signals a strategic pivot by threat actors, likely driven by advances in Windows security, including endpoint detection tools and Microsoft's default disabling of VBA macros.

#2 WolfsBane demonstrates a high level of sophistication with its streamlined deployment mechanism, comprising a dropper, launcher, and backdoor. Its use of custom libraries for network communication and rootkits to mask activity echoes the modularity and precision of its Windows counterpart.

#3 FireWood, on the other hand, builds on the Project Wood lineage by employing kernel-level rootkits to conceal processes and advanced encryption protocols like TEA for secure communications. The parallels between these backdoors in their configurations, command execution methods, and C&C communication mechanisms underscore their shared origin within Gelsemium's arsenal.

#4 The archives where these backdoors were discovered also contained auxiliary tools. Among them are SSH password stealers, privilege escalation utilities, and modified webshells. These tools allow seamless command execution, data manipulation, and file exfiltration, often in a stealthy manner. The webshells, some equipped with graphical interfaces and encrypted payloads, add a further layer of complexity, making detection and analysis particularly challenging.

#5 The evidence points to targeted campaigns against entities in Taiwan, the Philippines, and Singapore.  While WolfsBane is firmly attributed to Gelsemium, FireWood's association remains less certain. This ambiguity suggests the potential for shared tools among multiple Chinese APT groups. This trend highlights the growing collaboration among threat actors and the pressing need for stronger defenses focused on Linux environments.

# 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.

**Monitor Network Traffic:** Use network monitoring tools to detect unusual communications with Command-and-Control (C&C) servers. Pay special attention to domains and protocols flagged as indicators of compromise, such as those associated with Gelsemium.

**Audit Startup Processes:** Regularly inspect startup entries and scheduled tasks for anomalies. Look for suspicious .desktop files or services like display-managerd.service that may indicate persistence mechanisms.

**Network Segmentation:** Isolate the vulnerable systems by implementing network segmentation. This practice helps contain potential attacks and prevents unauthorized lateral movement within the network, minimizing the impact of successful exploitation.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0042<br>Resource Development | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0007<br>Discovery | TA0009<br>Collection | TA0010<br>Exfiltration |
| T1583<br>Acquire Infrastructure | T1583.001<br>Domains | T1583.004<br>Server | T1587<br>Develop Capabilities |
| T1587.001<br>Malware | T1059<br>Command and Scripting Interpreter | T1059.004<br>Unix Shell | T1037<br>Boot or Logon Initialization Scripts |

| | | | |
|---|---|---|---|
| T1037.004<br>RC Scripts | T1543<br>Create or Modify System Process | T1543.002<br>Systemd Service | T1574<br>Hijack Execution Flow |
| T1574.006<br>Dynamic Linker Hijacking | T1547<br>Boot or Logon Autostart Execution | T1547.013<br>XDG Autostart Entries | T1546<br>Event Triggered Execution |
| T1546.004<br>Unix Shell Configuration Modification | T1548<br>Abuse Elevation Control Mechanism | T1548.001<br>Setuid and Setgid | T1070<br>Indicator Removal |
| T1070.004<br>File Deletion | T1070.006<br>Timestomp | T1070.009<br>Clear Persistence | T1564<br>Hide Artifacts |
| T1564.001<br>Hidden Files and Directories | T1222<br>File and Directory Permissions Modification | T1222.002<br>Linux and Mac File and Directory Permissions Modification | T1027<br>Obfuscated Files or Information |
| T1027.009<br>Embedded Payloads | T1014<br>Rootkit | T1036<br>Masquerading | T1036.005<br>Match Legitimate Name or Location |
| T1082<br>System Information Discovery | T1083<br>File and Directory Discovery | T1056<br>Input Capture | T1041<br>Exfiltration Over C2 Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA1 | 0ab53321bb9699d354a032259423175c08fec1a4,<br>0fef89711da11c550d3914debc0e663f5d2fb86c,<br>9f7790524bd759373ab57ee2aafa6f5d8bcb918a,<br>72db8d1e3472150c1be93b68f53f091aacc2234d,<br>209c4994a42af7832f526e09238fb55d5aab34e5,<br>238c8e8eb7a732d85d8a7f7ca40b261d8ae4183d,<br>600c59733444bc8a5f71d41365368f3002465b10,<br>843d6b0054d066845628e2d5db95201b20e12cd2,<br>8532eca04c0f58172d80d8a446ae33907d509377,<br>85528eac10090ae743bcf102b4ae7007b6468255,<br>44947903b2bc760ac2e736b25574be33bf7af40b,<br>b2a14e77c96640914399e5f46e1dec279e7b940f,<br>b3dfb40336c2f17ec74051844ffaf65ddb874cfc,<br>bed9efb245fac8cfff8333ae37ad78ccfb7e2198, |

| TYPE | VALUE |
|---|---|
| SHA1 | cdbbb6617d8937d17a1a9ef12750bee1cddf4562,<br>f1df0c5a74c9885cb5934e3eee5e7d3cf4d291c0,<br>f43d4d46bae9ad963c2eb05ef43e90aa3a5d88e3,<br>fd601a54bc622c041df0242662964a7ed31c6b9c,<br>055f1e13e0fea44dc42e8cd8c9219ed588360304,<br>0cedfb1789ef139b6040cf8d84ba130360c4eb7d,<br>1042c798d7ff69eb52cbeae684c74fc0ee84aacd,<br>2d6ceaf73ea7f70135d9a82a397625c89c408f05,<br>4a932622a1a5259e9c97ebfa8dc11fa84dffe039,<br>6ae33a9df4e7d5d19c67edc1d1b73c1674ff5fc1,<br>6f43fe80806a3fe5c866c0b63cc5b105a85d0e75,<br>8ab3acc8a3f89e5b8e7a1929149d273eddadae64,<br>a80c7010fea9915a0a82108139aec3aa2363f0df,<br>bca97bf7e93309e49311701b22569395b2baecc7 |
| Domains | dsdsei[.]com,<br>asidomain[.]com,<br>4vw37z[.]cn,<br>acro[.]ns1[.]name,<br>domain[.]dns04.com,<br>info[.]96html[.]com,<br>microsoftservice[.]dns1[.]us,<br>pctftp[.]otzo[.]com,<br>sitesafecdn[.]hopto[.]org,<br>traveltime[.]hopto[.]org,<br>www[.]sitesafecdn[.]dynamic-dns[.]net,<br>www[.]travel[.]dns04[.]com |
| IPv4 | 149[.]248[.]14[.]53,<br>210[.]209[.]72[.]180 |

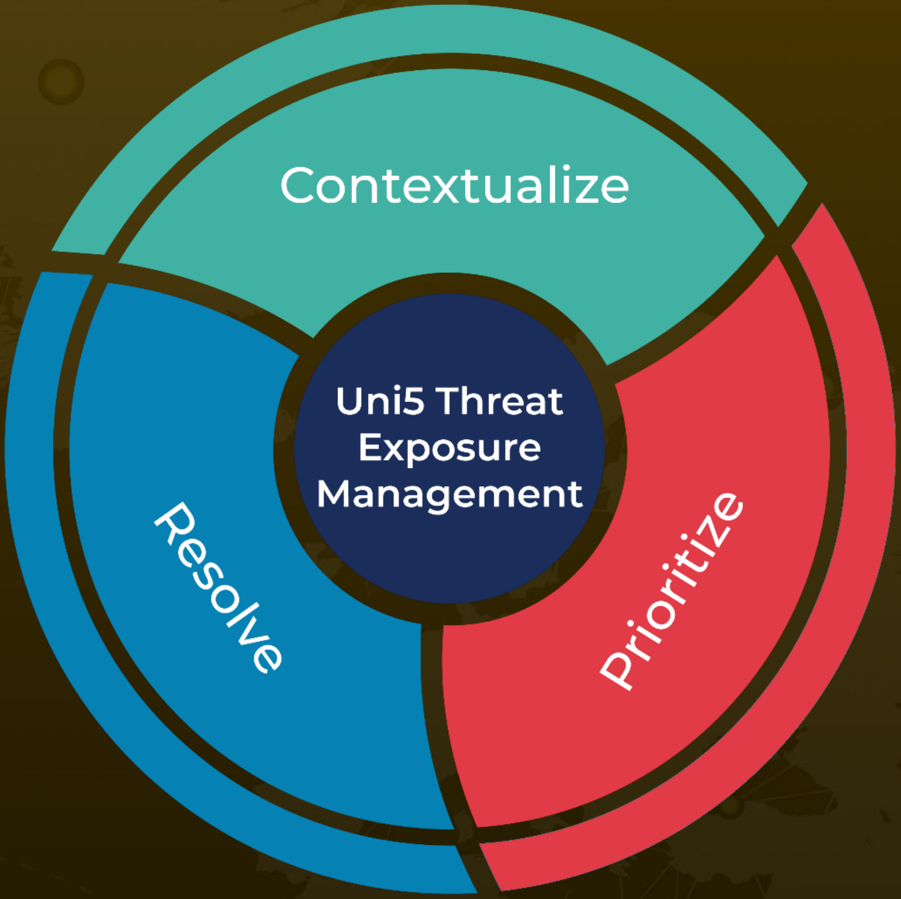
## References

https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/#Technical%20analysis

# 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

**November 25, 2024 • 5:50 AM**

More at www.hivepro.com