Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

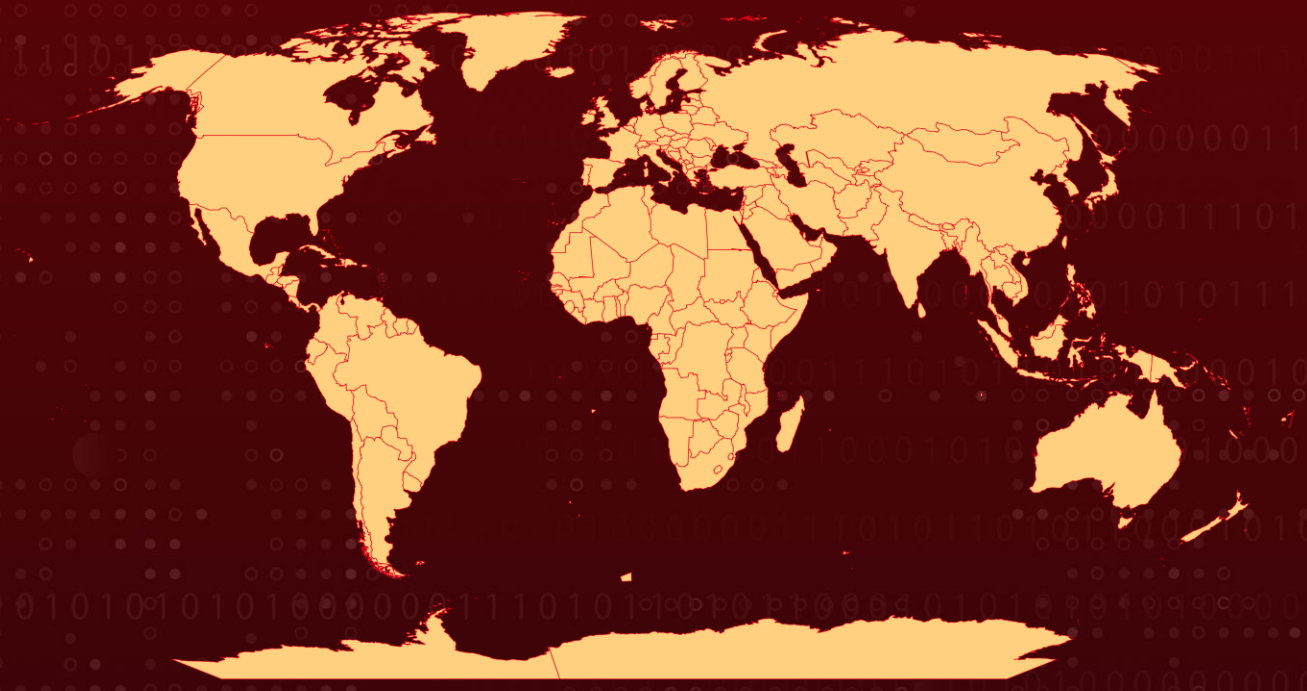
Multiple State-Sponsored Groups Exploit WinRAR Vulnerability in Phishing Attacks

Date of Publication	Last updated date	Admiralty Code	TA Number
October 18, 2023	October 19, 2023	A1	TA2023422

Summary

First Appearance: October 12, 2023
Attack Region: Worldwide
Affected Platforms: Windows
Malware: SmokeLoader, Nanocore RAT, Crimson RAT, AgentTesla, BOXRAT and Rhadamanthys infostealer
Attack: Multiple state-sponsored groups conduct phishing attacks, exploiting a WinRAR vulnerability to steal data, including browser credentials via PowerShell commands, and exfiltrating it through a legitimate service. Despite a patch being available, the widespread exploitation of the WinRAR flaw underscores the effectiveness of known vulnerability exploits.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR	✓	✓	✓

Attack Details

#1 A series of phishing attacks, attributed to a Russia-linked nation-state threat actor, exploit a recently discovered vulnerability (CVE-2023-38831) in WinRAR compression software using malicious archive files. The attack commences with a bait file, a PDF document inside the archive, displaying Indicator of Compromise (IoCs) related to various malware, including SmokeLoader, Nanocore RAT, Crimson RAT, and AgentTesla.

#2 Clicking the PDF initiates a BAT script, running PowerShell commands to establish a reverse shell, granting the attacker access to the victim's system. A separate PowerShell script is employed to extract data, including login credentials, from Google Chrome and Microsoft Edge browsers, with data exfiltrated via the legitimate service webhook[.]site.

#3 The lure file masquerades as an archive named "IOC_09_11.rar," designed to resemble a file for sharing IoCs. It exploits the WinRAR vulnerability and includes a bogus PDF file and a BAT script. The BAT script exploits the WinRAR vulnerability to extract content to the %TEMP% directory and execute the PDF, triggering malicious activity.

#4 The first PowerShell command generates a Private RSA Key in the %LOCALAPPDATA%\Temp directory, used by the second command to open a reverse shell, providing the attacker access via the SSH tool on TCP port 443 at a specific IP address. The third PowerShell command decrypts data, including login credentials from the victim's Chrome and Edge browsers, sent to the threat actor via webhook[.]site.

#5 Multiple state sponsored actors have been observed exploiting CVE-2023-38831, including APT 28, DarkPink, Konni, APT 40, Sandworm and APT 29. DarkPink has utilized this WinRAR 0-day vulnerability to target entities in Vietnam and Malaysia.

#6 In a September attack, Russian Sandworm hackers distributed Rhadamanthys infostealer malware via phishing attack exploiting CVE-2023-38831 with fake invitations to join a Ukrainian drone training school.

#7 APT28 targeted Ukrainian users with CVE-2023-38831 exploits hosted on servers from a free hosting provider, using a malicious PowerShell script (IRONJAW) to steal browser credentials.

#8 Additionally, APT40, a Chinese hacking group, exploited the WinRAR vulnerability in attacks against targets in Papua New Guinea, employing ISLANDSTAGER and BOXRAT for establishing persistence on compromised systems.

Recommendations

Patch or Update WinRAR: Ensure that all instances of WinRAR in your organization are updated to versions 6.23 or higher to address the CVE-2023-38831 vulnerability. Regularly check for updates and automate the patching process where possible.

Email Filtering and Scanning: Implement advanced email filtering and scanning solutions to detect and block phishing emails before they reach users' inboxes. These solutions should identify suspicious attachments and archive files.

Endpoint Security: Use endpoint security solutions that can detect and block malicious scripts, such as the PowerShell commands used in these attacks. Employ heuristic analysis to catch new or unknown threats.

Security Awareness Training: Provide security awareness training to employees to help them recognize phishing attempts, especially those involving PDF files within archives. Encourage them to be cautious when clicking on email attachments, even from seemingly trusted sources.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0001** Initial Access	**TA0011** Command and Control	**TA0007** Discovery
TA0005 Defense Evasion	**TA0010** Exfiltration	**TA0009** Collection	**TA0006** Credential Access
T1555.003 Credentials from Web Browsers	**T1555** Credentials from Password Stores	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1566 Phishing	**T1567** Exfiltration Over Web Service	**T1036** Masquerading	**T1027** Obfuscated Files or Information
T1070.004 File Deletion	**T1070** Indicator Removal	**T1104** Multi-Stage Channels	**T1140** Deobfuscate/Decode Files or Information
T1566.001 Spearphishing Attachment	**T1059.003** Windows Command Shell	**T1204.002** Malicious File	**T1082** System Information Discovery
T1005 Data from Local System	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol	**T1102** Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	91dec1160f3185cec4cb70fee0037ce3a62497e830330e9ddc2898f45682f63a, 072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7, 77cf5efde721c1ff598eeae5cb3d81015d45a74d9ed885ba48330f37673bc799
SHA1	Bd44774417ba5342d30a610303cde6c2f6a54f64, 9e630c9879e62dc801ac01af926fbc6d372c8416
MD5	9af76e61525fe6c89fe929ac5792ab62, 89939a43c56fe4ce28936ee76a71ccb0, 1536e9bf086982c072c2cba7d42b0a62
IPv4	216.66.35[.]145
URL	http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611, https://filetransfer[.]io/data-package/DVagoJxL/download, https://fex[.]net/s/bttyrz4, https://fex[.]net/s/59znp5b
Domain	webhook[.]site, ske9dhn.c1[.]biz, e9f0dkd.c1[.]biz

Patch Details

Update WinRAR version to 6.23 or later versions

Link:

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

References

https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack

https://nsfocusglobal.com/apt-group-darkpink-exploits-winrar-0-day-to-target-multiple-entities-in-vietnam-and-malaysia/

https://cybermaterial.com/pro-russian-hackers-exploit-winrar-flaw/

https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing

https://www.hivepro.com/winrar-zero-day-exploit-targeting-traders-since-april/

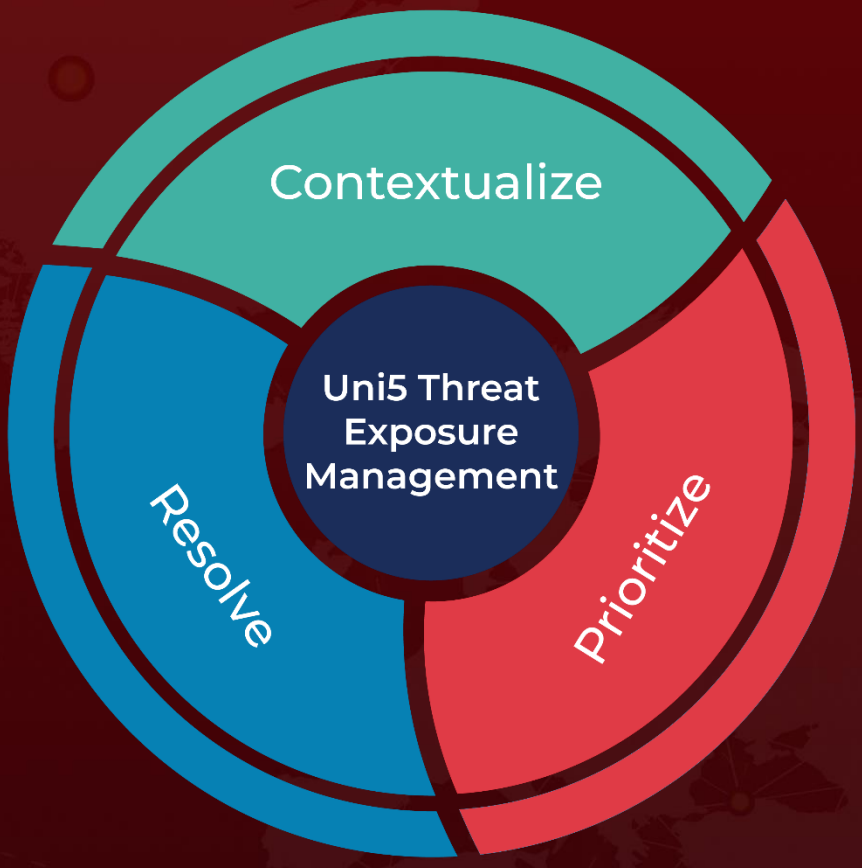
https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/

https://medium.com/@knownsec404team/konni-apt-exploits-winrar-vulnerability-cve-2023-38831-targeting-the-cryptocurrency-industry-d97f6ea7d584

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

October 18, 2023 . 5:30 AM

More at www.hivepro.com