Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

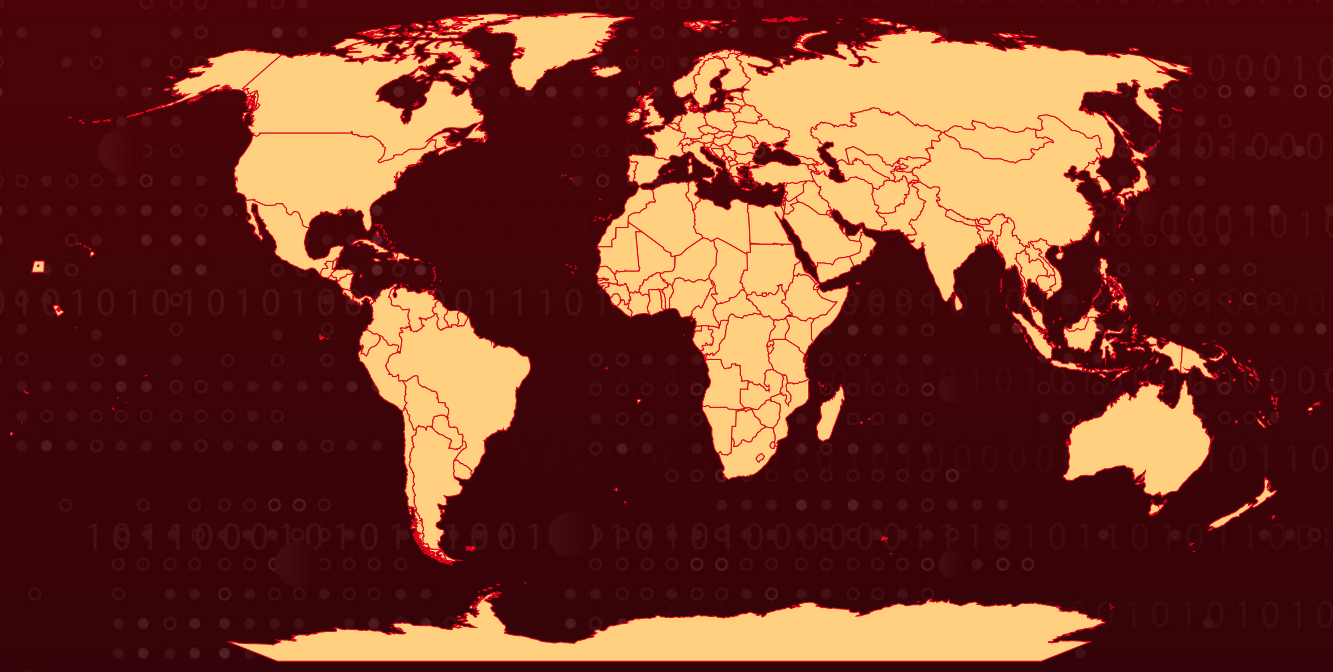
GitVenom Campaign Exploits GitHub to Target Crypto Users

Date of Publication	Admiralty Code	TA Number
February 27, 2025	A1	TA2025061

Summary

Active Since: 2023
Targeted Countries: Worldwide
Malware: AsyncRAT and Quasar RAT
Campaign Name: GitVenom
Targeted Industries: Cryptocurrency, Fintech, Gaming
Attack: The GitVenom campaign spreads malware via fake GitHub repositories, targeting developers and cryptocurrency users worldwide. Attackers hide malicious code in projects like automation tools, crypto bots, and game cheats. The malware deploys Node.js Stealer, AsyncRAT, Quasar RAT, and clipboard hijackers to steal credentials and funds. Notably, the attackers' Bitcoin wallet received nearly 5 BTC (around $485,000) in November 2024 alone. To prevent infection, users should verify repositories, inspect code, and use security tools.

Attack Regions



Attack Details

#1 The GitVenom campaign is a sophisticated malware operation that spreads malware through fake GitHub repositories, primarily targeting developers and cryptocurrency users. Active for at least two years, the campaign has impacted users globally, with a significant focus on Russia, Brazil, and Turkey.

#2 Attackers create seemingly legitimate repositories hosting automation tools, cryptocurrency bots, and game cheats to lure victims into downloading and executing malicious code. To enhance credibility, these repositories often include AI-generated README files and artificially inflated activity, tricking users into trusting and running harmful scripts.

#3 Once executed, the malware deploys different payloads depending on the programming language. Python projects use obfuscated scripts to decrypt and run additional malicious code, while JavaScript repositories rely on Base64-encoded scripts to trigger harmful functions. In C, C++, and C# projects, attackers embed malicious batch scripts within Visual Studio files that automatically execute during the build process.

#4 The GitVenom campaign employs multiple malware strains to compromise victims. The Node.js Stealer extracts sensitive data such as credentials, cryptocurrency wallets, and browser history, sending the stolen data via Telegram. Additionally, AsyncRAT and Quasar RAT allow attackers to gain remote control over infected devices, while a clipboard hijacker monitors copied cryptocurrency wallet addresses and replaces them with attacker-controlled ones, resulting in financial theft. Notably, the attackers' Bitcoin wallet received nearly 5 BTC (around $485,000) in November 2024 alone.

#5 Recent GitHub threats underscore serious vulnerabilities. A fake LDAPNightmare exploit for CVE-2024-49113 tricked users into running a malicious 'poc.exe' that exfiltrated sensitive data via FTP. Additionally, a flaw in Microsoft Copilot and Bing's caching exposed over 20,000 private repositories from major companies like Google, IBM, and PayPal, enabling unauthorized access.

#6 These incidents highlight the risks associated with blindly trusting open-source code from platforms like GitHub and underscore the importance of rigorous code inspection, regular security reviews, and robust repository verification to protect against evolving cyber threats.

Recommendations

- **Verify Code Sources:** Thoroughly inspect and validate the authenticity of third-party code before integrating or executing it in your environment.
- **Review Code Content:** Examine the code for any malicious or obfuscated segments that could indicate harmful intent.
- **Monitor Repository Activity:** Be cautious of repositories with unnatural activity patterns, such as frequent, non-substantive commits.
- **Utilize Security Tools:** Deploy endpoint protection, malware scanners, and behavior analysis tools to detect and block malicious scripts.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0009 Collection	TA0010 Exfiltration	TA0007 Discovery
TA0006 Credential Access	TA0002 Execution	TA0040 Impact	TA0005 Defense Evasion
TA0003 Persistence	T1204 User Execution	T1204.002 Malicious File	T1189 Drive-by Compromise
T1059.003 Windows Command Shell	T1027 Obfuscated Files or Information	T1036.005 Match Legitimate Name or Location	T1036 Masquerading
T1059 Command and Scripting Interpreter	T1555 Credentials from Password Stores	T1083 File and Directory Discovery	T1041 Exfiltration Over C2 Channel
T1560.001 Archive via Utility	T1560 Archive Collected Data	T1115 Clipboard Data	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	06d0d13a4ce73775cf94a4a4f2314490de1d5b9af12db8ba9b01cd14222a2756, bd44a831ecf463756e106668ac877c6b66a2c0b954d13d6f311800e75e9c6678
MD5	63739e000601afde38570bfb9c8ba589, 3684907e595cd04bf30b27d21580a7c6

References

https://securelist.com/gitvenom-campaign/115694/

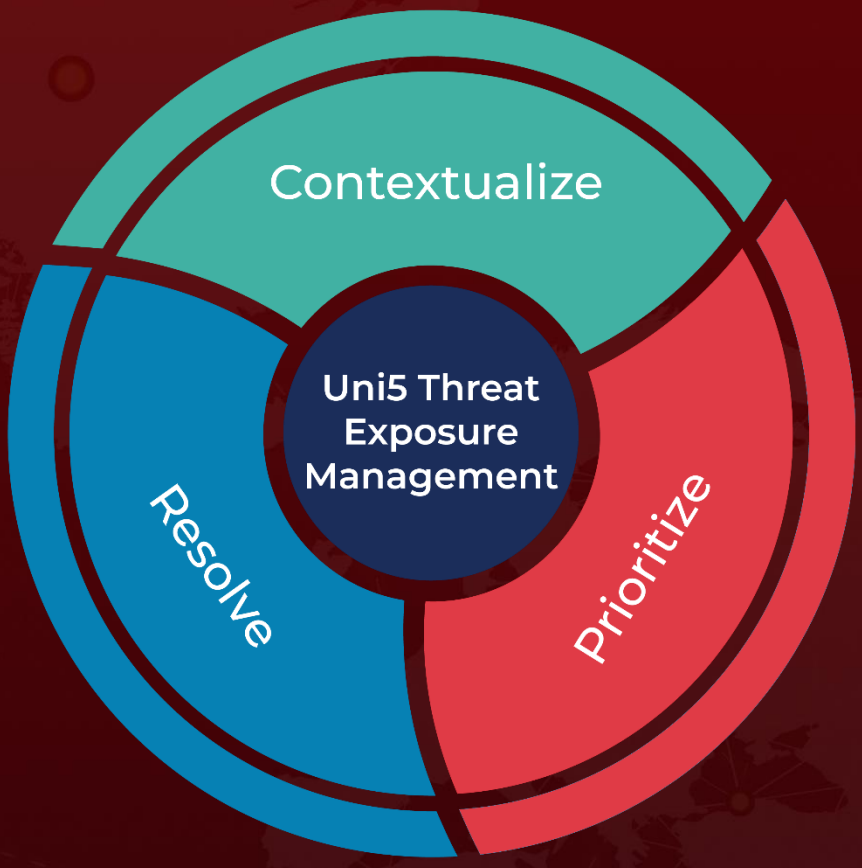
https://hivepro.com/threat-advisory/fake-ldapnightmare-exploit-on-github-spreads-infostealer-malware/

https://techcrunch.com/2025/02/26/thousands-of-exposed-github-repositories-now-private-can-still-be-accessed-through-copilot/?utm_source=chatgpt.com

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

February 27, 2025 • 7:30 PM

More at www.hivepro.com