Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

A New Face of AsyncRAT Utilizes WSF Scripts to Spread

Date of Publication	Admiralty Code	TA Number
December 7, 2023	A1	TA2023492

Summary

First appeared: 2019
Attack Region: Worldwide
Targeted Industry: Government, Aerospace, Hospitality, IT, Business services, Transportation, and Telecommunications
Malware : AsyncRAT
Affected Platform : Windows
Attack: AsyncRAT is a remote access trojan (RAT) malware known for stealing credentials and executing various malicious activities since 2019. Its recent variant, distributed through WSF script files, employs sophisticated fileless techniques, emphasizing the importance of user caution and robust security measures.

Attack Regions

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

Attack Details

#1 AsyncRAT is a remote access trojan (RAT) malware that has been a significant threat since 2019. Known for its diverse capabilities, AsyncRAT is designed to steal credentials, execute various forms of malware, and compromise system security. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system. The potential impacts of AsyncRAT include data theft, ransomware attacks, denial-of-service attacks, and the installation of additional malicious software.

#2 The malware commonly spreads through malicious email attachments, phishing scams, infected websites, and may be bundled with cracked software and pirated games. A notable variant of AsyncRAT is distributed through WSF script files, diverging from its previous distribution method using .chm files. This variant is concealed within compressed (.zip) files linked in emails, demonstrating a sophisticated approach to propagation.

#3 The attack flow of AsyncRAT involves a series of files being executed, including Error.vbs, Error.bat, Error.ps1, pwng.bat, and pwng.ps1. This execution leads to the activation of AsyncRAT, displaying persistence through scheduled tasks, registry entries, and self-executing bat files. The malware exfiltrates a wide range of information, such as system details, browser user data, and cryptocurrency wallet information.

#4 Exfiltrated data is encrypted and sent to a Command and Control (C2) server, with threat actors using multiple connection attempts on different port numbers to enhance detection evasion. The distribution method employs sophisticated fileless techniques, underscoring the importance of user caution when handling email attachments or links. The use of security monitoring features is crucial for identifying and restricting access from threat actors associated with AsyncRAT.

Recommendations

Email Security: Deploy robust email filtering solutions to detect and block malicious attachments and phishing attempts. Implement email authentication mechanisms (SPF, DKIM, DMARC) to prevent email spoofing and phishing.

Endpoint Protection: Utilize reputable antivirus and anti-malware solutions for early detection and removal of AsyncRAT and similar threats. Keep endpoint protection software up-to-date to recognize and mitigate the latest malware variants.

Software and System Updates: Regularly update operating systems, software, and applications to patch vulnerabilities. Implement automatic updates to ensure timely patching and security improvements.

User Privileges and Access Controls: Follow the principle of least privilege, granting users the minimum necessary access. Implement strong authentication mechanisms and enforce complex password policies.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0043 Reconnaissance
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0011 Command and Control
TA0009 Collection	TA0006 Credential Access	T1055 Process Injection	T1041 Exfiltration Over C2 Channel
T1566.002 Spearphishing Link	T1566 Phishing	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1566.001 Spearphishing Attachment	T1056.001 Keylogging
T1560 Archive Collected Data	T1056 Input Capture	T1059.001 PowerShell	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185[.]81[.]157[.]242
SHA1	316b99a2bf664ccd94eb050005975c52806d2163, 3b10e9a10fc90e2a0a28f13a84c9b58eeb382dfc, 921bd5cb08b5c6a77a28e2864417bb8cdefafbf0
Hostname	drippmedsot[.]mywire[.]org
SHA256	621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c, 70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75, a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387
MD5	0a80a592d407a2a8b8b318286dc30769, 61b7507a6814e81cda6b57850f9f31da, 750dc2354b0454eafd66900687a0f7d6, 790562cefbb2c6b9d890b6d2b4adc548, A31191ca8fe50b0a70eb48b82c4d6f39, Ac12d457d3ee177af8824cdc1de47f2a, B98e76816350a6a527fc311dae62b85e, c09266666ee71ade24e0e5f889cc8199

References

https://asec.ahnlab.com/en/59573/

https://asec.ahnlab.com/en/47525/

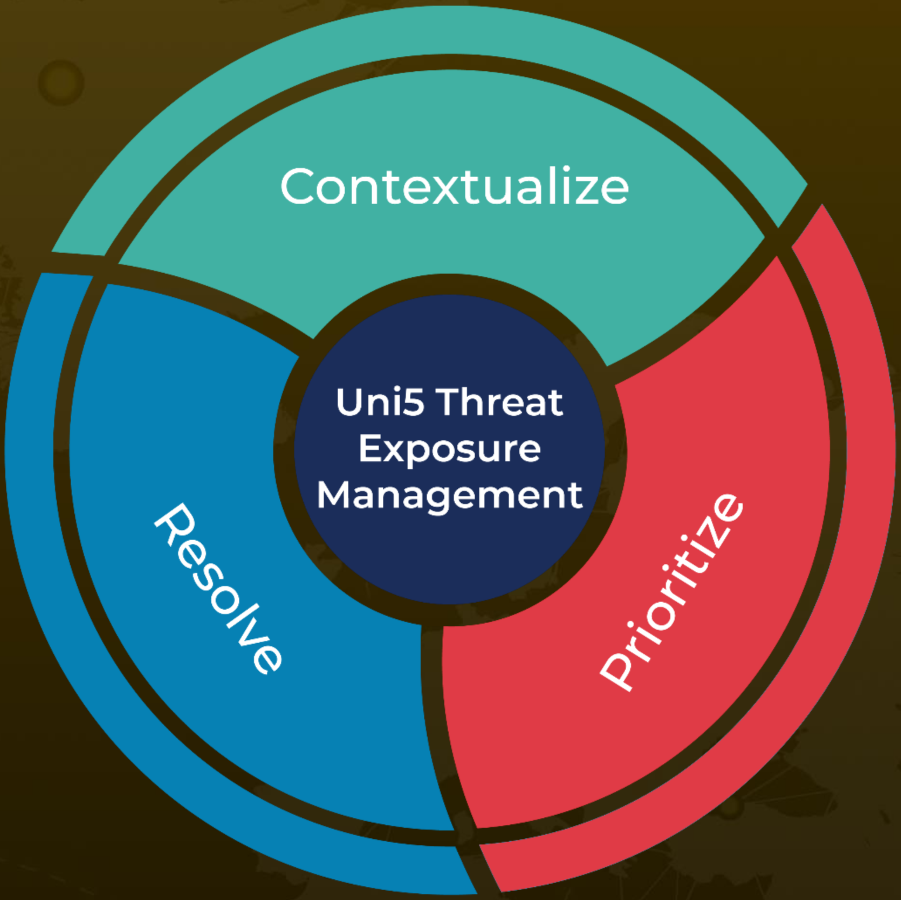
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/asyncrat#how-it-works

https://attack.mitre.org/software/S1087/

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 7, 2023 • 4:30 AM

More at www.hivepro.com