Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Cephalus Ransomware a Wake-Up Call for Stronger Endpoint Defense

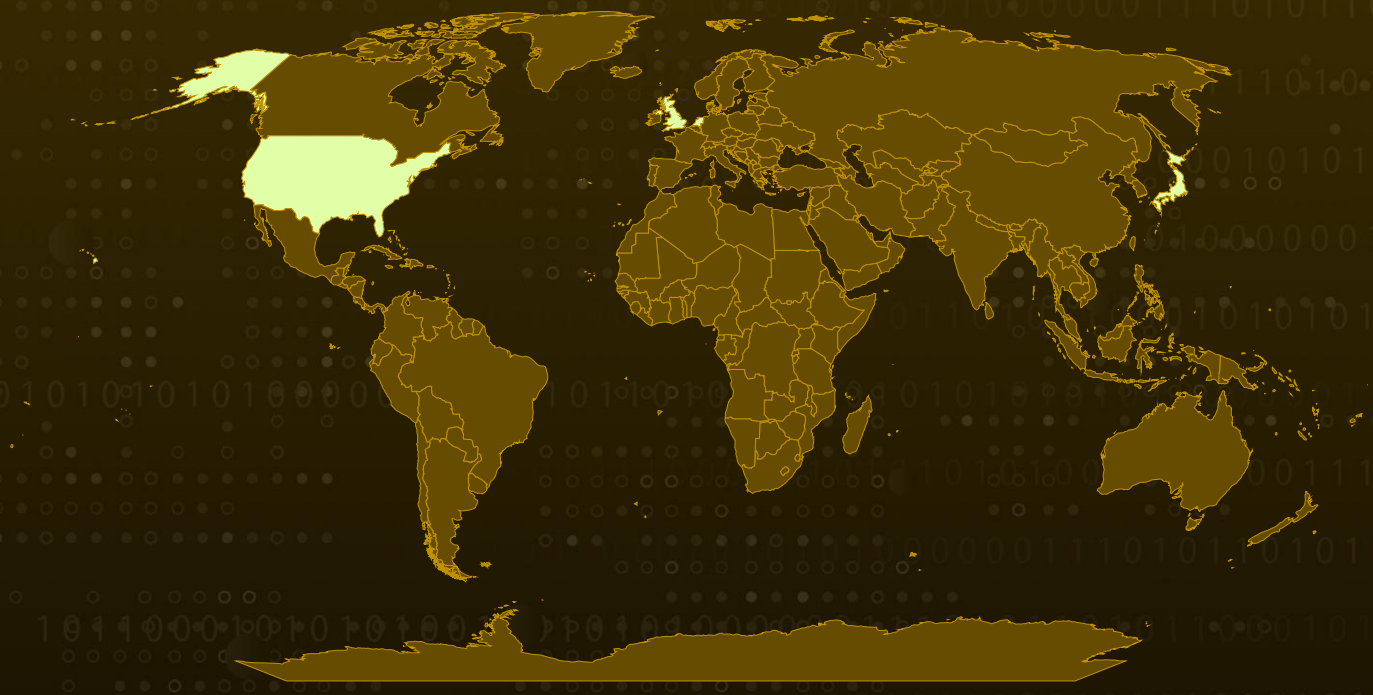
Date of Publication	Admiralty Code	TA Number
September 8, 2025	A1	TA2025272

Summary

Attack Commenced: August 2025
Malware: Cephalus Ransomware
Targeted Countries: United States, United Kingdom, Netherlands, Japan
Targeted Industries: Media, Technology, Aerospace, Defense, Real Estate, Business Services & Consulting, Legal, Financial Services, Healthcare, Architecture, Banking

Attack: In August 2025, the Cephalus ransomware emerged as a highly sophisticated cyber threat, targeting systems via Remote Desktop Protocol (RDP) by exploiting accounts lacking multi-factor authentication (MFA). Drawing its name from Greek mythology, Cephalus combines deception with technical finesse.

Attack Regions



Attack Details

#1 In August 2025, two ransomware incidents linked to Cephalus occurred on August 13 and August 16. The name Cephalus is derived from the Greek word for "head" and refers to a prominent figure in Greek mythology, underscoring its thematic significance.

#2 Cephalus ransomware gains initial access through Remote Desktop Protocol (RDP) by exploiting compromised accounts that lack multi-factor authentication (MFA). A notable characteristic of this ransomware is its deployment via DLL sideloading.

#3 Specifically, the legitimate SentinelOne executable is launched from the user's Downloads folder, subsequently loading SentinelAgentCore.dll, which in turn loads data.bin. Upon execution, the ransomware initiates a series of embedded commands designed to prevent system recovery.

#4 Cephalus begins by silently deleting all existing Volume Shadow Copies, followed by multiple PowerShell commands that create Windows Defender exclusions, modify the registry to disable Defender functionality, and stop related services. Encrypted files are renamed with a .sss extension, and a ransom note titled "recover.txt" is distributed across multiple directories.

#5 For data exfiltration, attackers utilize the MEGA cloud storage platform. Another distinguishing feature of the Cephalus ransom note is the inclusion of links to two online articles detailing past successful deployments of the ransomware, seemingly to validate their claims of data theft and create a heightened sense of urgency for victims to comply.

Recommendations

Enforce Multi-Factor Authentication (MFA) for All Remote Access: Cephalus ransomware exploits Remote Desktop Protocol (RDP) by targeting accounts without MFA. Implementing MFA adds an essential layer of protection, significantly reducing the risk of unauthorized access.

Limit and Monitor RDP Access: Restrict RDP access to only those users who need it and enforce strict monitoring. Disable unused remote access services and ensure all open ports are regularly scanned and secured.

Validate Executables and Application Behavior: Cephalus ransomware uses legitimate files, such as SentinelBrowserNativeHost.exe, to sideload malicious DLLs. Implement application allowlisting and behavioral monitoring to detect unusual file execution patterns and prevent abuse of trusted software.

Regularly Back Up Data and Secure Recovery Points: Since Cephalus deletes all Volume Shadow Copies to obstruct recovery, ensure that data backups are stored offline or in secure environments inaccessible to attackers. Regularly test restoration processes to confirm backup integrity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1036** Masquerading	**T1070.004** File Deletion
T1078 Valid Accounts	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol	**T1218** System Binary Proxy Execution
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1543** Create or Modify System Process	**T1562** Impair Defenses
T1562.002 Disable Windows Event Logging	**T1562.001** Disable or Modify Tools	**T1574** Hijack Execution Flow	**T1574.001** DLL

T1070 Indicator Removal	**T1070.001** Clear Windows Event Logs	**T1083** File and Directory Discovery	**T1012** Query Registry
T1005 Data from Local System	**T1560** Archive Collected Data	**T1560.001** Archive via Utility	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1567** Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage	**T1486** Data Encrypted for Impact
T1490 Inhibit System Recovery	**T1565** Data Manipulation	**T1491** Defacement	**T1112** Modify Registry

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	recover.txt, SentinelBrowserNativeHost.exe, SentinelAgentCore.dll, data.bin
File Path	C:\Users\[user]\Downloads
SHA256	0d9dfc113712054d8595b50975efd9c68f4cb8960eca010076b46d2fba3d2754, 82f5fb086d15a8079c79275c2d4a6152934e2dd61cc6a4976b492f74062773a7, b3e53168fc05aeedea828bd2042e2cc34bbf8193deadab9dd4aa507e5b9c045a, a34acd47127196ab867d572c2c6cf2fcccffa3a7a87e82d338a8efed898ca722, 91c459804dbf8739e2acbc6f13d8d324bceeed3f9a004f78d5475c717b04c8b5
Email	sadklajsdioqw[@]proton[.]me
Tox ID	91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
TOR Address	cephalus6oiypuwumqlwurvbmwsfglg424zjdmywfgqm4iehkqivsjyd[.]onion

Recent Breaches

https://shropdoc.org.uk/
https://coloradohealthnetwork.org/
https://lee-irvine.com/
https://system-exe.co.jp/
https://sskrplaw.com/
https://gmllp.com/
https://carestlhealth.org/

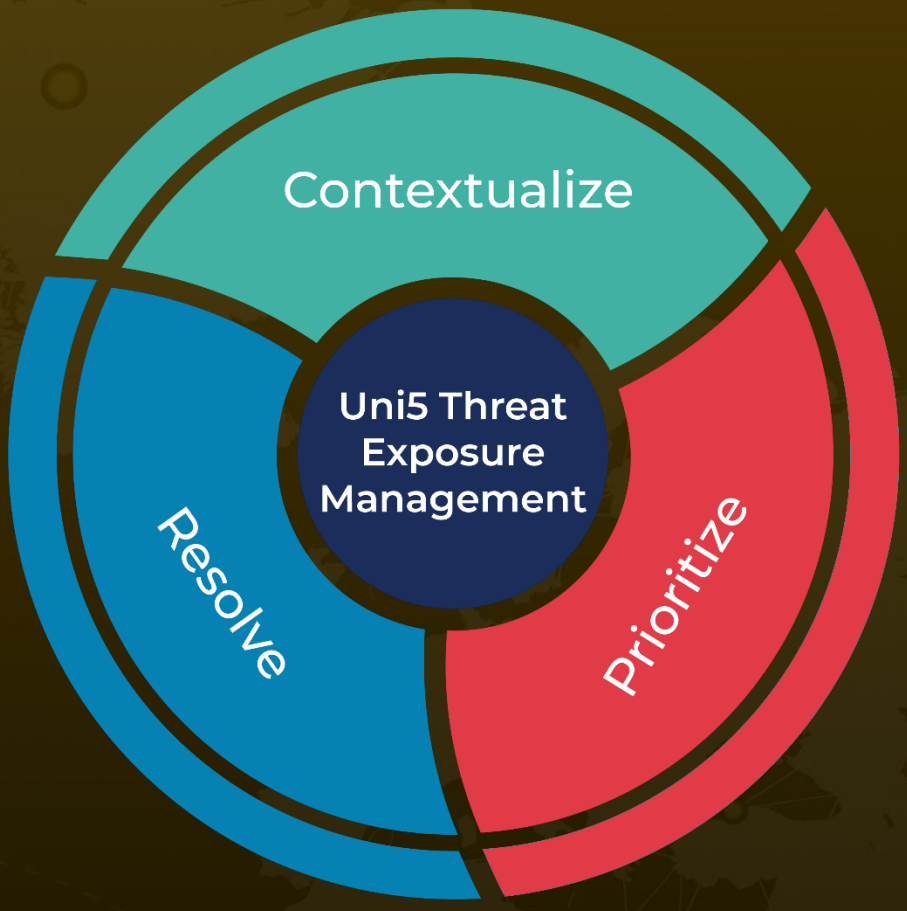
References

https://www.huntress.com/blog/cephalus-ransomware

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 8, 2025 . 6:00 AM

More at www.hivepro.com