

Date of Publication
June 9, 2025



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

2 to 8 JUNE 2025

Table Of Contents

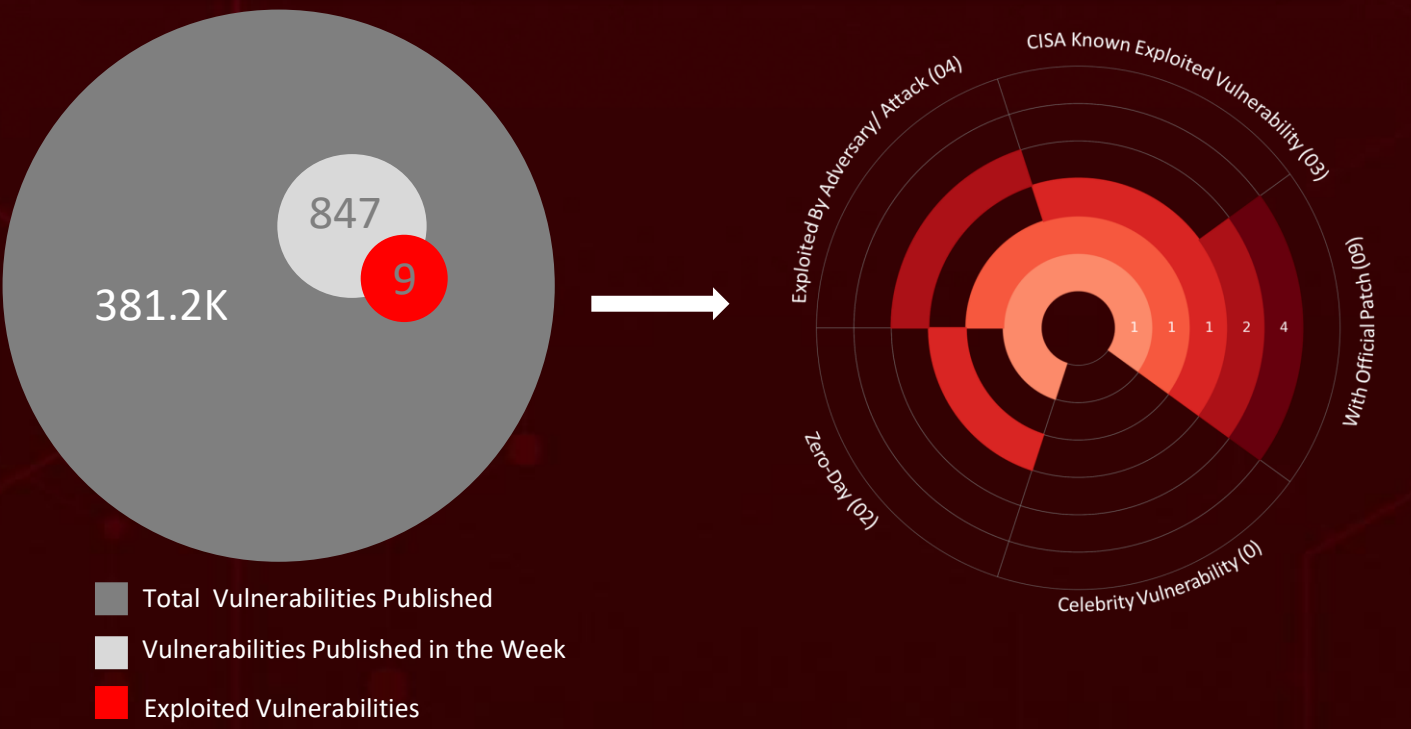
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	22

Summary

HiveForce Labs has identified a surge in cyber threats over the past week alone, with **five** attacks executed and **nine** vulnerabilities uncovered, highlighting the relentless nature of cyberattacks.

Spotlighting a wave of high-impact vulnerabilities and sophisticated attack campaigns. At the forefront is Google Chrome’s zero-day flaw in the V8 engine (**CVE-2025-5419**), already under active exploitation. Alongside it, Roundcube Webmail’s **CVE-2025-49113** exposes servers to remote code execution by authenticated users due to inadequate input validation, placing millions of outdated systems at immediate risk. Meanwhile, a critical flaw in Cisco ISE cloud deployments (**CVE-2025-20286**) threatens AWS, Azure, and OCI environments, where shared static credentials across instances allow unauthenticated attackers to gain full access and disrupt operations. The availability of public proof-of-concept exploits raises the stakes for defenders.

On the malware front, the emergence of **Lyrix ransomware** and **Chaos RAT** adds further pressure. Lyrix targets Windows systems with advanced evasion tactics, encrypting data, dismantling recovery options, and exfiltrating sensitive files, leaving victims with few alternatives other than paying the ransom. Simultaneously, Chaos RAT, a Go-based remote access tool, has been repurposed into cross-platform malware spreading through phishing emails to take control of both Windows and Linux environments. Amplifying the threat landscape is the **Phantom Enigma** campaign, a highly targeted phishing operation that began in Brazil and has spread internationally. Together, these threats reinforce a clear message that organizations must act swiftly to patch vulnerabilities, enhance threat detection, and invest in long-term cyber resilience to withstand the evolving tactics of today’s threat actors.



High Level Statistics

5

Attacks
Executed

9

Vulnerabilities
Exploited

0

Adversaries in
Action

- DragonForce
- Lyrix
- NetSupport RAT
- Chaos RAT
- Mesh Agent

- CVE-2025-42999
- CVE-2024-57727
- CVE-2024-57728
- CVE-2024-57726
- CVE-2025-5419
- CVE-2025-48827
- CVE-2025-48828
- CVE-2025-49113
- CVE-2025-20286



Insights

vBulletin Bleeds Again: Critical Flaws Under Active Exploitation

CVE-2025-48827 and CVE-2025-48828 make public forums a hacker's playground.

One Click, Full Control: Chrome Zero-Day CVE-2025-5419 Lets Hackers Hijack Your Device.

A New Player in the Ransomware Scene

Lyrix Hits Windows Systems Hard. Fast, evasive, and destructive this isn't your average ransomware.

CVE-2025-49113: Roundcube Flaw puts millions of mail servers at immediate risk.

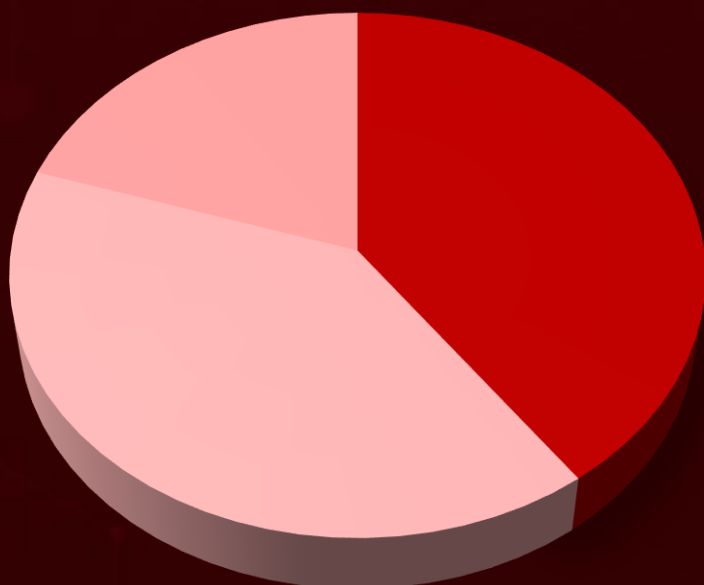
700+ Installs, Countless Breaches: Phantom Enigma Blends Phishing with Precision:

Sophisticated social engineering meets weaponized remote access tools.

Chaos RAT Isn't Just Watching - It's Commanding Your Entire System:

Go-based, stealthy, and deadly on both Linux and Windows.

Threat Distribution



■ Ransomware

■ RAT

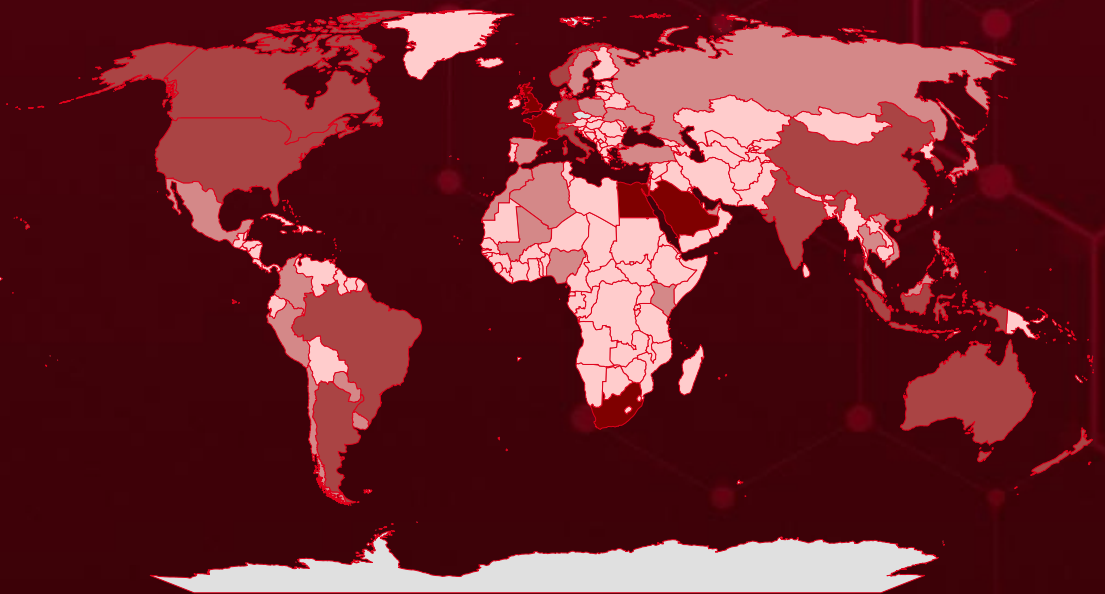
■ Hack tool



Targeted Countries

Most

Least



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

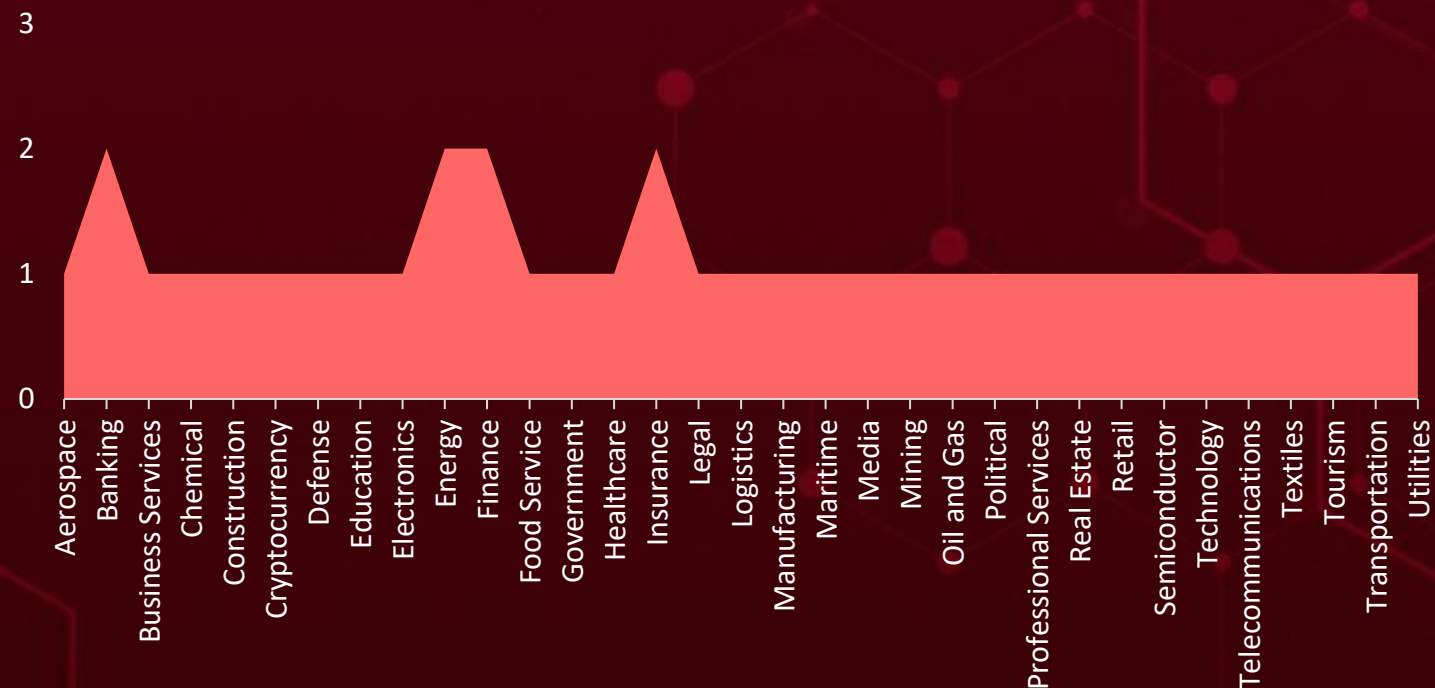
Countries
United Kingdom
South Africa
Saudi Arabia
Egypt
France
Italy
Canada
New Zealand
Czech Republic (Czechia)
China
Argentina
Brazil
Australia
Norway
South Korea
Singapore
India
Indonesia
Switzerland
Germany
United States

Countries
Spain
Israel
Turkey
Uruguay
Japan
Morocco
Malaysia
Denmark
United Arab Emirates
Nigeria
Colombia
Algeria
Kenya
Paraguay
Sweden
Peru
Thailand
Philippines
Ukraine
Poland
Chile

Countries
Russia
Mali
Mexico
Vietnam
Tanzania
Romania
Niger
Dominica
Solomon Islands
Dominican Republic
Uzbekistan
DR Congo
Panama
Ecuador
Central African Republic
Bahamas
State of Palestine
El Salvador
Turkmenistan
Equatorial Guinea
Nepal

Countries
Eritrea
Burkina Faso
Estonia
Cambodia
Eswatini
Saint Lucia
Ethiopia
Sierra Leone
Fiji
South Sudan
Finland
Congo
Bahrain
Tonga
Gabon
Cuba
Gambia
Namibia
Georgia
Brunei
Bangladesh

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1566

Phishing

T1588

Obtain Capabilities

T1190

Exploit Public-Facing Application

T1588.006

Vulnerabilities

T1204

User Execution

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1105

Ingress Tool Transfer

T1547

Boot or Logon Autostart Execution

T1204.002

Malicious File

T1070.004

File Deletion

T1059.001

PowerShell

T1071.001

Web Protocols

T1083

File and Directory Discovery

T1566.001

Spearphishing Attachment

T1562

Impair Defenses

T1547.001

Registry Run Keys / Startup Folder

T1041

Exfiltration Over C2 Channel

T1070

Indicator Removal

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DragonForce	<p>DragonForce ransomware is a financially motivated extortion tool designed to encrypt victims' files and demand payment for their recovery. Once a system is compromised, the ransomware appends encrypted files with extensions such as .dragonforce_encrypted or .cyberbears, signaling successful infection. Victims receive a ransom note stating that their data has been both stolen and encrypted, with attackers emphasizing their monetary intent rather than any political agenda. The note directs victims to contact the group via a Tor website or TOX ID, where they are offered a list of exfiltrated files and a free decryption of one file as proof of the attackers' capabilities.</p>	Exploiting Vulnerabilities, Phishing	CVE-2024-57727 CVE-2024-57728 CVE-2024-57726
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data, Data Theft	SimpleHelp remote support software v5.5.7 and before
ASSOCIATED ACTOR			PATCH LINK
-			https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
IOC TYPE	VALUE		
SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9		

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 CVEs
Lyrix	Lyrix Ransomware is a Python-based malware strain that has been converted into a Windows executable using PyInstaller, enabling it to run seamlessly on Windows systems. Designed to specifically target Windows environments, Lyrix employs strong encryption algorithms to lock victims' files and appends a distinct file extension to each encrypted file, making identification straightforward yet recovery difficult without the decryption key. The ransomware also integrates sophisticated evasion techniques and persistence mechanisms, allowing it to avoid detection and maintain a foothold on compromised systems.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data, Data Theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	fcfa43ecb55ba6a46d8351257a491025022f85e9ae9d5e93d945073f612c877b, 77706303f801496d82f83189beff412d83a362f017cadecc7a3e349a699ce458		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NetSupport RAT	NetSupport RAT (Remote Access Trojan) is a legitimate remote administration tool often exploited for malicious purposes. Cybercriminals use it to gain control over compromised systems, enabling them to execute commands, transfer files, and monitor activity.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote control and System compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	431b0b19239fc5e0eeaaee70cd6e807868142e8cd0b2b6b1bd4a7a2cc8eb57d15, Ab8fdde9fb9b88c400c737d460dcbf559648dc2768981bdd68f55e1f98292c2a ,b2daa2b5afb389828e088ec8b27c0636bdad94b2ef71dcf8034ee601cb60d8d6, 58874c0dc26a78cdc058f84af9967f31b3c43173edc7515fa400e6ef8386205f		

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 CVEs
<u>Chaos RAT</u>	Chaos RAT is a cross-platform, open-source remote access tool written in Go. First discovered in 2022 and continuously evolving through 2024 and into 2025, Chaos RAT was originally created for legitimate remote administration. However, threat actors have increasingly weaponized it to target both Windows and Linux systems. Typically delivered via phishing emails, Chaos RAT grants attackers' full control of infected machines, enabling them to steal sensitive data, run arbitrary commands, and establish persistent access. Notably, earlier versions of its web-based control panel contained serious vulnerabilities (now patched), which ironically posed risks not only to victims but also to the attackers using it.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1e074d9dca6ef0edd24afb2d13ca4429def5fc5486cd4170c989ef60efd0bbb0, d0a63e059ed2c921c37c83246cdf4de0c8bc462b7c1d4b4ecd23a24196be7dd7, 773c935a13ab49cc4613b30e8d2a75f1bde3b85b0bba6303eab756d70f459693, c8dc86afd1cd46534f4f9869efaa3b6b9b9a1efaf3c259bb87000702807f5844		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mesh Agent	Mesh Agent RAT is a remote access tool designed to run on a wide range of devices, enabling remote management through a MeshCentral server. The agent is available for multiple operating systems, including Windows, various Linux distributions, macOS, and FreeBSD, and is compiled for several processor architectures such as x86-32, x86-64, ARM, and MIPS. Its cross-platform flexibility makes it a powerful tool for legitimate administration but also a potential asset for threat actors in malicious campaigns.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Hack tool		Remote Management	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	07f7ce55e75afda05241c70710d5c6769909d94193e41b370a29b5dca3ef1f3d, 12155ad4d117ea2b13131df52de4045e635e100d45bac057d6f5674e894dec99		




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 PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-42999</u>		SAP NetWeaver Java systems Version 7.1x and above	UNC5221, UNC5174, CL-STA-0048
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:netweaver:7.5.*.*.*.*.*.*	KrustyLoader, Qilin ransomware, BianLian, RansomExx, PipeMagic
SAP NetWeaver Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57727		SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1566: Phishing, T1190: Exploit Public-Facing Application	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57728		SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Arbitrary File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE- 59 CWE-22	T1566: Phishing, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-57726</u>		SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEY	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-5419</u>		Google Chrome prior to 137.0.7151.68 Microsoft Edge	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1190: Exploit Public-Facing Application, T1566: Phishing, T1059: Command and Scripting Interpreter	https://chromerel-eases.googleblog.com/2025/06/stable-channel-update-for-desktop.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48827		vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*	-
vBulletin Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48828		vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*	-
vBulletin Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49113</u>		Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*.~.*.*.*.*.*.*	-
Roundcube Webmail Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20286</u>		Cisco ISE versions: 3.1 to 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:3.0:~.*.*.*.*.*.*	-
Cisco Identity Services Engine Static Credential Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-259	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials, T1078: Valid Accounts	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

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 **nine exploited vulnerabilities** and block the indicators related to the threat actor and malware **DragonForce Ransomware, Lyrix, NetSupport RAT, Chaos, Mesh Agent**.

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

- Running a Scan to discover the assets impacted by the **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor and malware **DragonForce Ransomware, Lyrix, NetSupport RAT, and Chaos RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[Critical CVE-2025-31324 Flaw in SAP NetWeaver Under Active Attack](#)

[DragonForce Is Selling DIY Ransomware Kits](#)

[Google Rushes to Fix Chrome Zero-Day Vulnerability](#)

[Lyrix Ransomware Turns Recovery Options Into Hollow Promises](#)

[Critical vBulletin Flaws Exploited in the Wild](#)

[Rising Use of Fake CAPTCHA Pages to Deliver NetSupport RAT](#)

[From ZIP to Zero Trust: The Finance Sector's Phishing Wake-Up Call](#)

[Chaos RAT: Open-Source Tool Turned Cyber Threat](#)

[Phantom Enigma Campaign Used Familiar Tools in Unfamiliar Ways](#)

[A Decade-Old Roundcube Glitch Comes Back to Bite](#)

[Cisco ISE Cloud Deployments Exposed to Remote Access Risk](#)

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
<u>DragonForce</u>	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9, d626eb0565fac6777fdc13fb0555967dc31e600c74fbbd110b744f8e3a59dd3f9
<u>Lyrix</u>	SHA256	fcfa43ecb55ba6a46d8351257a491025022f85e9ae9d5e93d945073f612c877b, 77706303f801496d82f83189beff412d83a362f017cadecc7a3e349a699ce458
<u>NetSupport RAT</u>	SHA256	431b0b19239fc5e0eeae70cd6e807868142e8cd0b2b6b1bd4a7a2cc8eb57d15, ab8fdde9fb9b88c400c737d460dcbf559648dc2768981bdd68f55e1f98292c2a, b2daa2b5afb389828e088ec8b27c0636bdad94b2ef71dcf8034ee601cb60d8d6, 58874c0dc26a78cdc058f84af9967f31b3c43173edc7515fa400e6ef8386205f, b258de3b7ef42b4f4bfb0fb5ffe7c55df6aef01cc591abe34a70d1ff82130cd5, e9fe19455642673b14c77d18a1e7ed925f23906bf11237dfafd7fb2cba1f666d, 1a128f6748d71d02c72ba51268be181143405830a4e48dfa53bf3d6ed3391211, 89043d2817d1bb4cb57ed939823dca0af9ae412655a6c75c694cb13d088efe5a,

Attack Name	TYPE	VALUE
<u>NetSupport RAT</u>	SHA256	8ffacc942d1c3f45e797369a1f4cbd5dcd84372abf979b06220236d5a5c ea649, b3e879b5952988fb0c656240365db8f01198f9d83cd2a3ec0e2a8ee17 2e20a11, c6907acabf2edf0be959c64a434e101963f7c18dcf79f116e0ce6b5ced5 dd08c, 07576e1db7e7bd0f7d2c54b6749fdd73c72dba8c2ba8ab110b305cfc10 c93c80, 80b274871e5024dfa9e513219fe3df82cc8fe4255010bd5d04d23d5833 962c10, d7fadf7ef45c475bd9a759a771d99ccf95edfa8a0c101ce2439a07b66c2 e5c72, f9a241a768397efb4b43924fbd32186fcb1c88716fff3085d3ddcdd322d 3404f
<u>Chaos RAT</u>	SHA256	1e074d9dca6ef0edd24afb2d13ca4429def5fc5486cd4170c989ef60efd 0bbb0, d0a63e059ed2c921c37c83246cdf4de0c8bc462b7c1d4b4ecd23a2419 6be7dd7, 773c935a13ab49cc4613b30e8d2a75f1bde3b85b0bba6303eab756d70 f459693, c8dc86afd1cd46534f4f9869efaa3b6b9b9a1efaf3c259bb87000702807f 5844, 90c8b7f89c8a23b7a056df8fd190263ca91fe4e27bda174a9c268adbfc5 c0f04, 8c0606db237cfa33fa3fb99a56072063177b61fa2c8873ed6af712bba2d c56d9, 2732fc2bb7b6413c899b6ac1608818e4ee9f0e5f1d14e32c9c29982eec d50f87, 839b3a46abee1b234c4f69acd554e494c861dcc533bb79bd0d15b9855 ae1bed7, 77962a384d251f0aa8e3008a88f206d6cb1f7401c759c4614e3bfe865e 3e985c, 57f825a556330e94d12475f21c2245fa1ee15aedd61bffb55587b54e97 0f1aad, 44c54d9d0b8d4862ad7424c677a6645edb711a6d0f36d6e87d7bae7a2 cb14d68, c9694483c9fc15b2649359dfbd8322f0f6dd7a0a7da75499e03dbc4de2 b23cad, 080f56cea7acfd9c20fc931e53ea1225eb6b00cf2f05a76943e6cf07705 04c64, a583bdf46f901364ed8e60f6aadd2b31be12a27ffccecc962872bc73a9ff d46c, a364ec51aa9314f831bc498ddaf82738766ca83b51401f77dbd857ba4e 32a53b,

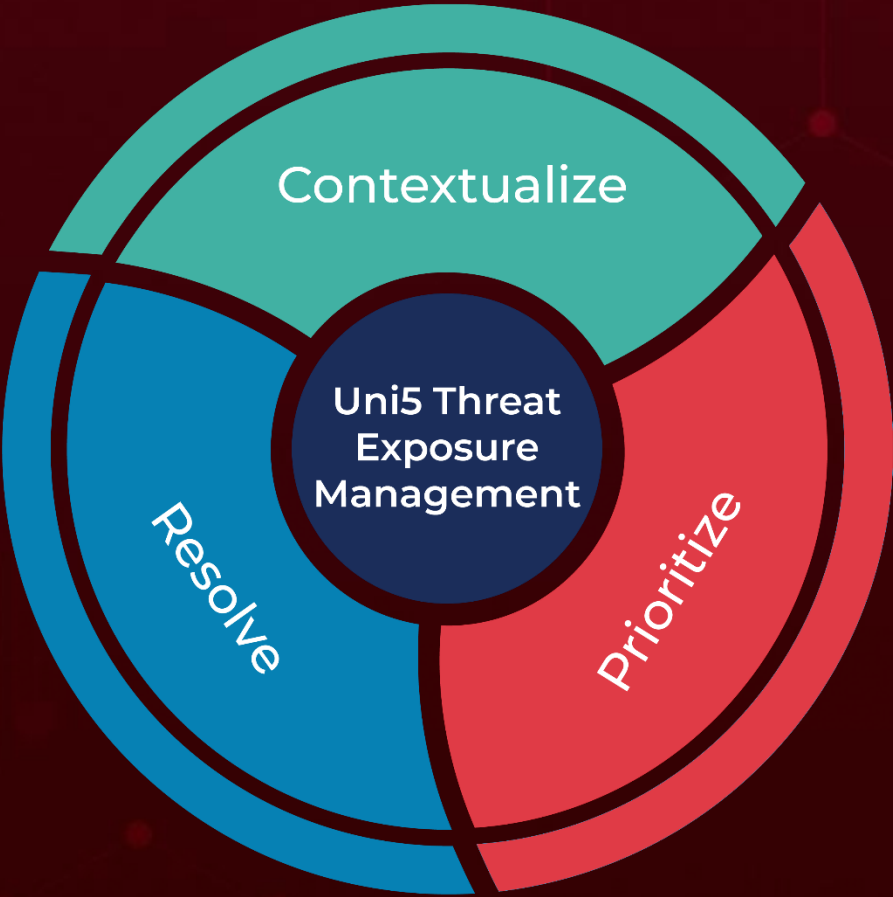
Attack Name	TYPE	VALUE
<u>Chaos RAT</u>	SHA256	a6307aad70195369e7ca5575f1ab81c2fd82de2fe561179e38933f9da28c4850, c39184aeb42616d7bf6daaddb9792549eb354076b4559e5d85392ade2e41763e, 67534c144a7373cacbd8f9bd9585a2b74ddbb03c2c0721241d65c62726984a0a, 719082b1e5c0d18cc0283e537215b53a864857ac936a0c7d3ddbaf7c7944cf79
<u>Mesh Agent</u>	SHA256	07f7ce55e75afda05241c70710d5c6769909d94193e41b370a29b5dca3ef1f3d, 12155ad4d117ea2b13131df52de4045e635e100d45bac057d6f5674e894dec99

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
June 9, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com