Date of Publication
February 10, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

02 to 08 FEBRUARY 2026

Table Of Contents

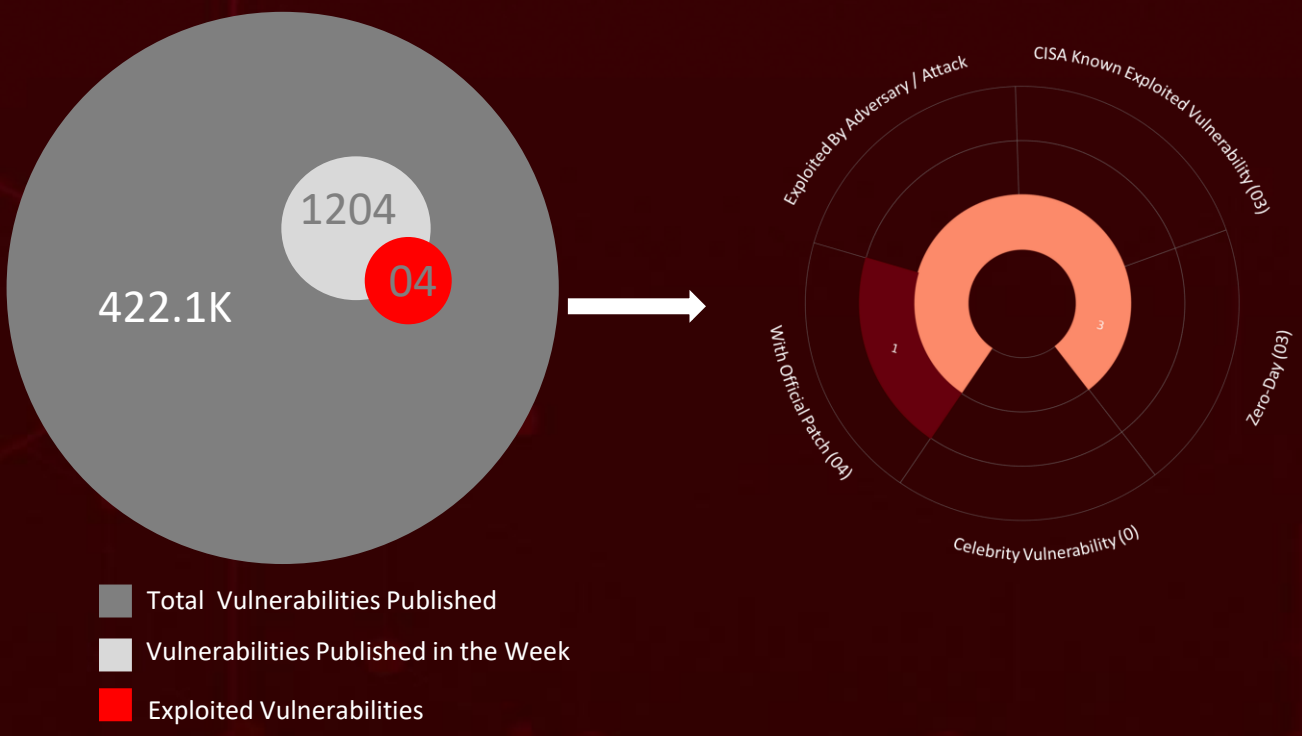
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **eleven** major attacks were detected, **four** critical vulnerabilities were publicly disclosed, and **five** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

CVE-2026-25253 is a high-risk remote code execution vulnerability in the open-source AI agent OpenClaw (Clawdbot/Moltbot). This "1-click" attack can leak authentication tokens and hijack WebSocket connections, giving attackers the ability to execute arbitrary commands on the victim's local machine.

In a separate attack, the Chinese state-sponsored APT group **Lotus Blossom** launched a sophisticated supply chain attack, compromising Notepad++ infrastructure to deploy a previously unknown backdoor, **Chrysalis**. Additionally, threat actors targeted the Open VSX Registry in a supply chain attack, hijacking a legitimate developer account (oorzc) to distribute **GlassWorm** malware via malicious updates. These updates were embedded in four trusted VS Code extensions, impacting over 22,000 users.

Finally, **APT28**'s **Operation Neusploit** signals a renewed wave of cyber-espionage activity across Central and Eastern Europe. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

11
Attacks Executed

4
Vulnerabilities Exploited

5
Adversaries in Action

- BadIIS
- GlassWorm
- Chrysalis
- MiniDoor
- PixyNetLoader
- AsyncRAT
- Amaranth Loader
- TGAmaranth RAT
- Crimson RAT
- GymRAT
- Supershell

- CVE-2026-25253
- CVE-2026-21509
- CVE-2025-8088
- CVE-2025-8110

- UAT-8099
- Lotus Blossom
- APT28
- Amaranth-Dragon
- Transparent Tribe

Insights

UAT-8099 Targets IIS Servers to Steal Credentials and Alter Search Rankings

DEAD#VAX Campaign: The Invisible Threat That Takes Control Without a Trace

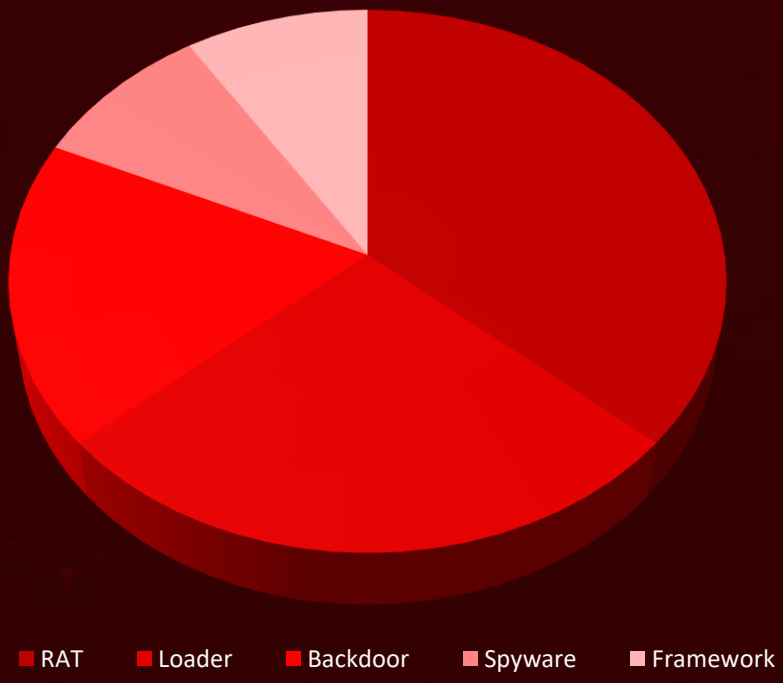
Operation Neusploit: APT28's High-Tech Espionage Campaign Targets Eastern Europe's Key Sector

CVE-2025-8088: The Flaw **Amaranth-Dragon** Uses to Breach Southeast Asian Governments

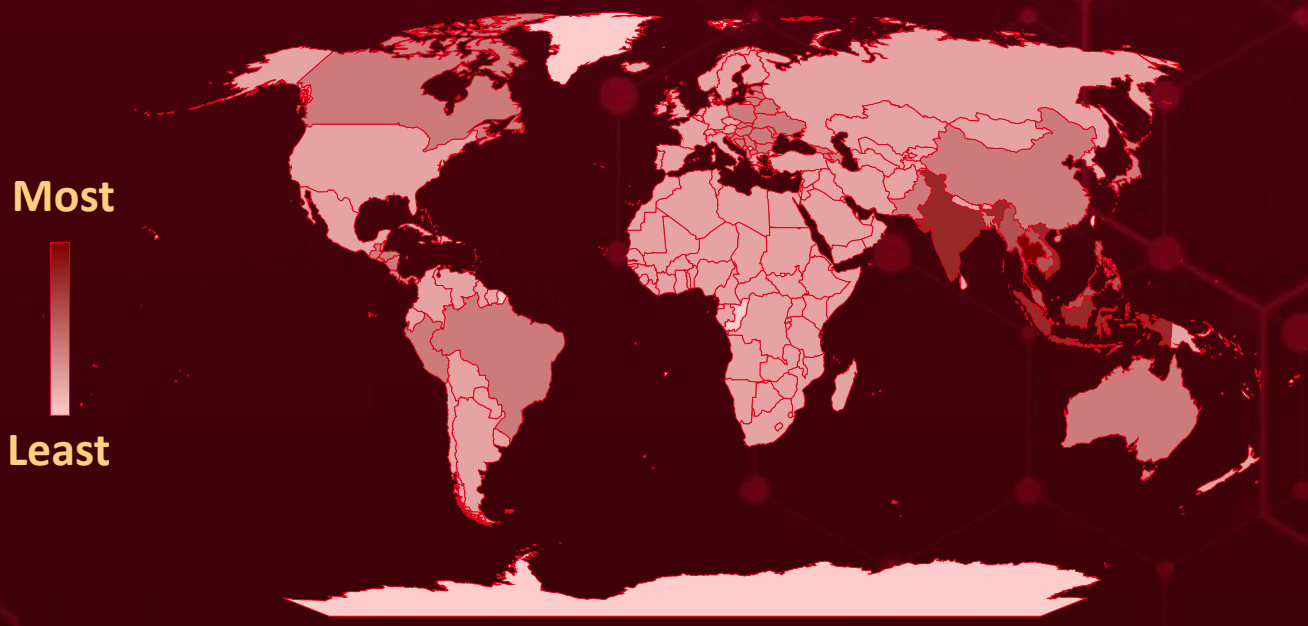
Hackers Exploit **React2Shell** to Hijack Web Traffic, Targeting Asian Government and Educational Sites

Crimson RAT and Targeted Social Engineering: **Transparent Tribe** Targets India's Startup Scene

Threat Distribution

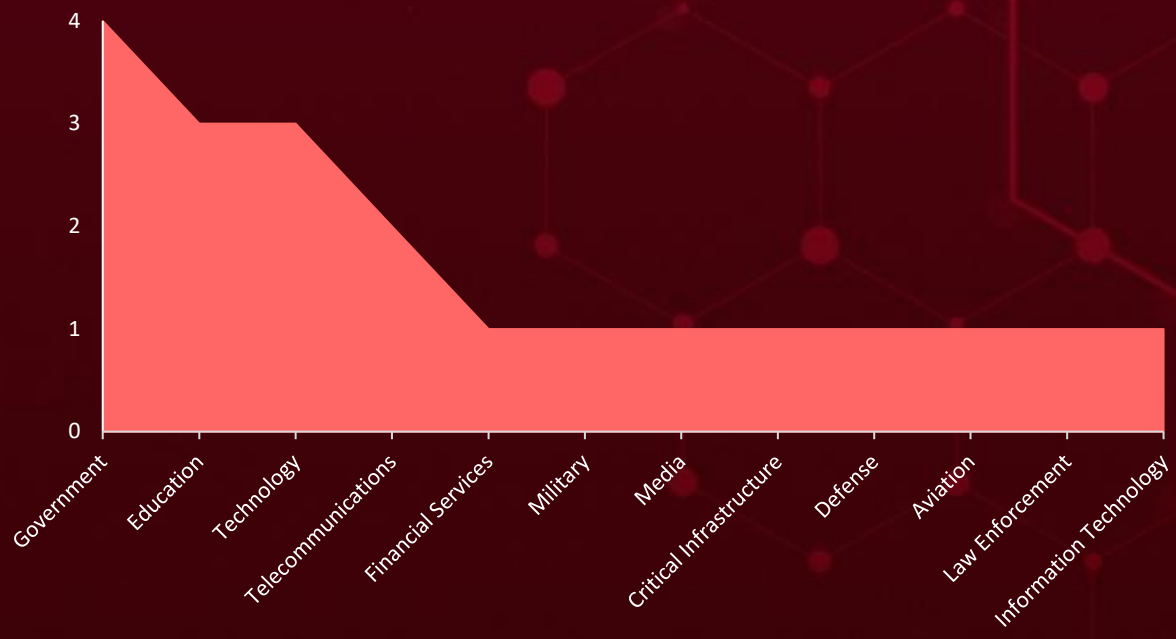


Targeted Countries



Countries	Countries	Countries	Countries
Thailand	Moldova	Egypt	Greece
Vietnam	Guatemala	Saudi Arabia	Palestine
Indonesia	Brazil	Belgium	Grenada
India	Honduras	Suriname	Colombia
Singapore	North Macedonia	Equatorial Guinea	Bhutan
Myanmar	Hungary	Denmark	Qatar
Malaysia	Panama	Eritrea	Guinea
Brunei	Ukraine	New Zealand	Guyana
Philippines	Bangladesh	Argentina	Côte d'Ivoire
Cambodia	Australia	Chile	Haiti
Laos	Romania	Eswatini	Cuba
Timor-Leste	Azerbaijan	Congo	Holy See
Slovakia	Bulgaria	Ethiopia	South Africa
Pakistan	Belize	Fiji	Bolivia
Montenegro	Slovenia	Sierra Leone	Sri Lanka
Canada	Armenia	Finland	Afghanistan
Poland	Lithuania	South Sudan	Switzerland
China	Albania	France	Iceland
Bosnia and Herzegovina	Japan	Tajikistan	Czechia
Costa Rica	Latvia	Gabon	Botswana
Nicaragua	Togo	Turkey	Trinidad and Tobago
Croatia	Russia	Gambia	Algeria
Peru	North Korea	Uruguay	Tuvalu
El Salvador	Dominica	Benin	Iran
Serbia	Solomon Islands	Nepal	United Kingdom
Estonia	Dominican Republic	Germany	United Arab Emirates
Belarus	Namibia	Niger	
Georgia	Ecuador	Ghana	United States of America
	Papua New Guinea	Norway	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1140** Deobfuscate/ Decode Files or Information
T1082 System Information Discovery	**T1041** Exfiltration Over C2 Channel	**T1566** Phishing	**T1204** User Execution	**T1083** File and Directory Discovery
T1547 Boot or Logon Autostart Execution	**T1204.002** Malicious File	**T1059.001** PowerShell	**T1566.001** Spearphishing Attachment	**T1059.003** Windows Command Shell
T1574 Hijack Execution Flow	**T1053** Scheduled Task/Job	**T1027.002** Software Packing	**T1543** Create or Modify System Process	**T1574.001** DLL

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BadIIS	BadIIS malware is being used in the wild for SEO fraud. Through reverse engineering and infection chain analysis, two clusters were customized by UAT-8099 to target specific regions. The first cluster, BadIIS IISHijack, is named after the original malware file. The second cluster, BadIIS asdSearchEngine, is designed for similar malicious SEO manipulation.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Traffic Hijacking, System Compromise	Microsoft Windows Server, Linux
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-8099			
IOC TYPE	**VALUE**		
SHA256	1ab98783a02ad9f127e776c435ef4e24a18ab93c4b4ee5ede722817d4b20771a, 1ece4d8603f5e28a7b0f6a8c83963a57cf23e5d2fadfc138419c3a051a75c93a, 2cc87bd2ae25a5119cb950618850eddeb578954fa780b125c1f51d234fb405e3,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GlassWorm	GlassWorm is a self-propagating malware campaign that weaponizes the VS Code extension ecosystem. It conceals malicious logic using invisible Unicode characters and distributes trojanized extensions through VSCode and OpenVSX, currently focusing on macOS developers.	Supply Chain Compromise	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	macOS
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	ad6d0679b5b9d2b2458047d4a9adc2d9920abbcf71f9b987b917f07d325ec3f3, 9707200067f6903f70c65721338dc1de18f1cab687a85c868d632cf12bb2f278		

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
Chrysalis	The Chrysalis backdoor was a highly capable malware that used obfuscation, custom API hashing, and RC4 encryption for its configuration data. It communicated over HTTPS for secure command-and-control traffic and maintained persistence via Windows services or registry Run keys. Chrysalis collected system information and supported remote shell access, process execution, file management, directory enumeration, and self-removal to evade detection.	Supply Chain Compromise	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	Notepad++
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Lotus Blossom			
IOC TYPE	**VALUE**		
SHA256	a511be5164dc1122fb5a7daa3eef9467e43d8458425b15a640235796006590c9, 8ea8b83645fba6e23d48075a0d3fc73ad2ba515b4536710cda4f1f232718f53e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MiniDoor	MiniDoor is a lightweight DLL that drops a malicious Outlook VBA project on the system. It modifies Outlook's registry settings to weaken security, enabling macros to run automatically and ensuring the malicious project executes every time Outlook is launched.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Drops a malicious Outlook VBA project	-
Spyware			**PATCH LINK**
ASSOCIATED ACTOR			-
APT28			
IOC TYPE	**VALUE**		
SHA256	bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e		

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
PixyNetLoader	PixyNetLoader uses multiple evasion techniques to avoid detection. The loader activates only when explorer.exe is running and performs timing checks to identify sandbox environments. If the environment seems legitimate, it extracts hidden shellcode from a PNG image using steganography, concealing data within the image pixels.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		drops malicious components	-
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
APT28			
IOC TYPE	**VALUE**		
SHA256	0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e, a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an open-source Windows RAT, ranked 6th in global prevalence in 2024. Its capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft	-
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524,		

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
Amaranth Loader	Amaranth Loader is a custom tool designed to deliver encrypted payloads, primarily deploying the Havoc C2 Framework. It retrieves an encrypted payload, decrypts it using AES, and executes it directly in memory.	Exploiting Vulnerability	CVE-2025-8088
		IMPACT	**AFFECTED PRODUCT**
TYPE		Loads another payload	RARLAB WinRAR
Loader			**PATCH LINK**
ASSOCIATED ACTOR			https://www.win-rar.com/download.html?&L=0
Amaranth-Dragon			
IOC TYPE	**VALUE**		
SHA1	00351add8e0bca838e8dac40875b8ad5195805bd, 481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TGAmaranth RAT	TGAmaranth RAT is a fully functional 64-bit DLL remote access tool (RAT) that uses a hardcoded Telegram bot as its C&C. It uses an encrypted bot token to connect to telegram, listens for incoming bot messages, and interprets them as commands.	Exploiting Vulnerability	CVE-2025-8088
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	RARLAB WinRAR
RAT			**PATCH LINK**
ASSOCIATED ACTOR			https://www.win-rar.com/download.html?&L=0
Amaranth-Dragon			
IOC TYPE	**VALUE**		
SHA1	803fb65a58808fd3752f9f76b5c75ca914196305		

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
Crimson RAT	Crimson RAT is a remote access trojan used for intelligence gathering. It also uses a custom TCP-based command-and-control protocol rather than standard HTTP/HTTPS, complicating network-level detection. Once active, the implant enables system reconnaissance, file exfiltration, remote command execution, and long-term persistence.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, Execute commands	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Transparent Tribe			
IOC TYPE	VALUE		
SHA256	1092761df305e910f806834fb774dfb09dc64a4d399d578a0d1bf1dd5daf0f98		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GymRAT	GymRAT is a malware that primarily targets Windows systems. It is often distributed via phishing and malicious attachments, enabling remote access to compromised machines. GymRAT's capabilities include keylogging, credential theft, and stealing sensitive data, allowing attackers to control and monitor infected devices.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Steal Data	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Transparent Tribe			

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">Supershell</td><td rowspan="6">Supershell is an open-source Command and Control (C2) platform designed to establish a reverse SSH shell that communicates over web services. This mechanism provides attackers with remote control and the ability to execute arbitrary code on a compromised system.</td><td>Exploiting Vulnerability</td><td>CVE-2025-8110</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="4">Execute Code</td><td>Gogs</td></tr>
<tr><td>Framework</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://github.com/gogs/gogs/releases</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA1</td><td colspan="3">d8fcd57a71f9f6e55b063939dc7c1523660b7383, efda81e1100ea977321d0f2eeb0dfa7a6b132abd</td></tr>
</table>

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-2026-25253	✗	OpenClaw Clawdbot/Moltbot (Before 2026.1.29)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openclaw:openclaw:*:*:*:*:*:*:*:*	-
OpenClaw Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-669	T1566: Phishing, T1528: Steal Application Access Token, T1059: Command and Line Interface, T1204: User Execution, T1071: Application Layer Protocol	https://github.com/openclaw/openclaw/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21509		Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	MiniDoor, PixyNetLoader
Microsoft Office Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing, T1204: User Execution, T1559: Inter-Process Communication, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8088		WinRAR Versions up to and including 7.12	Amaranth-Dragon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Amaranth Loader, TGAmaranth RAT
RARLAB WinRAR Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8110	 ZERO-DAY	Gogs (Prior to 0.13.4, all versions through 0.13.3)	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	Supershell
Gogs Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1083: File and Directory Discovery	https://github.com/gogs/gogs/releases

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-8099	-	Education, Technology, Telecommunications	India, Thailand, Vietnam, Canada, Brazil, Pakistan, Japan
	MOTIVE		
	Information theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	BadIIS	Microsoft Internet Information Services (IIS)

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011:Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1505: Server Software Component; T1505.003: Web Shell; T1505.004: IIS Components; T1136: Create Account; T1136.001: Local Account; T1078: Valid Accounts; T1078.003: Local Accounts; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1027: Obfuscated Files or Information; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1071: Application Layer; Protocol T1071.001: Web Protocols; T1572: Protocol Tunneling; T1491: Defacement; T1491.002: External Defacement

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Lotus Blossom (also known as LOTUS PANDA, Billbug, Bronze Elgin, Spring Dragon, Raspberry Typhoon, Thrip)</td><td>China</td><td rowspan="3">Government, Financial Services, Information Technology, Telecom, Aviation, Critical Infrastructure, Media</td><td rowspan="3">Australia, Belize, Brunei, Cambodia, Costa Rica, El Salvador, Guatemala, Honduras, Indonesia, Laos, Malaysia, Myanmar, Nicaragua, Panama, Philippines, Singapore, Thailand, Timor-Leste, Vietnam</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Chrysalis Backdoor</td><td>Notepad++</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1204: User Execution T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1106: Native API; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process ; T1543.003: Windows Service; T1574: Hijack Execution Flow ; T1574.002: DLL; T1027: Obfuscated Files or Information ; T1027.007: Dynamic API Resolution; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1055: Process Injection; T1620: Reflective Code Loading; T1480: Execution Guardrails ; T1480.002: Mutual Exclusion; T1083: File and Directory Discovery; T1082: System Information Discovery; T1005: Data from Local System; T1071: Application Layer Protocol ; T1071.001: Web Protocols; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1070: Indicator Removal ; T1070.004: File Deletion</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)	Russia	All	Central and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-21509	MiniDoor, PixyNetLoader	Microsoft Office

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0042: Resource Development; T1566: Phishing T1566.001: Spearphishing Attachment; T1203: Exploitation for Client Execution; T1106: Native API; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1137: Office Application Startup ; T1137.006: Add-ins; T1574: Hijack Execution Flow; T1574.001: DLL; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.002: Mutual Exclusion; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.003: Steganography; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1114: Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1588: Obtain Capabilities; T1588.006: Vulnerabilities

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Amaranth-Dragon	China	Government, Law Enforcement	Cambodia, Thailand, Laos, Indonesia, Singapore, Philippines, Brunei, Malaysia, Myanmar, Timor-Leste, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-8088	Amaranth Loader, TGAmaranth RAT	RARLAB WinRAR
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spear-phishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1203: Exploitation for Client Execution; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1140: Deobfuscate/Decode Files or Information; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1055: Process Injection; T1055.012: Process Hollowing; T1620: Reflective Code Loading; T1056: Input Capture; T1057: Process Discovery; T1082: System Information Discovery; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Transparent Tribe (also known as APT36, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134)	Pakistan	Startups, Technology, Government, Defense, Military, Education	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Crimson RAT, GymRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0003: Persistence; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1553: Subvert Trust Controls; T1553.005: Mark-of-the-Web Bypass; T1027: Obfuscated Files or Information; T1027.001: Binary Padding; T1027.002: Software Packing; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1547: Boot or Logon Autostart Execution; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1016: System Network Configuration Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1113: Screen Capture; T1125: Video Capture; T1123: Audio Capture; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **UAT-8099, Lotus Blossom, APT28, Amaranth-Dragon, Transparent Tribe,** and malware **BadIIS, GlassWorm, Chrysalis, MiniDoor, PixyNetLoader, AsyncRAT, Amaranth Loader, TGAmaranth RAT, Crimson RAT, GymRAT,** and **Supershell.**

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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **UAT-8099, Lotus Blossom, APT28, Amaranth-Dragon, Transparent Tribe,** and malware **BadIIS, Chrysalis, PixyNetLoader, Amaranth Loader,** and **TGAmaranth RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

UAT-8099 Cybercrime Group Leverages BadIIS

Attackers Hijack Open VSX Extensions to Spread GlassWorm Malware

One Click to Compromise: Inside OpenClaw’s Critical RCE Flaw

Chrysalis Backdoor: A Quiet Passenger in Notepad++ Updates

Operation Neusploit: APT28 Weaponizes CVE-2026-21509

DEAD#VAX: AsyncRAT Deployment via IPFS-Hosted VHD Phishing

Web Traffic Hijacking via Malicious NGINX Configuration Injection

Amaranth-Dragon: Low Noise, High Impact Espionage in Southeast Asia

Transparent Tribe Targets India's Startup Ecosystem with Crimson RAT

The Gogs Blind Spot: A Zero-Day Fueled Mass Compromise

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
BadIIS	SHA256	1ab98783a02ad9f127e776c435ef4e24a18ab93c4b4ee5ede722817d4b20771a, 1ece4d8603f5e28a7b0f6a8c83963a57cf23e5d2fadfc138419c3a051a75c93a, 2cc87bd2ae25a5119cb950618850eddeb578954fa780b125c1f51d234fb405e3, 4bc189af91779582a1d29cfe187aa233e7ba50d223261fb9fbe31df5b06dff96, 6be5c8882bc02cf4e86d2ab9d20aa3446b71dd12c73f9c6bf0faf9412d7d23ba, 9a2fd34e22c5f3d3d5fb96e3cd514dad7b03ed7bf53a87e7d8d9b73987d02ece, 11ea6aa2b31677f8a36627d4af709e70cff4a033b0975f63c19b28945e6226b7, 29ffb1d28f98582e81e78e6b2d5502da50c8ebdee0d40005a86b0dadece2923b, 56be91643dd8b86f347cc8d743c568f2d0169781ba999a2f708e503b59ecff76, 70d6bc89451e36889c045f30de22bc02e032788c8938baa0d5802e8f747c3e79, 91e1f4fc92f104ec8b29bb56df87f8e7d8b518c63997e2ea162d3f1cac3fcac1, 416ef6da8a27a99cbce6517d31857c8b8b55f02e9c8118510dc33814fb6f57be,

Attack Name	TYPE	VALUE
BadIIS	SHA256	660ccb6dcfad97bfaddc667c61b1904e99a06eab981d44119092624d42912d68, 9458a75c1e24add9a48e0425e514a5f0cb46a826bff30ea7ea34e69099345f29, 265336511db98a4c40476455e2ae93aaf926abecd8f9b9d741f8d253abb80357, a781581baf6e1e335f22c9ffbb2656a2d9c8e51f463e3a48068210425df1c205, ab03a7caed279fc6411ec19386faff3b65be34c91c3f0550eaef84a663720d0d, bcc393c1686a0f5d493041e98dcafe0098d952d5e93eb4d2ebdb63c0efd2de33, c7a22f5c55ac1373a5964a6598da2a9afd8a61b9d729b9bf52a93c967a7f0eda, cdf454173bac13266e0f7db5de386439f197e2c480e1cc303dd7e806484645da, e84a16c8e25a4e40926cbb4cc210a09830298b6f99d532035f5136d05ffc008c, e448557d26cf2917efded8e30c67db8094ce1f6db78801742988ea21f3429d7c, 5d320b60d2f40c200e81eaeb67a86a04782bff84582c73e726255dba2dcb821e, 99f2c4773560eb515cfcb0ad45cf8e47c46580ab19494463160f885e048ce830, 565502d2454e4b65d3bd810fccf4b429264562fefa5cfff24c905b76b3b860a6, a34ea8fb565ac6f57eefc987c61159c1e6f1af6a8717ffb42f4b745db3bf9e31, 187e1417fd9d4f4a44e4f7b7172aef056e9d0ab5d7a7addf61c2cfa893f74fd1, 6b60b6df8a1a95f51ffe57255c05d26eb9e113857efac3b29d6ef080b8d414f3, 672ffdf1e9d4848015d29a68111266ef55fc6702dfe7b2053ce677882648dd5d, ebeef831c52b7e930a6456caedf7849814b8d4def2bc0e70a0e7a357621ef6bc, 230b84398e873938bbcc7e4a1a358bde4345385d58eb45c1726cee22028026e9, 48ec6530470b295db455bf2c72dc4fbd18672725f45821304f966d436b428865, 33d3ccf82279d94a8e8e772a0c4963d65a1f3576dbd6ed7b4ab8a0ee4869f97f, d8c0ef6dbf7d4572f92d3a492f32061ab8f3dd46beb9ff5a0bf9bf550935458c

Attack Name	TYPE	VALUE
GlassWorm	SHA256	ad6d0679b5b9d2b2458047d4a9adc2d9920abbcf71f9b987b917f07d325ec3f3, 9707200067f6903f70c65721338dc1de18f1cab687a85c868d632cf12bb2f278, b62acc93eb77a4ffb88cf49a8bcef574e6216e10714433a9cb1230bdb2c90546, 6beaf047e948c366cb21d16818e1d0bb0ebbd928f40fe22c521344ad9c38f32e, e46ab145387e8ae996a202520f73088ae735f88f18fab1ed60469334d58d727d, 4210121526cb985d0026469de0dc5f3767ce792149164df8fd0b43b4d6f30959, c8c523ff27a7fc4bef39dce97261c97bf724556cf32d0030090c168f82b20c7a, da4aefbcda028808dc892ad5a10bb528f129883ab9c29bb6800d298d3c26f848, d84cbd286724fe8c38f4e389ce9f582df93cac37172823f4eecacdcef0a5975d, 6f698f6983fc7ece0cade5f0c1bc7a66f7400229e0e99271ea9df6bece9473cf, ca2a7d82456036d905b5ea0e25678d8e6af165dc5d2a850450f22e2e63cb2767, 130d1f487072e512611489c4cd725bdfb59c31327d056bdbd22bea4f8fab576b, a3e5d8643dffb775a32fe73b08319dd6b201ec0f0215a048a22f0c47b9a08066
Chrysalis	SHA256	a511be5164dc1122fb5a7daa3eef9467e43d8458425b15a640235796006590c9, 8ea8b83645fba6e23d48075a0d3fc73ad2ba515b4536710cda4f1f232718f53e, 77bfea78def679aa1117f569a35e8fd1542df21f7e00e27f192c907e61d63a2e, 3bdc4c0637591533f1d4198a72a33426c01f69bd2e15ceee547866f65e26b7ad, 0a9b8df968df41920b6ff07785cbfebe8bda29e6b512c94a3b2a83d10014d2fd
MiniDoor	MD5	f05d0b13c633ad889334781cf4091d3e
	SHA1	7bbb530eb77c6416f02813cd2764e49bd084465c
	SHA256	bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e
PixyNetLoader	MD5	859c4b85ed85e6cc4eadb1a037a61e16
	SHA1	da1c3e92f69e6ca0e4f4823525905cb6969a44ad
	SHA256	0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e, a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1

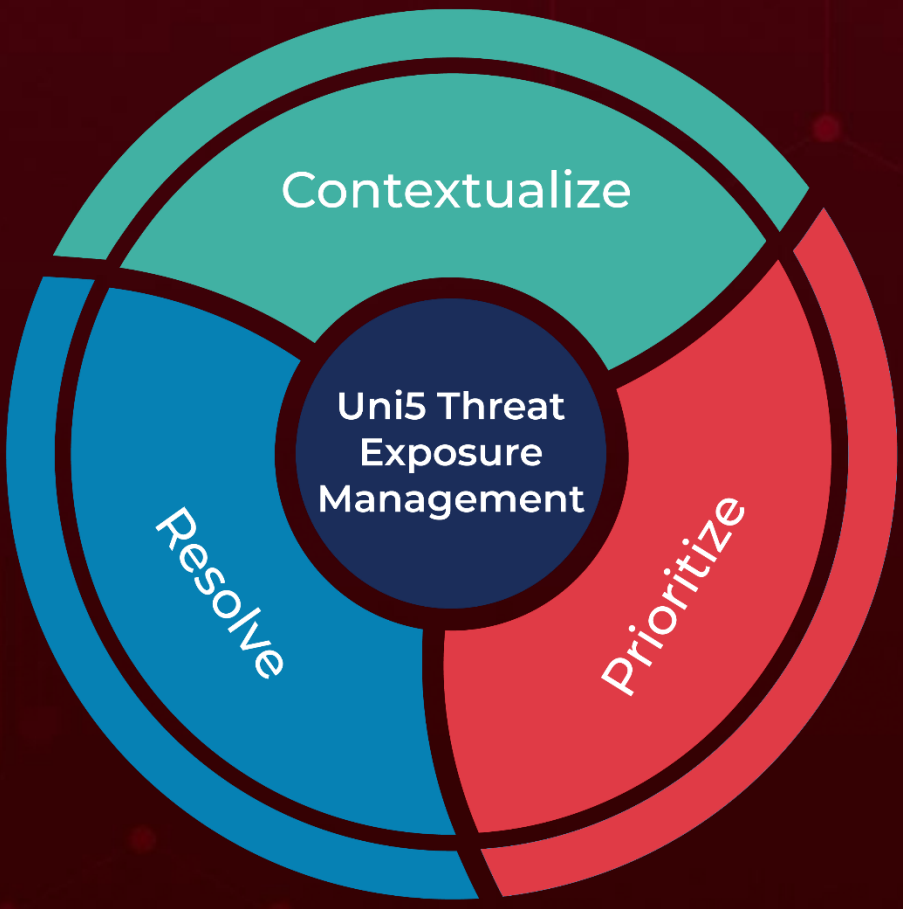
Attack Name	TYPE	VALUE
AsyncRAT	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ececf197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87
Supershell	IPv4	119[.]45[.]176[.]196
	SHA1	d8fcd57a71f9f6e55b063939dc7c1523660b7383, efda81e1100ea977321d0f2eeb0dfa7a6b132abd
Amaranth Loader	SHA1	00351add8e0bca838e8dac40875b8ad5195805bd, 481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2, 718c5846d3b903e3e9e2df9281f5e25b371465f2, 9afadca9b2dad54004bd376dbee7e98c38dbdf50, b4dc300031edf5dd4968028146b0d608bdd975c5, c54a68d6bcc6d04ff08ad9619706e54923a20248, cd949663598c49141a98b438cf408113602e5c19, ddea99cb2db5e95552dccc8804125f19b30af536
	SHA256	d7711333c34a27aed5d38755f30d14591c147680e2b05eaa0484c958ddaae3b6
TGAmaranth RAT	SHA1	803fb65a58808fd3752f9f76b5c75ca914196305
	SHA256	a3805b24b66646c0cf7ca9abad502fe15b33b53e56a04489cfb64a238616a7bf
Crimson RAT	MD5	5b4a48815446cd40d8e141cbf8582296
	SHA256	1092761df305e910f806834fb774dfb09dc64a4d399d578a0d1bf1dd5daf0f98
	IPv4	93[.]127[.]133[.]9
	Domain	Sharmaxme11[.]org

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

February 10, 2026 . 4:00 AM

More at www.hivepro.com