Date of Publication
November 17, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

10 to 16 NOVEMBER 2025

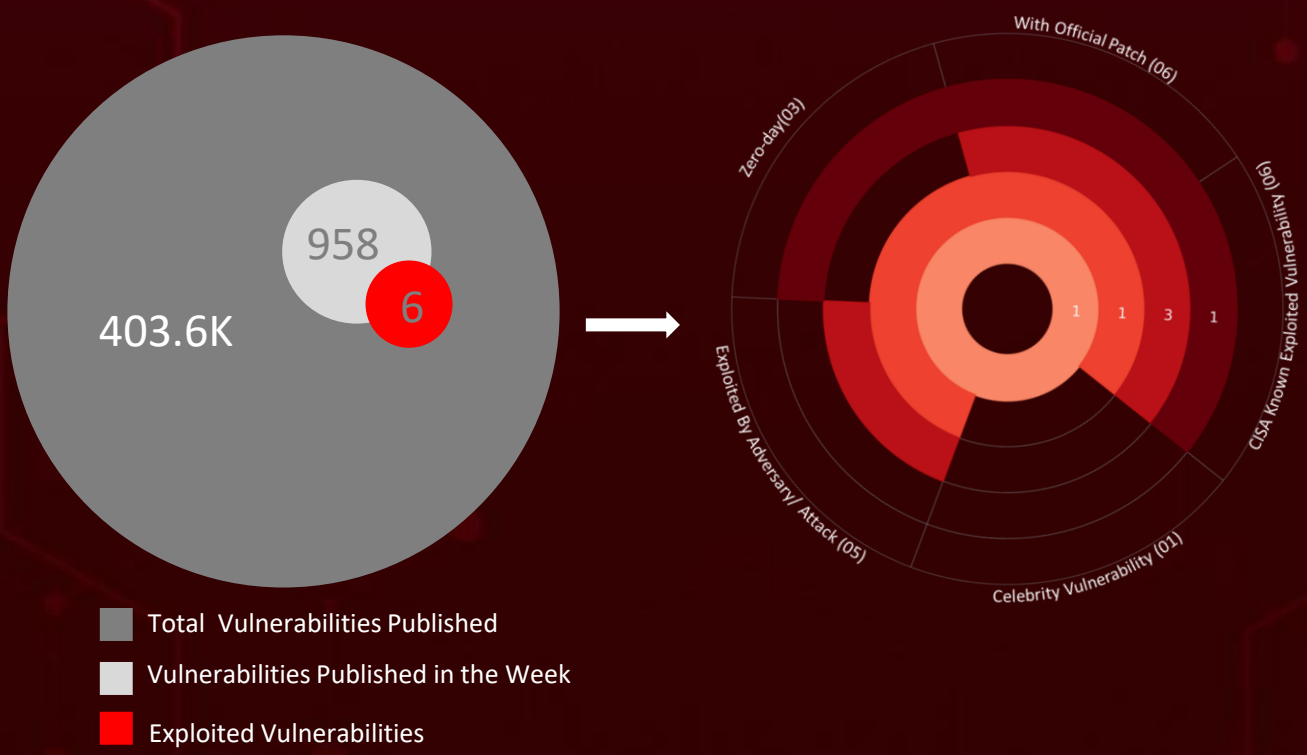
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **four** major attacks were detected, **six** critical vulnerabilities were actively exploited, and **three** threat actor were closely monitored, reflecting an alarming escalation in malicious activities.

Microsoft's November 2025 Patch Tuesday fixed 63 flaws, including a Windows Kernel zero-day, making rapid patching and verified ESU coverage critical to prevent remote attacks and privilege escalation. **UNC6485's** exploitation of **CVE-2025-12480** shows how a single Triofox flaw can enable full system takeover, letting attackers create rogue admins, deploy remote-access tools, and steal data, spotlighting the growing risks in remote-access and file-sharing platforms.

Additionally, **APT41** exploited critical vulnerabilities to infiltrate a U.S. policy non-profit in April 2025, deploying stealthy tools for espionage in line with China's ongoing targeting of U.S. policy institutions. **Lazarus** is targeting aerospace and defense firms with a macro-laden Word file that deploys an upgraded Comebacker backdoor, using multi-stage, memory-resident, and encrypted tactics to support stealthy espionage. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

4
Attacks Executed

6
Vulnerabilities Exploited

3
Adversaries in Action

- PureRAT
- Deed RAT
- PatoRAT
- Comebacker

- CVE-2022-26134
- CVE-2021-44228
- CVE-2017-9805
- CVE-2017-17562
- CVE-2025-62215
- CVE-2025-12480

- APT41
- UNC6485
- Lazarus

Insights

Attackers are pushing trojanized LogMeIn Resolve and PDQ Connect installers via fake download pages to deploy **PatoRAT** for stealthy data theft and system takeover.

APT41 exploited key vulnerabilities to spy on a U.S. policy non-profit, highlighting ongoing China-linked espionage risks.

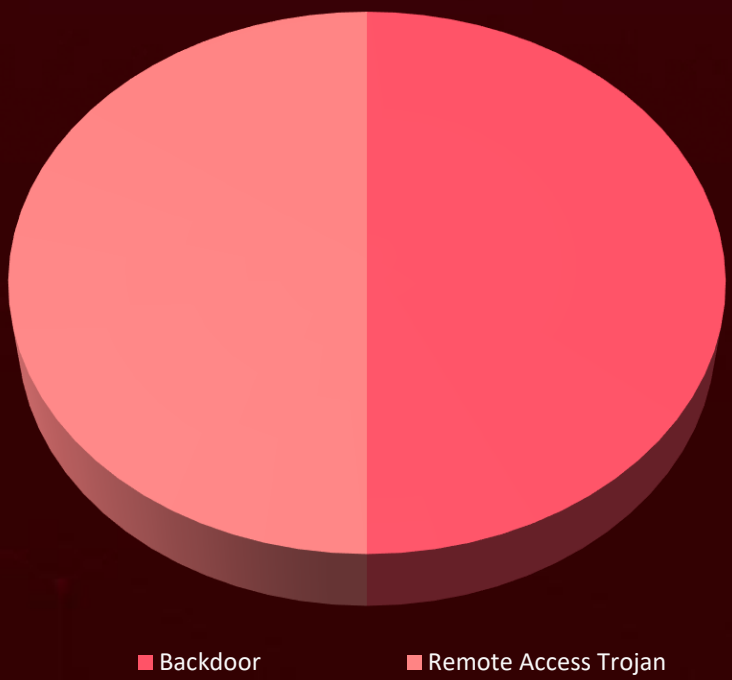
CVE-2025-12686, a critical zero-click buffer overflow in Synology BeeStation OS, allows remote code execution, making immediate patching essential to protect affected devices.

Microsoft's November 2025 Patch Tuesday fixed 63 flaws, including a Windows Kernel zero-day, making rapid patching.

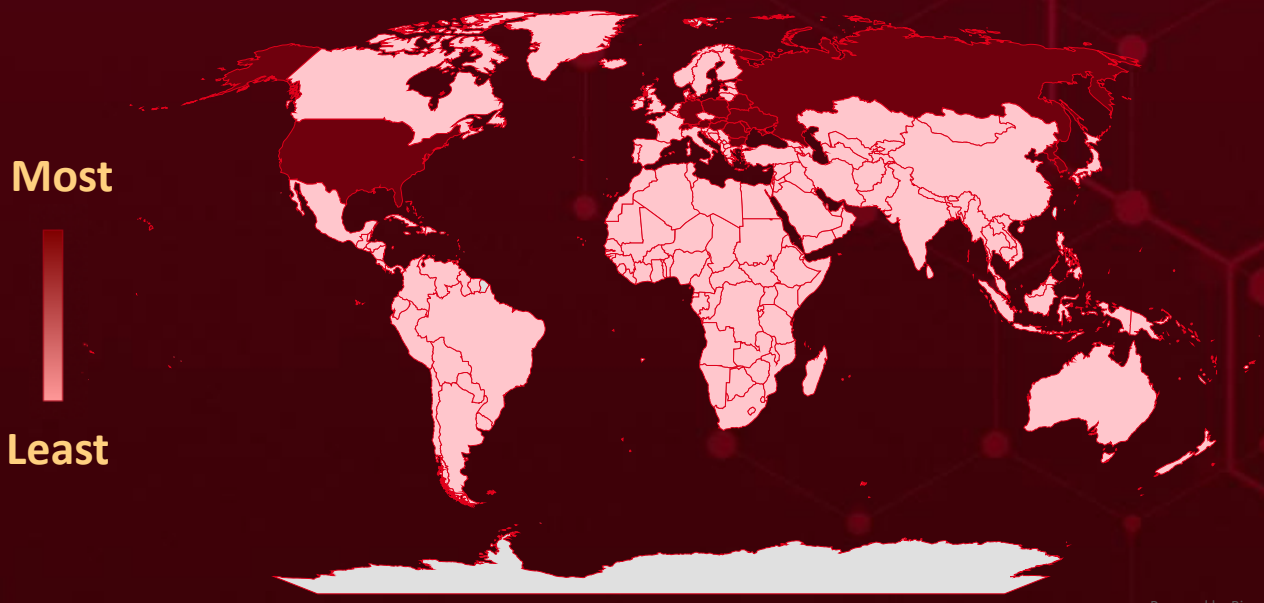
UNC6485 is exploiting CVE-2025-12480 in Triofox to gain full system control, create rogue admin accounts, and deploy remote-access tools, putting organizations at high risk.

A stealthy **Europe-wide phishing campaign** is using brand-mimicking HTML files with embedded JavaScript to steal credentials and funnel them to Telegram, bypassing traditional security controls.

Threat Distribution

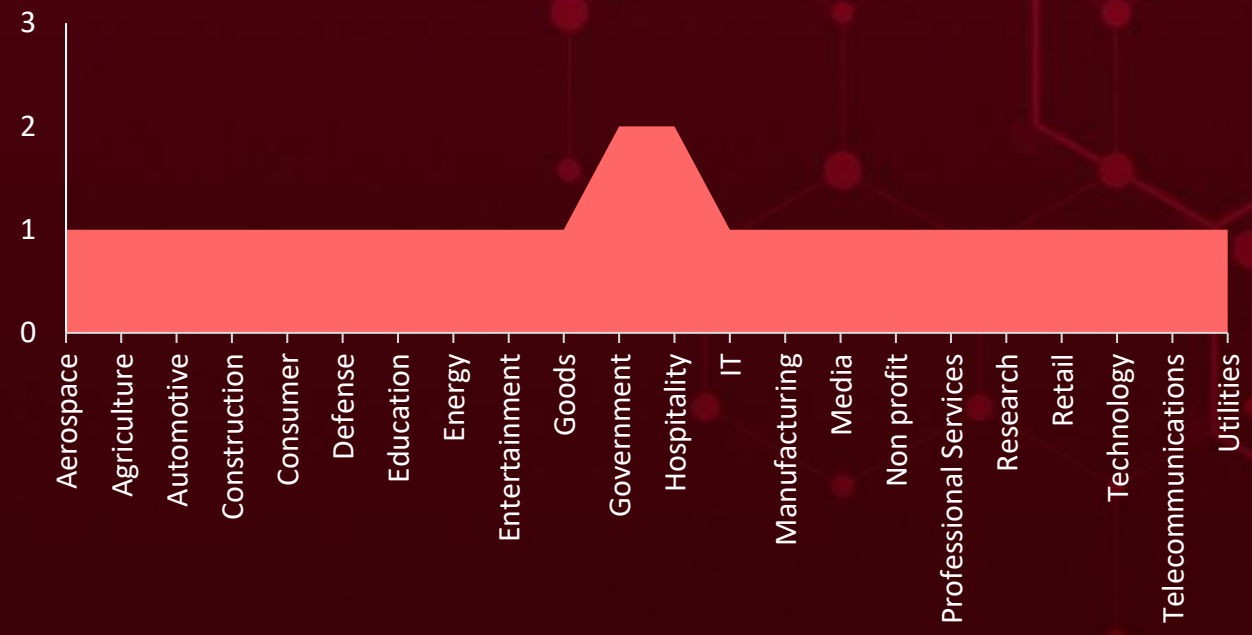


Targeted Countries



Countries	Countries	Countries	Countries
Ukraine	Malawi	Barbados	Ecuador
Russia	Bolivia	Chile	South Africa
Poland	Myanmar	Trinidad and Tobago	Egypt
Austria	Bosnia and Herzegovina	China	Sri Lanka
South Korea	Papua New Guinea	Belgium	El Salvador
Belarus	Botswana	Colombia	Suriname
North Korea	Saudi Arabia	Maldives	Equatorial Guinea
Bulgaria	Brazil	Comoros	Tajikistan
Romania	State of Palestine	Mauritania	Eritrea
Germany	Brunei	Congo	Togo
Slovakia	Tuvalu	Armenia	Estonia
Hungary	Andorra	Costa Rica	Turkey
Switzerland	Malta	Morocco	Eswatini
Liechtenstein	Burkina Faso	Côte d'Ivoire	Algeria
Moldova	Oman	Nauru	Ethiopia
United States	Cambodia	Croatia	Madagascar
Azerbaijan	Albania	Nicaragua	Fiji
Mexico	Cameroon	Cuba	Malaysia
Thailand	Saint Lucia	North Macedonia	Finland
Belize	Canada	Djibouti	Mali
Nigeria	Sierra Leone	Rwanda	France
Benin	Central African Republic	Dominica	Marshall Islands
Solomon Islands		San Marino	French Guinea
Bhutan		Dominican Republic	Mauritius
			Gabon

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1190 Exploit Public-Facing Application

T1068 Exploitation for Privilege Escalation

T1566 Phishing

T1204 User Execution

T1203 Exploitation for Client Execution

T1059.001 PowerShell

T1036 Masquerading

T1082 System Information Discovery

T1027 Obfuscated Files or Information

T1588 Obtain Capabilities

T1562 Impair Defenses

T1078 Valid Accounts

T1133 External Remote Services

T1566.001 Spearphishing Attachment

T1588.006 Vulnerabilities

T1204.001 Malicious Link

T1105 Ingress Tool Transfer

T1041 Exfiltration Over C2 Channel

T1588.005 Exploits

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PureRAT	PureRAT is a modular remote-access trojan designed for full system compromise. It can steal credentials, cryptocurrency data, and perform extensive surveillance. The malware uses evasion techniques to avoid detection and maintain persistence.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan		Data theft, Remote control	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	703355e8e93f30df19f7f7b8800bd623f1aee1f020c43a4a1e11e121c53b5dd1, 5301f5a3fb8649edb0a5768661d197f872d40cfe7b8252d482827ea27077c1ec, 64838e0a3e2711b62c4f0d2db5a26396ac7964e31500dbb8e8b1049495b5d1f3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Deed RAT	Deed RAT (aka Snappy Bee, Poisonplug.deed) is a plugin-based RAT that enables attackers to load multiple modules.It provides system discovery, command execution, and stealthy persistence.The malware is often linked to espionage activities due to its sophistication.	delivered via backdoor loaders	CVE-2022-26134 CVE-2021-44228 CVE-2017-9805 CVE-2017-17562
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan		System compromise, remote command execution, data collection	Windows
ASSOCIATED ACTOR			**PATCH LINK**
APT41			✓
IOC TYPE	**VALUE**		
SHA256	99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106		

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
PatoRAT	PatoRAT is a remote access trojan (RAT) with backdoor capabilities, primarily written in Delphi and recently observed exploiting remote management tools like LogMeIn and PDQ Connect to gain access and persistence on target systems. It is designed to give attackers control over infected devices, enabling activities such as data theft, credential harvesting, and additional malware deployment.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, remote control	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	cfef3afccf056917d4798aa605698d7bfdd34418d5baebcb7a1a43274aec4ef2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Comebacker	Comebacker is a backdoor used by Lazarus-linked operations. It establishes encrypted communication and deploys additional payloads. The malware supports stealthy execution and memory-based loading.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Payload delivery, backdoor access	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	f2b3867aa06fb38d1505b3c2b9e523d83f906995dcdd1bb384a1087b385bfc50		

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
CVE-2022-26134	✗	Atlassian Confluence Server and Data Center	APT41
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	Deed RAT
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1190 : Exploit Public-Facing Application, T1203 : Exploitation for Client Execution	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228		Apache Log4j2	APT41
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Deed RAT
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9805		Apache Struts	APT41
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:struts:-:*:*:*:*:*:*:*	Deed RAT
Apache Struts Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://cwiki.apache.org/confluence/display/WW/S2-052

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-17562		Embedthis GoAhead	APT41
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:embedthis:goahead:*:*:*:*:*:*:*:*	Deed RAT
Embedthis GoAhead Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://github.com/advisories/GHSA-q5wm-274q-f3v6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-62215		Windows: 10 - 11 25H2 Windows Server: 2019 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Windows Kernel Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362 CWE-415	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-62215

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-12480		Gladinet Triofox version 16.4.10317.56372	UNC6485
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	-
Gladinet Triofox Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://access.triofox.com/releases_history/

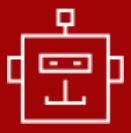
Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)	China	Government, Non profit	United States
	MOTIVE		
	Financial crime, Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2022-26134 CVE-2021-44228 CVE-2017-9805 CVE-2017-17562	Deed RAT (aka Snappy Bee, Poisonplug.deed)	Atlassian Confluence Server/Data Center, Apache Log4j2, Apache Struts, Embedthis GoAhead

TTPs

TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; T1127.001: MSBuild; T1127: Trusted Developer Utilities Proxy Execution; T1190: Exploit Public-Facing Application; T1574.002: DLL; T1021; TA0002: Execution; TA0011: Command and Control; TA0008: Lateral Movement; T1082: System Information Discovery; T1053.005: Scheduled Task; T1204; TA0003: Persistence; TA0010: Exfiltration; T1071: Application Layer Protocol; T1046; TA0007: Discovery; TA0009: Collection; T1059: Command and Scripting Interpreter; T1071.001: Network Service Discovery; T1053: Scheduled Task/Job; T1027: User Execution; T1574: Hijack Execution Flow; T1219: Remote Services: Obfuscated Files or Information; T1003.006: DCSync; T1041: Remote Access Software Exfiltration Over C2 Channel; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits: Web Protocols; T1548: Abuse Elevation Control Mechanism; T1059.001: PowerShell; T1003: OS Credential Dumping; T1059.003: Windows Command Shell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Lazarus Group (aka UNC2970, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)	North Korea	Aerospace, Defense, and Research	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	Comebacker	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1574: Hijack Execution Flow; T1583: Acquire Infrastructure; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1027.013: Encrypted/Encoded File; T1218; T1574.002: DLL; T1583.001: Domains; T1204.005: Malicious Library; T1059.003; T1573: Encrypted Channel; T1566.001: Spearphishing Attachment; T1059.001: PowerShell: Windows Command Shell Visual Basic; T1547.009; T1573.001: Symmetric Cryptography; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.005; T1140: Shortcut Modification; T1027.015: Compression; T1620: System Binary Proxy Execution: Deobfuscate/Decode: Files or Information; T1218.011: Rundll32; T1102: Reflective Code Loading Web Service; T1547.001: Registry Run Keys / Startup Folder; T1027: Obfuscated Files or Information; T1132: Data Encoding; T1132.001: Standard Encoding			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 UNC6485	-	-	-
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2025-12480	-	Gladinet Triofox
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1562: Impair Defenses; T1190: Exploit Public-Facing Application; T1055: Process Injection; T1136: Create Account; T1136.001: Local Account; T1569: System Services; T1569.002: Service Execution; T1219: Remote Access Tools; T1219.002: Remote Desktop Software; T1572: Protocol Tunneling; T1098: Account Manipulation; T1105: Ingress Tool Transfer; T1087: Account Discovery; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or: Location; T1027: Obfuscated Files or Information; T1562.001: Disable or Modify Tools; T1068: Exploitation for Privilege Escalation			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actor **UNC6485, Lazarus, APT41** and malware **PureRAT, Deed RAT, PatoRAT, Comebacker.**

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Lazarus, APT41** and malware **PureRAT, Deed RAT, PatoRAT, Comebacker** in Breach and Attack Simulation(BAS).

Threat Advisories

I Paid Twice: Inside the Booking.com Phishing Fraud

APT41 Cyber-Espionage Campaign Targets U.S. Policy Institutions

Critical Flaw Exposes Synology Devices to Remote Attacks

Telegram-Powered Credential Theft Campaign Sweeps Europe

Microsoft's November 2025 Patch Tuesday Roundup

CVE-2025-12480: Triofox Exploit Turns Trusted Access Into a Security Nightmare

Threat Actors Turn RMM Tools into Backdoor Gateways

Lazarus Group's New Comebacker Variant Targets Aerospace & Defense

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)

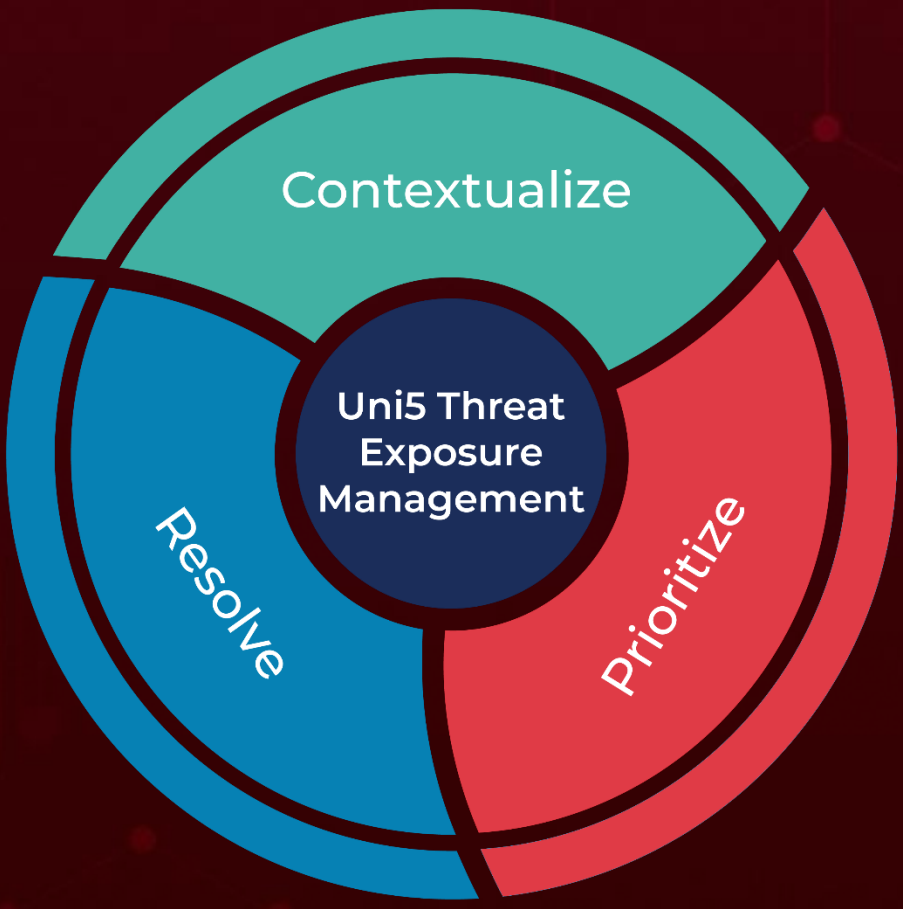
Attack Name	TYPE	VALUE
PureRAT	URL	hxxps[://]ctrlcapaserc[.]com/loggqibkng, hxxps[://]bqknsieasrs[.]com/loggqibkng
	SHA256	703355e8e93f30df19f7f7b8800bd623f1aee1f020c43a4a1e11e121c53b5dd1, 5301f5a3fb8649edb0a5768661d197f872d40cfe7b8252d482827ea27077c1ec, 64838e0a3e2711b62c4f0d2db5a26396ac7964e31500dbb8e8b1049495b5d1f3
	Domain	sqwqwasresbkng[.]com
	IPv4:Port	85[.]208[.]84[.]94[:]56001 77[.]83[.]207[.]106[:]56001
Deed RAT	SHA256	99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106
PatoRAT	SHA256	cfef3afccf056917d4798aa605698d7bfdd34418d5baebcb7a1a43274aec4ef2
Comebacker	SHA256	f2b3867aa06fb38d1505b3c2b9e523d83f906995dcdd1bb384a1087b385bfc50

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

November 17, 2025 . 9:30 AM

More at www.hivepro.com