Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

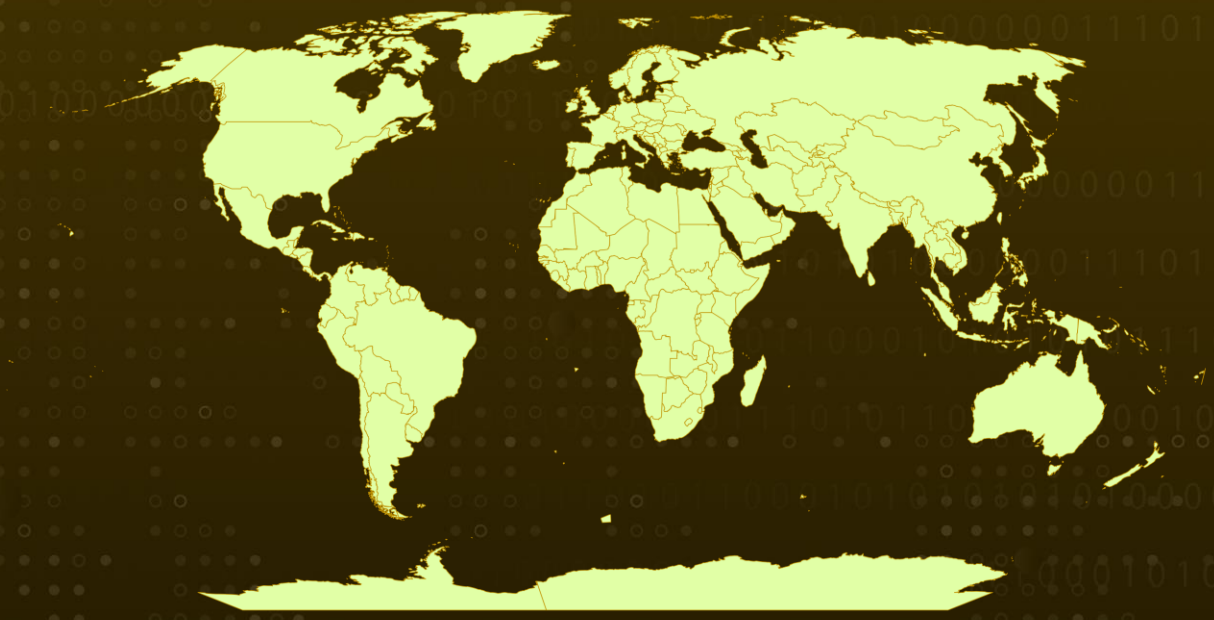
Deceptive WinRAR PoC Released on GitHub Drops VenomRAT

Date of Publication	Admiralty Code	TA Number
September 21, 2023	A1	TA2023381

Summary

Attack Began: August 21, 2023
Malware: VenomRAT
Attack Region: Worldwide
Attack: A hacker is disseminating a counterfeit proof-of-concept (PoC) exploit for a WinRAR vulnerability that was recently patched on GitHub, with the intention of infecting those who download it with the VenomRAT malware.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-25157	GeoServer SQL Injection Vulnerability	GeoServer	✗	✗	✓
CVE-2023-40477	WinRAR Remote Code Execution Vulnerability	WinRAR: 6.00 - 6.22 beta 1	✗	✗	✓

Attack Details

#1 A malicious threat actor distributed a fake proof-of-concept (PoC) via GitHub, claiming to exploit a recently revealed Remote Code Execution (RCE) vulnerability in WinRAR, which is identified as CVE-2023-40477. Their objective was to compromise users who downloaded this code by introducing the Venom RAT malware. It's crucial to underscore that this PoC is counterfeit and incapable of exploiting the intended vulnerability; rather, it is based on publicly available PoC code related to a GeoServer vulnerability documented under CVE-2023-25157.

#2 This deceptive PoC is a Python script contained within a ZIP archive named CVE-2023-40477-main.zip, specifically labeled as poc.py. Upon execution, instead of triggering an exploit, the PoC generates a batch script. This batch script, in turn, retrieves an encoded PowerShell script and proceeds to execute it on the host system.

#3 The purpose of this PowerShell script is to download the VenomRAT malware and establish a scheduled task to run it every three minutes. Once VenomRAT gains a foothold on a Windows device, it activates a keylogger, capturing and storing all keystrokes in a locally saved text file. The VenomRAT client implicated in this incident begins logging keystrokes, with the captured keystrokes saved in %APPDATA%\MyData\DataLogs_keylog_offline.txt.

#4 Subsequently, the client establishes communication with its Command and Control (C2) server, processing the server's commands as they are received. Although the attack has now ceased, it serves as a clear reminder of the inherent risks associated with obtaining PoCs from GitHub and executing them without conducting a comprehensive assessment to ensure their security.

Recommendations

Exercise Caution with GitHub PoCs: Exercise extreme caution when sourcing Proof-of-Concept (PoC) code from GitHub or any other platform. Always verify the credibility and reputation of the source, and thoroughly review the code for potential malicious intent before execution.

Vet Untrusted Code: Before executing any code, whether it's a PoC or not, conduct a thorough security assessment. Analyze the code to identify potential threats, vulnerabilities, or malicious behavior. If possible, use sandboxed environments for initial testing.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as frequent and unusual execution of reconnaissance commands.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**T1059** Command and Scripting Interpreter	**T1010** Application Window Discovery
T1059.001 PowerShell	**T1140** Deobfuscate/Decode Files or Information	**T1497** Virtualization/Sandbox Evasion	**T1083** File and Directory Discovery
T1018 Remote System Discovery	**T1057** Process Discovery	**T1082** System Information Discovery	**T1056.001** Keylogging
T1071 Application Layer Protocol	**T1105** Ingress Tool Transfer		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	baiwu123.e2.luyouxia[.]net, 123zhang123.e1.luyouxia[.]net, 7706d61f16.zicp[.]fun, s1567749.e1.luyouxia[.]net, binzai.e3.luyouxia[.]net, 7706d61f16.zicp[.]fun, yk.tym[.]pw, bj-1.lcf[.]icu, bj-1.lcf[.]icu

TYPE	VALUE
SHA256	61dd71441a2b4955467243e986c38f1ea543bae7b1546f003c4a30074dd6c04e, cabc45f1dab04be3fc63192d98324d2665599a6d6ea2f0277ecd27a62fb694f3, 79b87d7accc9cbd1414b72ca13c48a385be9cb06c1bb53d845e94107b579bf62, 4b84283c40560991da34ef2b465a4724facd0932acebff60466d8d5ff1916bd5, 75c12ccacd764101736b213981355b39056227929214c8963e9bf3ea5a60f6ef, 1648bea3c1c3b00e7f9c9bf7f65be833fa7f291f0e05a342382e9e36f0350c60, b23e4ea87917a517565de8471a101ab55c2a31186c8a23e9e8af71b359d35aa9, 65235e5bd2f9b30e2b272602a83a8f3805cfca50252da8a79e279f232a6d3990, ecc3971af558300b451a87b51d0324737174ea1993d8aa7424078fb1bd97ffb3, f9497f07d69b043501cc52bf2db7828abad35a14bd95bb05e6b5ab9e4408de4e, 48f61821feeaa45c53daaeb567e142ce9614d131dcf886506a31bf0ba2d75c45, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, d0e7f2c67877f06c0e8854b1a37f6f04d181537d77e242f46401415da17f9b03, 8ef5c7eaa352e547c2e0de266844122ab471cd2ac73a9388b4f1416b2ac8c840, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, a9e8b6b187c3bbfccfec6266b95c079bf27752d22bcd04c97df8a62f4a6dcd59, 4c69911de167a507a1c6effb9724ab72ca0026d1fdfa9c747f70800abdbcbbe5, a45f92a6de5f22b3d360d79721345fc7410467f8472fcf1e8e9b5b0ca8099a3f, a45f92a6de5f22b3d360d79721345fc7410467f8472fcf1e8e9b5b0ca8099a3f

TYPE	VALUE
IPv4:PORT	20.195.166[.]5:30120, 193.161.193[.]99:27573, 3.127.59[.]75:11670, 3.127.59[.]75:4824, 91.137.64[.]248:19102, 196.115.8[.]54:1288, 109.123.237[.]143:4449, 109.123.237[.]143:2247, 213.52.130[.]95:9200, 213.52.130[.]95:1337, 121.127.233[.]181:4449, 121.127.233[.]181:4449, 146.90.154[.]118:4449, 43.205.210[.]118:4449, 185.106.94[.]165:4449, 185.106.94[.]165:2323, 91.192.100[.]61:4449, 91.192.100[.]61:2323, 20.150.193[.]28:4449, 5.230.54[.]132:4449, 185.221.67[.]43:4449, 185.221.67[.]43:4449, 121.127.233[.]181:4449, 193.161.193[.]99:1194, 193.161.193[.]99:27573, 93.82.44[.]26:4040, 45.123.56[.]33:4449, 147.185.221[.]16:10735, 146.70.50[.]106:3222, 36.73.32[.]123:4449, 95.214.26[.]78:5566

Patch Links

https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d

https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

References

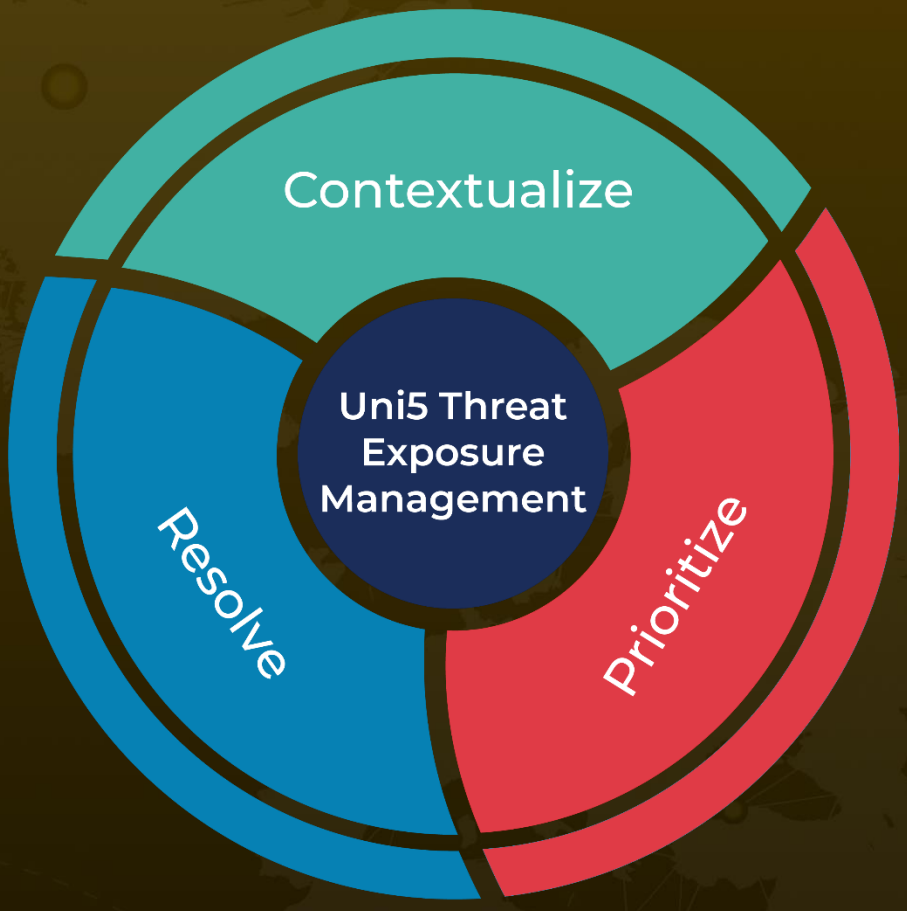
https://unit42.paloaltonetworks.com/fake-cve-2023-40477-poc-hides-venomrat/

https://github.com/pan-unit42/iocs/blob/master/venomrat_iocs.csv

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

September 21, 2023 . 8:30 AM

More at www.hivepro.com