Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

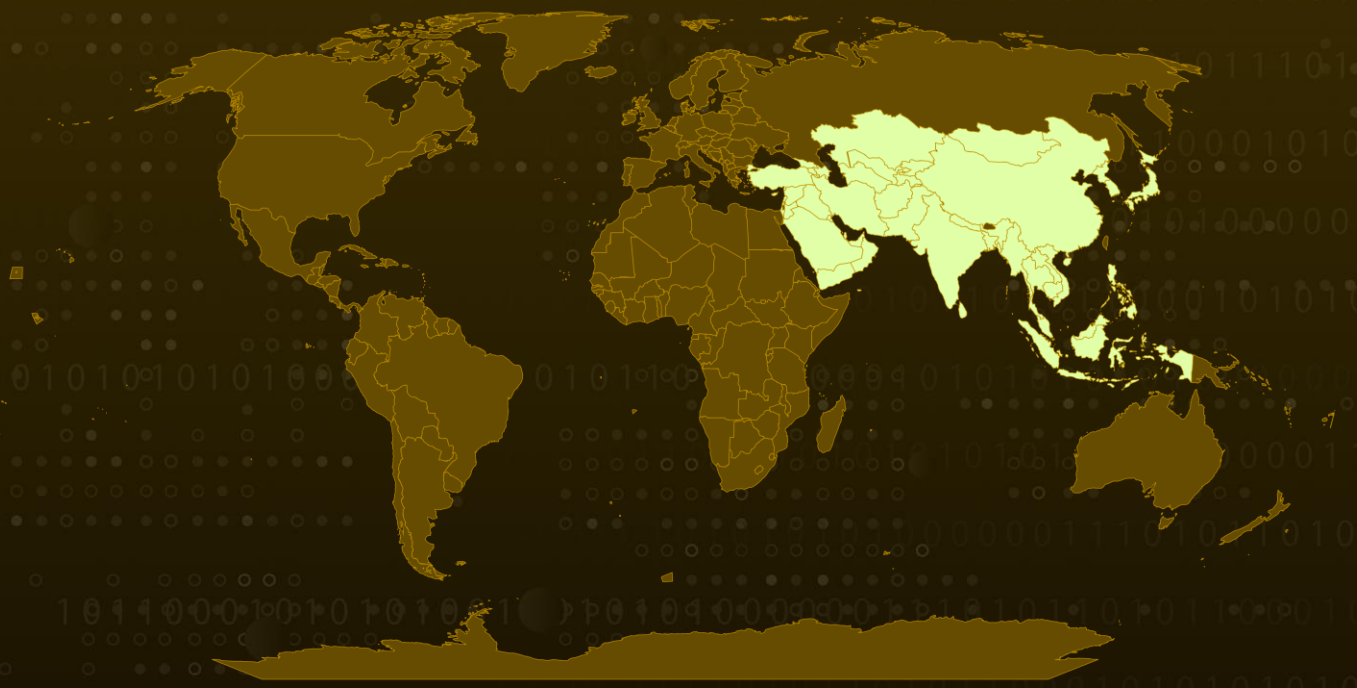
WogRAT Backdoor Poses Risk to Windows and Linux Users

Date of Publication	Admiralty Code	TA Number
March 7, 2024	A1	TA2024089

Summary

Attack Began: February 25, 2024
Targeted Region: Asia
Malware: WogRAT
Affected Platform: Windows, Linux
Attack: WogRAT, a backdoor malware targeting both Windows and Linux, spreads through aNotepad, an online notepad service. It disguises itself as system tools to trick users into downloading it, mainly targeting users in Asia. Users are cautioned to download software from official sources and update antivirus to thwart WogRAT infections.

Attack Regions



Attack Details

#1 WogRAT is a backdoor malware that can be used by attackers to gain remote access to a victim's computer. WogRAT has been in use since at least late 2022. The malware is distributed through a free online notepad platform called aNotepad. This malware targets both Windows and Linux systems, with different distribution methods and functionalities. In the case of Windows, the malware disguises itself as legitimate utility tools, whereas in Linux, it changes its name to mimic a legitimate process to avoid detection.

#2 WogRAT for Windows operates by downloading encrypted strings from aNotepad, decrypting them, and loading a backdoor malware called WingsOfGod. It collects system information and communicates with a Command and Control (C&C) server, allowing for command execution, file downloading/uploading, and more.

#3 The Linux version of WogRAT, shares similarities with the Windows version. It receives commands via a reverse shell from a server controlled by the threat actor, employing Tiny SHell's routines. Communication with the C&C server is encrypted using AES-128 keys generated from HMAC SHA1 algorithms.

#4 To avoid WogRAT infections, users are advised to download software from official sources and keep antivirus software updated. Vigilance is crucial, especially when downloading executables from file-sharing platforms.

Recommendations

Exercise Caution with Downloads: Users should exercise caution when downloading files, especially from untrusted sources or file-sharing sites. It's crucial to verify the authenticity of the source before downloading any software or files.

Download from Official Websites: Whenever possible, download software and applications from official websites or trusted repositories. Avoid downloading executable files from unfamiliar or suspicious websites to minimize the risk of downloading malware.

Keep Software Updated: Regularly update your operating system, antivirus software, and other applications to the latest versions. Software updates often include security patches that protect against known vulnerabilities exploited by malware like WogRAT.

Behavior-Based Detection: Employ behavior-based detection techniques to identify and block unusual or suspicious activity on endpoints and network devices. Monitor for signs of unauthorized access, data exfiltration, or abnormal system behavior that may indicate the presence of WogRAT or similar threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0011** Command and Control	**TA0009** Collection
TA0007 Discovery	**TA0005** Defense Evasion	**TA0010** Exfiltration	**T1071.002** File Transfer Protocols
T1036 Masquerading	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1059** Command and Scripting Interpreter
T1082 System Information Discovery	**T1071.001** Web Protocols	**T1573.002** Asymmetric Cryptography	**T1573** Encrypted Channel
T1041 Exfiltration Over C2 Channel	**T1132.001** Standard Encoding	**T1132** Data Encoding	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	w.linuxwork[.]net, linuxwork[.]net
MD5	290789ea9d99813a07294ac848f808c9, 1aebf536268a9ed43b9c2a68281f0455, 194112c60cb936ed1c195b98142ff49d, 1341e507f31fb247c07beeb14f583f4f, fff21684df37fa7203ebe3116e5301c1, f97fa0eb03952cd58195a224d48f1124, f271e0ae24a9751f84c5ae02d29f4f0e, e9ac99f98e8fbd69794a9f3c5afdcb52, da3588a9bd8f4b81c9ab6a46e9cddedd, a35c6fbe8985d67a69c918edcb89827e, 929b8f0bdbb2a061e4cf2ce03d0bbc4c, 7bcfea3889f07f1d8261213a77110091, 655b3449574550e073e93ba694981ef4, 5769d2f0209708b4df05aec89e841f31, 3669959fdb0f83239dba1a2068ba25b3
URLs	hxxps://t0rguard[.]net/c/, hxxps://w.newujs[.]com/c/, hxxps://newujs[.]com/tt.php?fuckyou=1, hxxp://newujs[.]com/dddddd_oo, hxxp://newujs[.]com/abc, hxxp://newujs[.]com/a14407a2, hxxps://js.domaiso[.]com/jquery.min-2.js, hxxps://jp.anotepad[.]com/note/read/b896abi9, hxxp://newujs[.]com/cff/wins.jpg

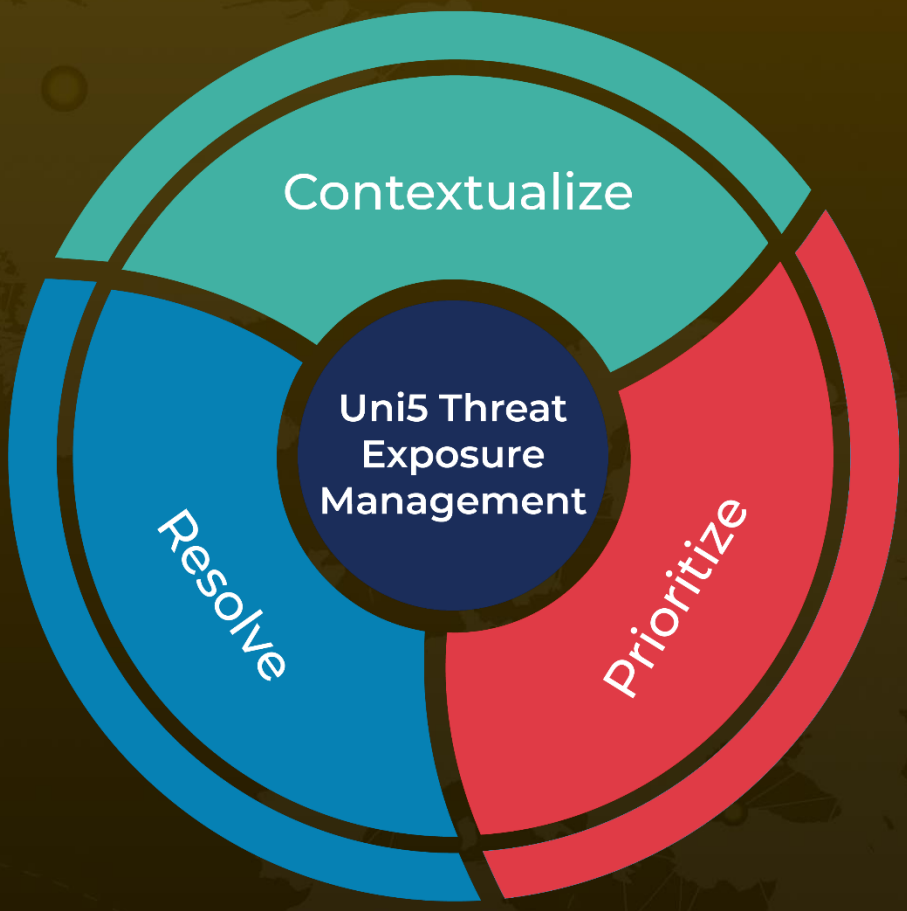
References

https://asec.ahnlab.com/en/62446/

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

March 7, 2024 • 2:30 AM

More at www.hivepro.com