Date of Publication
September 15, 2025

Hive Pro

HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

8 to 14 SEPTEMBER 2025

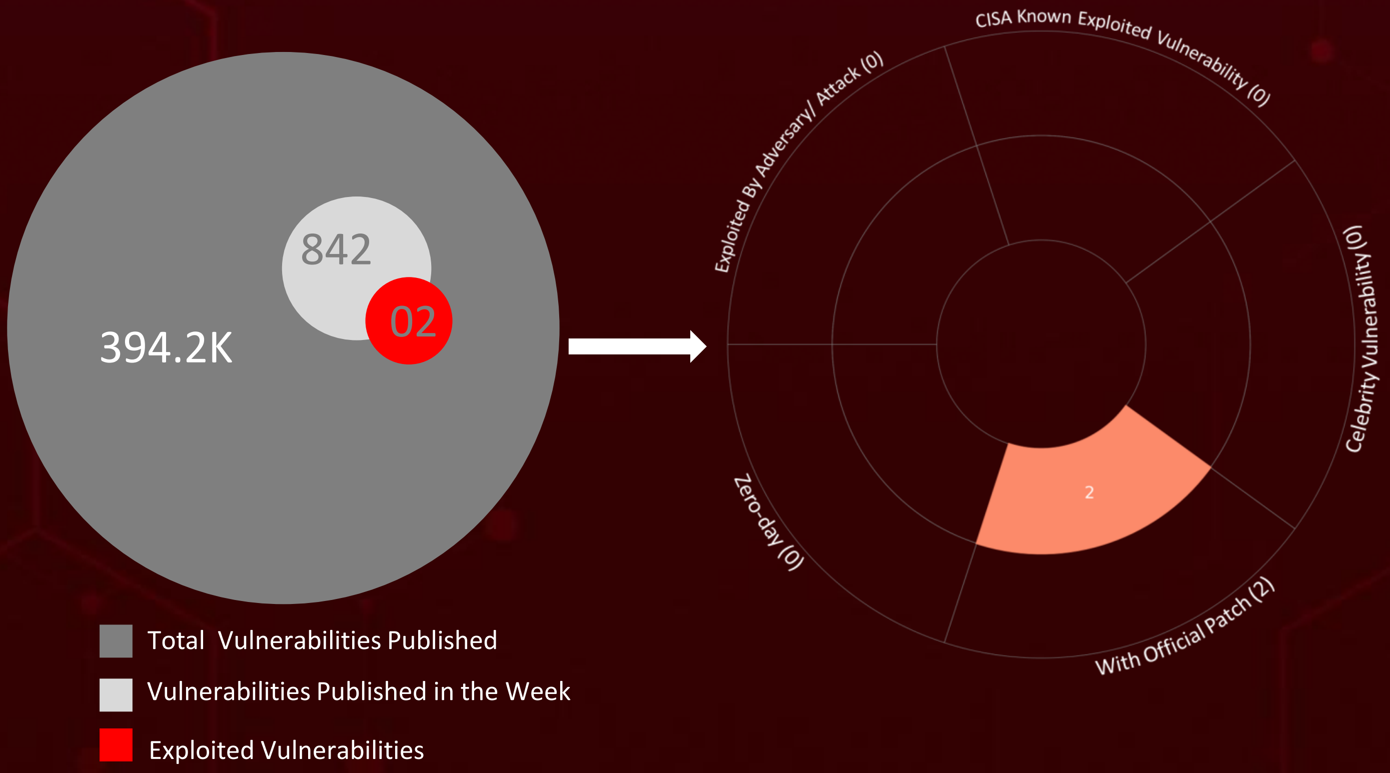
Table Of Contents

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **eleven** major attacks were detected, and **two** critical vulnerabilities were publicly disclosed, reflecting an alarming escalation in malicious activities.

Microsoft's September 2025 Patch Tuesday addresses 86 security vulnerabilities, including 8 critical flaws, affecting widely used products such as Windows SMB, Microsoft Office, SQL Server, and graphics components. Among the most concerning is **CVE-2025-55234**, a privilege escalation vulnerability in Windows SMB that has been publicly disclosed, increasing its risk profile. The update also resolves **CVE-2024-21907**, a serious flaw in Newtonsoft.Json, a third-party component used in SQL Server, which attackers could exploit to trigger a denial-of-service.

Recent threats, such as the **Cephalus** and **The Gentlemen** ransomware campaigns, demonstrate how cybercriminals are leveraging advanced tactics and targeting critical systems. This underscores the growing importance of proactive security updates and robust monitoring to defend against sophisticated, rapidly evolving attacks.



High Level Statistics

11
Attacks Executed

2
Vulnerabilities Exploited

0
Adversaries in Action

- Cephalus
- GPUGate
- Stealerium
- Warp Stealer
- Phantom Stealer
- MostereRAT
- The Gentlemen
- ZynorRAT
- kkRAT
- ValleyRAT
- FatalRAT

- CVE-2025-55234
- CVE-2024-21907

Insights

The Supply Chain Nightmare: 6,700 Repositories Exposed in **s1ngularity Attack**

Cephalus Ransomware: Why Your Weak RDP Credentials Could Be a Gateway to Disaster

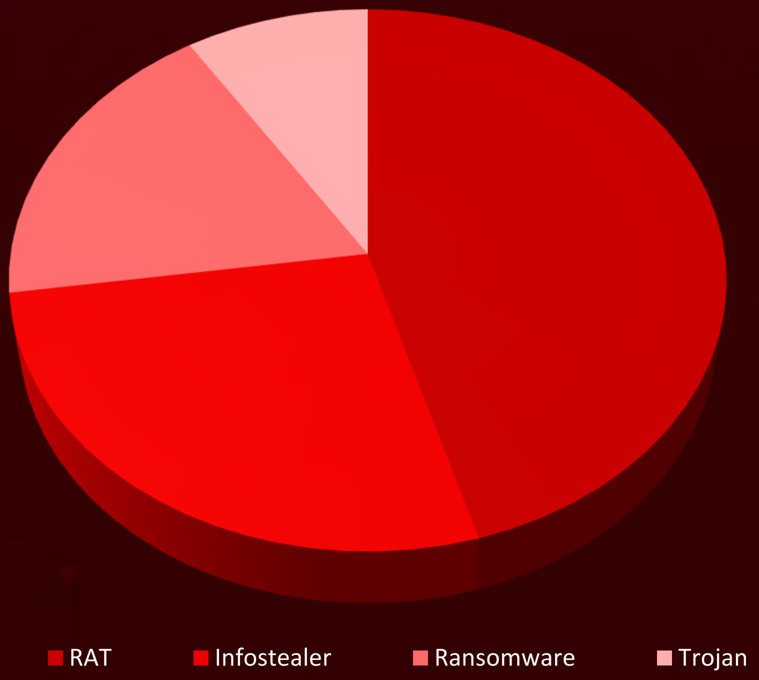
Stealerium's New Wave: Turning Financial Panic into Cyber Exploitation

Ransomware with Refinement: The Gentlemen's Stealth Infiltration Across 17 Countries

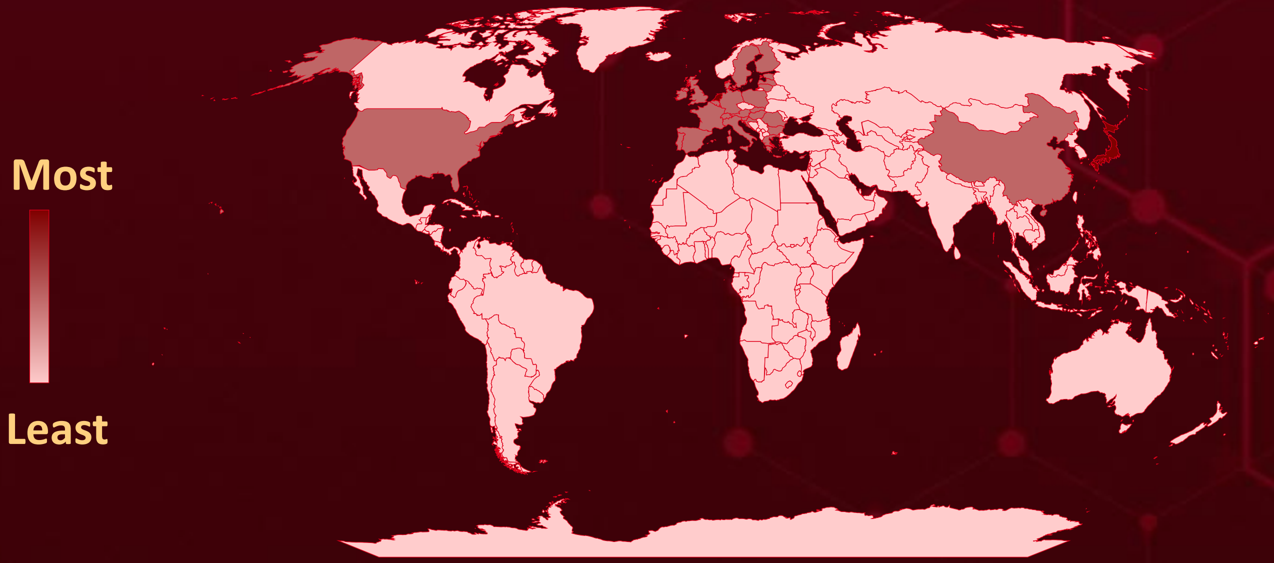
kkRAT: Stealth, Persistence, and Cryptocurrency Theft in One Trojan

ZynorRAT The Trojan That Turns Everyday Apps into Attack Platforms

Threat Distribution



Targeted Countries



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

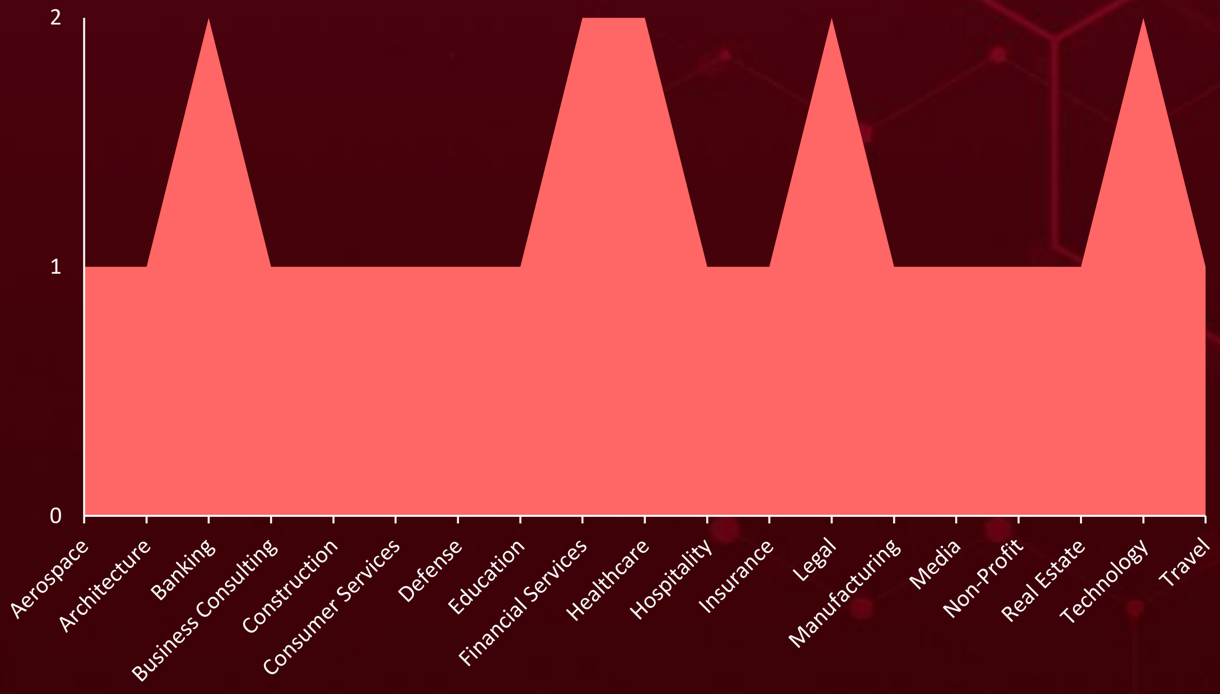
	Countries
■	Japan
■	Netherlands
▨	Liechtenstein
▨	Slovenia
▨	Belgium
▨	Bulgaria
▨	United Kingdom
▨	China
▨	Luxembourg
▨	Croatia
▨	Romania
▨	Cyprus
▨	Sweden
▨	Denmark
▨	Austria
▨	Estonia
▨	Lithuania
▨	Finland
▨	Malta
▨	Monaco
▨	Poland
▨	France
▨	Portugal
▨	Germany
▨	Slovakia
▨	Greece
▨	Spain

	Countries
▨	Hungary
▨	Switzerland
▨	Ireland
▨	United States
▨	Italy
▨	Latvia
□	South Africa
□	North Korea
□	Micronesia
□	Chile
□	Rwanda
□	Angola
□	Togo
□	Colombia
□	Namibia
□	Comoros
□	Paraguay
□	Congo
□	Serbia
□	Costa Rica
□	Suriname
□	Côte d'Ivoire
□	Ukraine
□	Antigua and Barbuda
□	Montenegro
□	Cuba

	Countries
□	New Zealand
□	Argentina
□	Pakistan
□	Czech Republic
□	Brunei
□	Czechia
□	San Marino
□	Armenia
□	Burkina Faso
□	Djibouti
□	Sri Lanka
□	Dominica
□	Tajikistan
□	Dominican Republic
□	Turkey
□	DR Congo
□	Uruguay
□	Ecuador
□	Bosnia and Herzegovina
□	Egypt
□	Mozambique
□	El Salvador
□	Nepal
□	Equatorial Guinea
□	Niger
□	Canada

	Countries
□	Norway
□	Australia
□	Panama
□	Eswatini
□	Philippines
□	Ethiopia
□	Andorra
□	Fiji
□	Saint Lucia
□	Albania
□	Saudi Arabia
□	Azerbaijan
□	Sierra Leone
□	Gabon
□	Solomon Islands
□	Gambia
□	South Sudan
□	Georgia
□	State of Palestine
□	Bahamas
□	Cameroon
□	Ghana
□	Thailand
□	Bahrain
□	Trinidad and Tobago
□	Grenada
□	Tuvalu

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1027 Obfuscated Files or Information	T1021 Remote Services
T1083 File and Directory Discovery	T1071.001 Web Protocols	T1053 Scheduled Task/Job	T1005 Data from Local System	T1204 User Execution
T1071 Application Layer Protocol	T1059.001 PowerShell	T1566 Phishing	T1543 Create or Modify System Process	T1204.002 Malicious File
T1082 System Information Discovery	T1112 Modify Registry	T1486 Data Encrypted for Impact	T1113 Screen Capture	T1552 Unsecured Credentials

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Cephalus</td><td rowspan="6">Cephalus ransomware is known for using DLL sideloading, where a legitimate SentinelOne executable from the user's Downloads folder loads a malicious SentinelAgentCore.dll. This DLL then loads a file named data.bin, which triggers the ransomware and executes a series of commands to block system recovery.</td><td>Remote Desktop Protocol (RDP) via compromised accounts</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PLATFORM</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Prevention of Recovery, Information theft, Financial Loss</td><td>-</td></tr>
<tr><td>Ransomware</td><td><b>PATCH LINK</b></td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">b3e53168fc05aeedea828bd2042e2cc34bbf8193deadab9dd4aa507e5b9c045a,
a34acd47127196ab867d572c2c6cf2fcccffa3a7a87e82d338a8efed898ca722</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">GPUGate</td><td rowspan="6">GPUGate is an advanced malware that exploits users' trust by embedding malicious links within legitimate-looking GitHub commits, leading victims to download a convincing counterfeit installer. What makes GPUGate particularly dangerous is its hardware-aware design; it only activates on real devices with compatible GPUs, allowing it to avoid detection by sandboxes and most security tools.</td><td>Social Engineering, Malvertising</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PLATFORM</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">System Infiltration, Information theft</td><td rowspan="2">-</td></tr>
<tr><td>Trojan</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e4d63c9aefed1b16830fdfce831f27b8e5b904c58b9172496125ba9920c7405b,
3746217c25d96bb7efe790fa78a73c6a61d4a99a8e51ae4c613efbb5be18c7b4</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Stealerium	Stealerium is an open-source information stealer built on the .NET framework. It uses 'netsh wlan' commands to gather saved Wi-Fi profiles and nearby networks, which could be used for tracking locations or moving laterally across systems. With advanced persistence methods, wide-ranging data theft capabilities, and multiple ways to exfiltrate information, Stealerium's flexibility and availability make it an increasingly dangerous threat.	Financial-Themed Phishing Emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Information theft, Persistence	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a00fda931ab1a591a73d1a24c1b270aee0f31d6e415dfa9ae2d0f126326df4bb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Warp Stealer	Warp is a powerful malware designed to steal and exfiltrate sensitive information. Its code shows significant overlap with Stealerium, suggesting it may have borrowed elements from it. Warp Stealer can extract a wide range of data, including browser credentials, cryptocurrency wallets, Wi-Fi profiles, and VPN settings. The stolen information is then transmitted to attackers through multiple channels such as Discord, Telegram, and email.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCT
Infostealer		Information Theft, Network Exposure	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	65c886b3e4da2a71c6d381c64c2391c7b4bd780353960ceca13735eec93a3118		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Phantom Stealer	Phantom Stealer is promoted as an 'ethical hacking' tool for 'educational purposes' and is sold using a pricing model ranging from $70 to $700. It shares code similarities with Stealerium. Once installed and executed, it gathers extensive system information, including Windows version, hardware details, browser cookies, passwords, card data, images, and documents and sends the stolen data to attackers through channels like Telegram, Discord, or SMTP.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Theft, Stealthy Exfiltration	-
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
URL	hxxps[:]//phantomsoftwares[.]site/home/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MostereRAT	MostereRAT is a stealthy Remote Access Trojan that silently infiltrates systems by disguising itself with celebrity images, creating fake services, and disabling security protections to avoid detection. Built with Easy Programming Language (EPL), it uses secure, encrypted channels to deliver malicious payloads, bypass defenses, and provide attackers with full remote access.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCT
TYPE		Security Evasion, Complete Remote Control	-
RAT			
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	4e3cdeba19e5749aa88329bc3ac67acd777ea7925ba0825a421cada083706a4e

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
The Gentlemen	The Gentlemen ransomware group systematically targets infrastructure, adjusting their tools during attacks to evade endpoint defenses and security software. Their campaign involves thorough enumeration of groups and accounts, manipulation of Group Policy using elevated PowerShell and console tools, and tailored payload delivery. They maintain persistence and stealth through remote access with AnyDesk, registry changes, and encrypted data exfiltration using WinSCP.	Exploiting internet-exposed services	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	-
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA1	c12c4d58541cc4f75ae19b65295a52c559570054

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ZynorRAT	ZynorRAT is a Go-based remote access trojan that transforms a simple Telegram bot into a powerful command-and-control platform. It offers a complete set of RAT capabilities, including remote command execution, file theft, system and process enumeration, screenshot capture, and persistence to maintain long-term access.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote Control, Information Theft, System Surveillance	Windows, Linux
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	037e5fe028a60604523b840794d06c8f70a9c523a832a97ecaaccd9f419e364a, 47338da15a35c49bcd3989125df5b082eef64ba646bb7a2db1565bb413b69323, c890c6e6b7cc6984cd9d9061d285d814841e0b8136286e6fd943013260eb8461

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">kkRAT</td><td rowspan="6">kkRAT is a remote access trojan that uses advanced anti-analysis techniques, privilege escalation, and BYOVD methods to evade detection and disable security tools. It maintains persistence through scheduled tasks, registry modifications, and startup shortcuts. Its plugin-based architecture allows attackers to remotely control systems, gather system information, proxy connections, and hijack the clipboard to steal cryptocurrency.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Evasion of Detection, Financial Theft, Remote Access</td><td rowspan="2">Windows</td></tr>
<tr><td>RAT</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">f557a90c1873eeb7f269ae802432f72cc18d5272e13f86784fdc3c38cbaca019</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">ValleyRAT</td><td rowspan="6">ValleyRAT is a remote access trojan (RAT) designed to infiltrate systems and give attackers unauthorized control. It adds new capabilities, including screenshot capture, process filtering, forced shutdown, and clearing Windows event logs to cover its tracks.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Service Disruption, Remote Access, Information Theft</td><td rowspan="2">Windows</td></tr>
<tr><td>RAT</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>IPv4:Port</td><td colspan="3">156[.]238[.]238[.]111[:]8111</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FatalRAT	FatalRAT is a remote access trojan (RAT) that provides attackers with persistent, full control over compromised systems. It enables keystroke logging, data theft, and remote command execution. To evade detection, attackers exploit legitimate Chinese cloud services like myqcloud CDN and Youdao Cloud Notes, using a multi-stage payload delivery to silently deploy the malware and bypass security defenses.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Access, Information Theft, Bypassing Security Defenses	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
IPv4:Port	103[.]199[.]101[.]3[:]8081

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55234	⊗	Windows Server: 2025, 2022, 2019, 2012 R2, 2016; Windows 10 Version 21H2; Windows 11 Version: 21H2, 24H2	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	-
Windows SMB Elevation of Privilege Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1021.002: SMB/Windows Admin Shares, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-55234

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2024-21907	⊗	Microsoft SQL Server 2019, 2017, 2016, Newtonsoft.Json before version 13.0.1	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:newtonsoft:json.net:*:*:*:*:*:*:*:*	-
Newtonsoft.Json Denial of Service Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-755	T1498: Network Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21907

Adversaries in Action

No Active Adversaries tracked this week.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploitable vulnerabilities** and block the indicators related to the malware **Cephalus, GPUGate, Stealerium, Warp Stealer, Phantom Stealer, MostereRAT, The Gentlemen, ZynorRAT, kkRAT, ValleyRAT, FatalRAT.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **two exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the malware **Cephalus Ransomware, GPUGate, Stealerium Infostealer, MostereRAT, and ZynorRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Cephalus Ransomware a Wake-Up Call for Stronger Endpoint Defense

GPUGate: Weaponizing Ads and GitHub to Outsmart Sandboxes

s1ngularity Nx Supply Chain Attack: AI-Driven Credential Theft & Mass Exposure

Stealerium Changing the Rules of Cyber Espionage

MostereRAT: A Deep Dive into an EPL-Backed Phishing Operation

The Gentlemen Ransomware: A Rising Global Cyber Threat

Microsoft September 2025 Patch Tuesday Roundup

ZynorRAT: Go-Based Malware Taking Shape on Telegram

kkRAT Malware Campaign Targeting Chinese-Speaking Users

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Cephalus	SHA256	b3e53168fc05aeedea828bd2042e2cc34bbf8193deadab9dd4aa507e5b9c045a, a34acd47127196ab867d572c2c6cf2fcccffa3a7a87e82d338a8efed898ca722, 91c459804dbf8739e2acbc6f13d8d324bceeed3f9a004f78d5475c717b04c8b5, cd28d8cc58d17521f68f04ce33ec23a3ccce95a6a4a94e8dd19697fb0bbf04b4
	Email	sadklajsdioqw[@]proton[.]me
	Tox ID	91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
	TOR Address	cephalus6oiypuwumqlwurvbmwsfglg424zjdmywfgqm4iehkqivsjyd[.]onion
GPUGate	SHA256	e4d63c9aefed1b16830fdfce831f27b8e5b904c58b9172496125ba9920c7405b, 3746217c25d96bb7efe790fa78a73c6a61d4a99a8e51ae4c613efbb5be18c7b4, ad07ffab86a42b4befaf7858318480a556a2e7c272604c3f1dcae0782339482e
Stealerium	SHA256	a00fda931ab1a591a73d1a24c1b270aee0f31d6e415dfa9ae2d0f126326df4bb
Warp Stealer	SHA256	65c886b3e4da2a71c6d381c64c2391c7b4bd780353960ceca13735eec93a3118
Phantom Stealer	URL	hxxps[:]//phantomsoftwares[.]site/home/
MostereRAT	SHA256	4e3cdeba19e5749aa88329bc3ac67acd777ea7925ba0825a421cada083706a4e

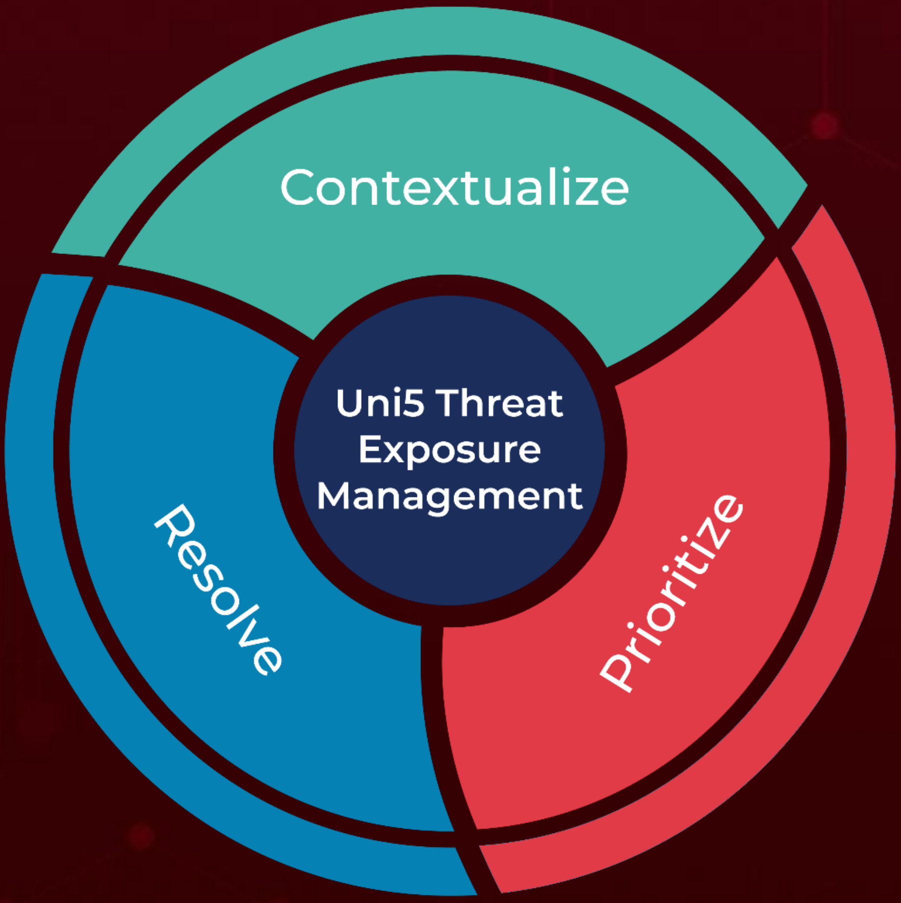
Attack Name	TYPE	VALUE
The Gentlemen	SHA1	c12c4d58541cc4f75ae19b65295a52c559570054
ZynorRAT	SHA256	037e5fe028a60604523b840794d06c8f70a9c523a832a97ecaaccd9f419e364a, 47338da15a35c49bcd3989125df5b082eef64ba646bb7a2db1565bb413b69323, c890c6e6b7cc6984cd9d9061d285d814841e0b8136286e6fd943013260eb8461, 237a40e522f2f1e6c71415997766b4b23f1526e2f141d68ff334de3ff5b0c89f, 48c2a8453feea72f8d9bfb9c2731d811e7c300f3e1935bddd7188324aab7d30d, 4cd270b49c8d5c31560ef94dc0bee2c7927d6f3e77173f660e2f3106ae7131c3, a6c450f9abff8a22445ba539c21b24508dd326522df525977e14ec17e11f7d65, bceccc566fe3ae3675f7e20100f979eaf2053d9a4f3a3619a550a496a4268ef5, 8b09ba6e006718371486b3655588b438ade953beecf221af38160cbe6fedd40a, f9eb2a54e500b3ce42950fb75af30955180360c978c00d081ea561c86e54262d
kkRAT	SHA256	f557a90c1873eeb7f269ae802432f72cc18d5272e13f86784fdc3c38cbaca019
	IPv4:Port	154[.]44[.]30[.]27[:]8250
ValleyRAT	IPv4:Port	156[.]238[.]238[.]111[:]8111
FatalRAT	IPv4:Port	103[.]199[.]101[.]3[:]8081

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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 15, 2025 • 6:30 AM

More at www.hivepro.com