Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Zero-day vulnerability leveraged to deploy Cuba Ransomware

Date of Publication	Admiralty Code	TA Number
August 11, 2022	A1	TA2022169

Summary

The threat actors behind the Cuba ransomware have stepped up their game by using a new Remote Access Trojan called ROMCOM and weaponizing a local privilege escalation vulnerability(CVE-2022-24521). A wide range of industries was targeted, including professional and legal services and state and local government.

CVE Table

CVE	NAME	PATCH
CVE-2022-24521	Privilege escalation in Microsoft Windows common log file system driver	✓
CVE-2020-1472	Netlogon Elevation of Privilege Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0002 Execution	**T1059** Command and Scripting Interpreter	**T1106** Native API	**TA0004** Privilege Escalation
T1546 Event Triggered Execution	**TA0009** Collection	**T1113** Screen Capture	**TA0005** Defense Evasion
T1218 System Binary Proxy Execution	**T1027** Obfuscated Files or Information	**TA0011** Command and Control	**T1095** Non-Application Layer Protocol
TA0001 Initial Access	**T1566** Phishing	**TA0007** Discovery	**T1057** Process Discovery
T1497 Virtualization/Sandbox Evasion	**TA0040** Impact	**T1486** Data Encrypted for Impact	**TA0006** Credential Access
T1003 OS Credential Dumping	**T1003.001** LSASS Memory		

Technical Details

#1 The conventional Cuba ransomware payload has primarily stayed constant since the operation's commenced in 2019. A new addition is the use of an expired legal NVIDIA certificate to certify a kernel driver that is dropped during the early stages of infection.

#2 The ransomware encrypts the file with ChaCha from the open source WolfSSL repository and RSA for key encryption. When a file is successfully encrypted, the extension .cuba is added to the filename.

#3 The adversary then transmits a local privilege escalation tool using an exploit for CVE-2022-24521, a bug in the Windows Common Log File System Driver that was resolved in April 2022 stating it to be zero-day.

#4 Cuba ransomware received a minor update in the ransom note by enabling communication via TOX due to its secure messaging feature. It was also discovered that the ZeroLogon hack tool was being utilized to get DA (domain administrator) permissions by exploiting CVE-2020-1472.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-24521	Windows: 7 - 11 21H2 and Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-119
CVE-2020-1472	Windows Server: 2008 R2 - 2019 2004	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	CWE-330

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	07905de4b4be02665e280a56678c7de67652aee318487a44055700396d37ecd0 af6561ad848aa1ba53c62a323de230b18cfd30d8795d4af36bf1ce6c28e3fd4e 24e018c8614c70c940c3b5fa8783cb2f67cb13f08112430a4d10013e0a324eaa ab5a3bbad1c4298bc287d0ac8c27790d68608393822da2365556ba99d52c5dfb 6866e82d0f6f6d8cf5a43d02ad523f377bb0b374d644d2f536ec7ec18fdaf576 3febf726ffb4f4a4186571d05359d2851e52d5612c5818b2b167160d367f722c 3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0 36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24 1450f7c85bfec4f5ba97bcec4249ae234158a0bf9a63310e3801a00d30d9abcc 0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf 0eff3e8fd31f553c45ab82cc5d88d0105626d0597afa5897e78ee5a7e34f71b3 a4665231bad14a2ac9f2e20a6385e1477c299d97768048cb3e9df6b45ae54eb8 cfe7b462a8224b2fbf2b246f05973662bdabc2c4e8f4728c9a1b977fac010c15 b5978cf7d0c275d09bedf09f07667e139ad7fed8f9e47742e08c914c5cf44a53 324ccd4bf70a66cc14b1c3746162b908a688b2b124ad9db029e5bd42197cfe99 3496e4861db584cc3239777e137f4022408fb6a7c63152c57e019cf610c8276e
Domains	CombinedResidency[.]org optasko[.]com

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

References

https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 11, 2022 • 4:07 AM

More at www.hivepro.com