Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

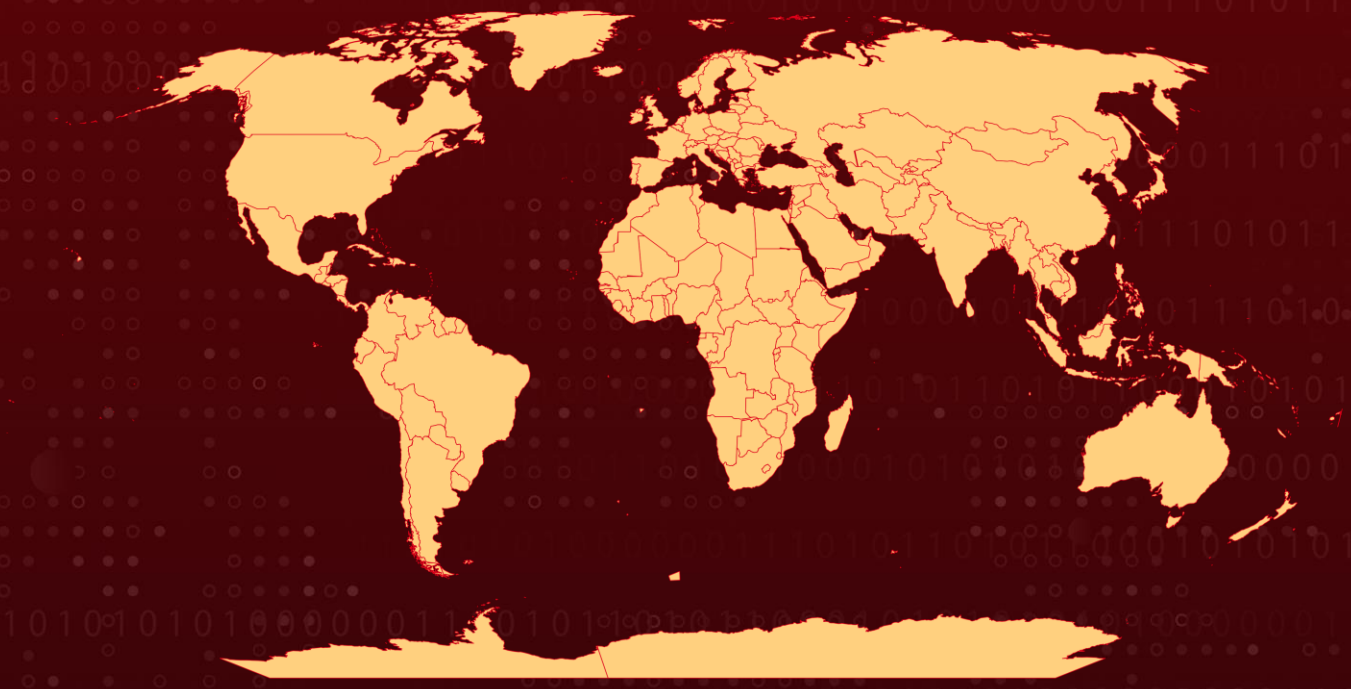
Linux malware leverages plugin exploits to backdoor WordPress sites

Date of Publication	Admiralty Code	TA Number
January 2, 2023	A1	TA2023002

Summary

First appeared: December 2022
Attack Region: Worldwide
Attack: Linux malware has been injecting malicious JavaScript and exploiting weaknesses in some obsolete WordPress plugins.

Attack Regions



Attack Details

#1

WordPress sites are being exploited by an unidentified strain of Linux malware that exploits flaws in plugins and compromises the sites by injecting malicious JavaScripts that are run sequentially until one of them succeeds. The malware targets both 32-bit and 64-bit Linux systems, enabling the malicious user to execute commands remotely.

#2

Before attacking, the malware contacts its command-and-control server and obtains the address of the site to be infected. Users are sent to attacker-controlled sites when they click on any aspect of an infected page. These redirections may be employed to help circumvent detection and blocking in phishing, malware distribution, and malvertising campaigns.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	T1560 Archive Collected Data
T1057 Process Discovery	T1003 OS Credential Dumping	T1055 Process Injection	T1068 Exploitation for Privilege Escalation
T1110 Brute Force	T1134 Access Token Manipulation	T1204 User Execution	T1001 Data Obfuscation

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	215a4470063080696630fb6015378938e8c16a15 c1620c4a48a3dcb1d27e587f456b371fc43bcb3d 9e6178d90f58e9459377a17a7ec2f5bedecd7515 6bcbd2a5dbfc9a5763c47b7eb327e7df35b401d1 c0053393f9dbe6113bef85dd88b02fa101df030c c9f7cbc5e634370c396b88c74f426e7a82e23455
Domains	lobbydesires[.]com letsmakeparty3[.]ga deliverygoodstrategies[.]com gabriellalovecats[.]com css[.]digestcolect[.]com clon[.]collectfasttracks[.]com count[.]trackstatisticsss[.]com
IP Addresses	109[.]234.38[.]69 198[.]24.166[.]222 193[.]37.213[.]197 45[.]9.148[.]48

References

https://news.drweb.com/show/?i=14646&lng=en&c=23

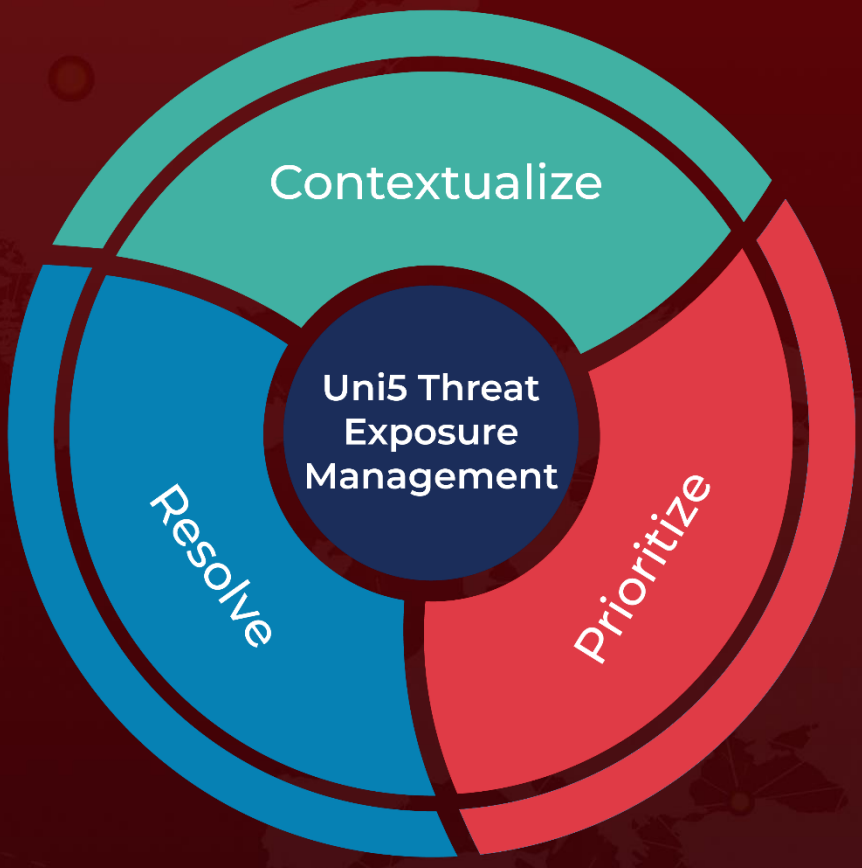
https://github.com/DoctorWebLtd/malware-iocs/tree/master/Linux.Backdoor.WordPressExploit.1

https://www.bleepingcomputer.com/news/security/new-linux-malware-uses-30-plugin-exploits-to-backdoor-wordpress-sites/

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

January 2, 2023 • 5:55 AM

More at www.hivepro.com