Date of Publication
October 21, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

13 to 19 OCTOBER 2025

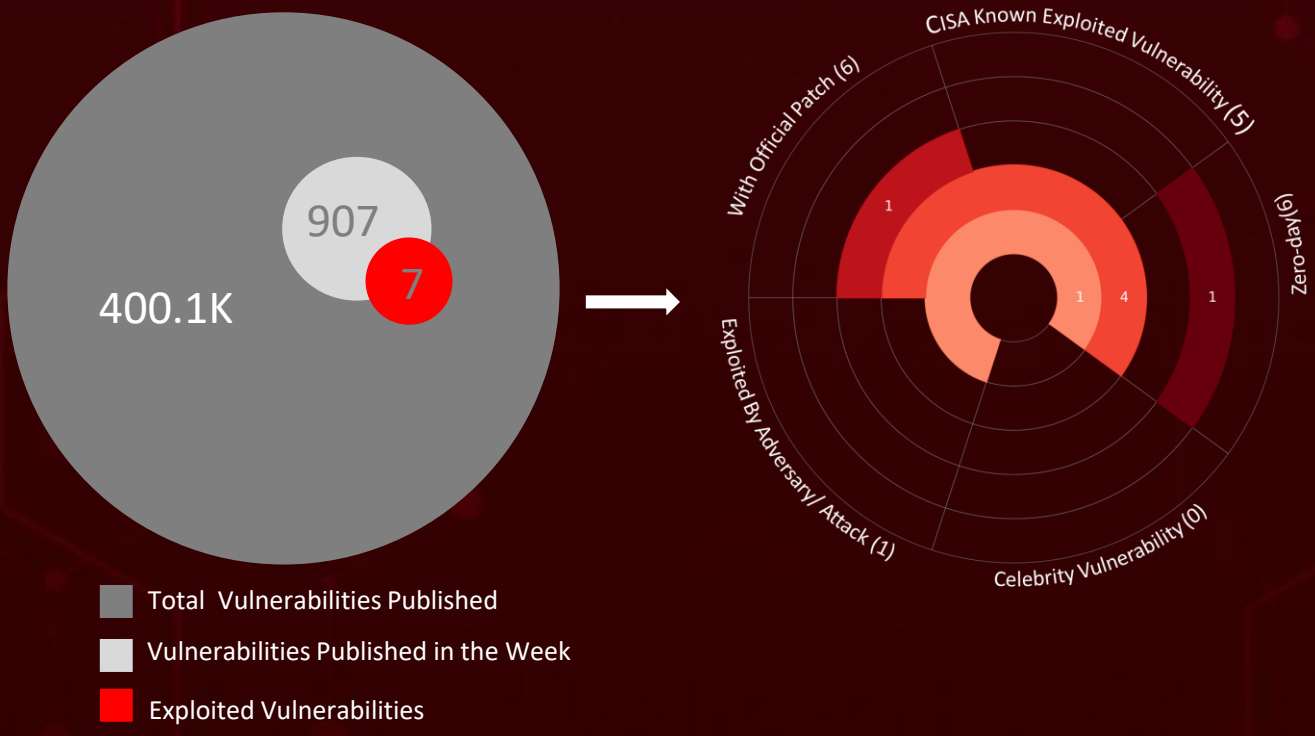
Table Of Contents

Summary

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

Microsoft's October 2025 Patch Tuesday fixes 196 vulnerabilities, including **three zero-days** across Windows and Microsoft products, requiring urgent patching. CVE-2025-11371 is an unauthenticated LFI in **Gladinet CentreStack/TrioFox** that exposes the ASP.NET machine key (via Web.config), enabling RCE when chained with CVE-2025-30406, actively exploited since Sept 2025 and unpatched, posing critical enterprise risk.

Additionally, **TA585** is a financially motivated group targeting finance & accounting firms with precision social-engineering and renting **MonsterV2**, a $800–$2,000/month MaaS offering remote access, data theft, and SonicCrypt-protected surveillance, making it a highly adaptive 2025 threat. In August 2025, a suspected China-linked actor gained persistent access to **F5 systems**, exfiltrating source code and vulnerability data, highlighting serious risks to enterprises and government networks. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

7
Attacks Executed

7
Vulnerabilities Exploited

2
Adversaries in Action

- Stealit
- Astaroth
- MonsterV2
- Lumma
- Rhadamanthys
- Medusa
- ValleyRAT

- CVE-2025-11371
- CVE-2025-30406
- CVE-2025-59230
- CVE-2025-47827
- CVE-2025-24990
- CVE-2025-53868
- CVE-2025-10035

- TA585
- Storm-1175

Insights

Astaroth targets Brazil with DocuSign-themed phishing that uses GitHub as resilient backup to load obfuscated JS/AutoIt in-memory loaders stealing banking and crypto credentials.

TA585 is a financially motivated group targeting finance firms with social-engineering lures and deploying **MonsterV2** MaaS for remote access, data theft, and surveillance.

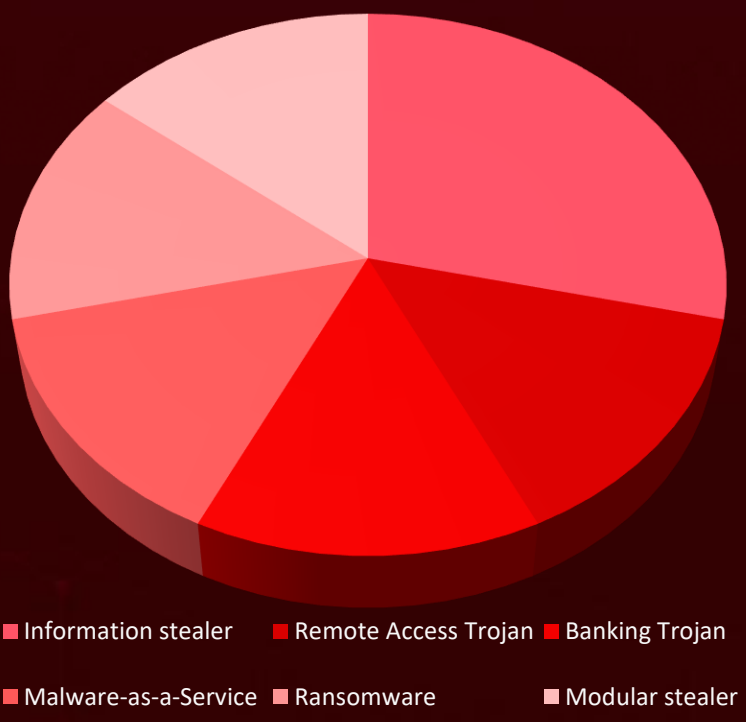
Operation Silk Lure targets fintech and crypto professionals with fake Chinese-language résumés delivering malicious .LNK files that install ValleyRAT for data theft and persistence.

CVE-2025-11371 unauthenticated LFI in Gladinet CentreStack/TrioFox exposing the Web.config machineKey and enabling RCE when chained with **CVE-2025-30406**.

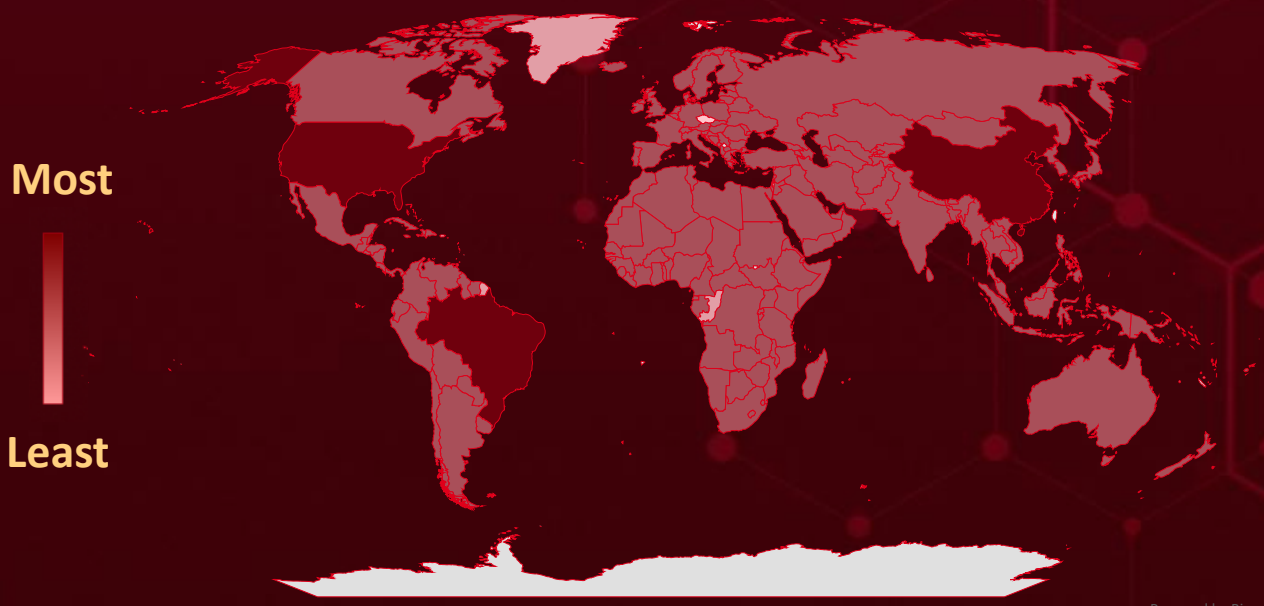
Microsoft's October 2025 Patch Tuesday fixes 196 vulnerabilities, including **3 zero-days**, across Windows, Office, SharePoint, Azure Entra ID, and more, addressing RCE, privilege escalation, and DoS issues.

Stealit's latest campaign showcases how threat actors are exploiting Node.js's SEA feature to deliver stealthy, standalone data-stealing malware disguised as legitimate software.

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
United States	Croatia	Qatar	Eritrea
Brazil	New Zealand	Cuba	Canada
China	Cyprus	Slovenia	Estonia
Mongolia	Peru	Austria	Myanmar
Italy	El Salvador	Tanzania	Eswatini
India	Russia	Czech Republic (Czechia)	Angola
Israel	Finland	Moldova	Ethiopia
Japan	South Korea	Denmark	Nigeria
Argentina	France	Nauru	Fiji
Singapore	Switzerland	Djibouti	Oman
Australia	Germany	North Macedonia	Belize
United Kingdom	Greece	Dominica	Papua New Guinea
Barbados	Ukraine	Cambodia	Benin
Mexico	St. Vincent & Grenadines	Dominican Republic	Poland
Belarus	Palau	Saint Kitts & Nevis	Gabon
Romania	Morocco	DR Congo	Albania
Belgium	Congo	Seychelles	Gambia
Netherlands	Sao Tome & Principe	Ecuador	Samoa
Turkey	Costa Rica	Chad	Georgia
Guatemala	Turkmenistan	Egypt	Senegal
Brunei	Côte d'Ivoire	Sweden	Bhutan
Jamaica	Nicaragua	Azerbaijan	Central African Republic
Colombia	Armenia	Tonga	Ghana
Kazakhstan		Equatorial Guinea	Somalia

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1190 Exploit Public-Facing Application

T1068 Exploitation for Privilege Escalation

T1566 Phishing

T1203 Exploitation for Client Execution

T1204 User Execution

T1566.001 Spearphishing Attachment

T1036 Masquerading

T1588 Obtain Capabilities

T1027 Obfuscated Files or Information

T1204.001 Malicious Link

T1486 Data Encrypted for Impact

T1588.005 Exploits

T1133 External Remote Services

T1059.001 PowerShell

T1082 System Information Discovery

T1588.006 Vulnerabilities

T1105 Ingress Tool Transfer

T1041 Exfiltration Over C2 Channel

T1078 Valid Accounts

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Stealit	Stealit is a sophisticated information-stealer that targets credentials, cryptocurrency wallets, and browser data. It is commonly distributed via phishing emails and malicious downloads. The malware operates stealthily, often bypassing antivirus software. It is designed to exfiltrate sensitive data to remote servers without user awareness.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular stealer		Data theft, Remote control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	554b318790ad91e330dced927c92974d6c77364ceddfb8c2a2c830d8b58e203c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Astaroth	A Latin American banking Trojan that uses sophisticated fileless techniques and abuses legitimate services like GitHub for configuration resilience. Its main goal is to steal banking and cryptocurrency credentials, primarily targeting South American countries.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Banking credentials	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	251cde68c30c7d303221207370c314362f4adccdd5db4533a67bedc2dc1e6195		

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 CVEs</th></tr>
<tr><td>MonsterV2</td><td rowspan="6">MonsterV2 is an advanced version of the Monster stealer family, focused on credential and cookie theft from browsers, cryptocurrency wallets, and messaging apps. It leverages Telegram bots or C2 panels for exfiltration and operates via loaders or spam campaigns. The malware’s new variant enhances obfuscation and persistence while expanding support for stealing data from password managers.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td rowspan="3">Malware-as-a-Service</td><td rowspan="3">Data theft, remote control</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>TA585</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">ccac0311b3e3674282d87db9fb8a151c7b11405662159a46dda71039f2200a67</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
Lumma Stealer	Lumma Stealer is a potent info-stealing malware that evadesdetection by injecting itself intomemory, employing multiplelayers of encryption andobfuscation. The payload,cleverly disguised as a Base64-encoded DLL concealed within ablock of French text, isspecifically crafted to bypassmost antivirus defenses.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Information stealer		Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
TA585			-

IOC TYPE	VALUE
SHA256	e17bf83e09457d8cecd1f3e903fa4c9770e17e823731650a453bc479591ac511, 0f6481dabf7871823f259eb95f3b85c37d1de8a7d1884ac77a97d887cf96f75d, 8d7f3d4905f17b6e488d485169fe6ace11a2f2771f432ebf25425179312fbb50, 6d41d871f00a12249ee90afb22a1da514b0ee0b16a0943a60e481d44f9b57be7, c7196ff93362110d20441bb1548884eff42deda49e759dc3e8a943a310f2b170

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
Rhadamanthys	Rhadamanthys is information-stealing malware distributed through large-scale phishing campaigns. It is designed to exfiltrate sensitive data from infected systems, including credentials and financial information. Targeting various sectors globally has been observed, often masquerading as legitimate communications to deceive victims.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Information stealer		Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
TA585			-
IOC TYPE	**VALUE**		
SHA256	9007661e48e9d4b325029b08a941aa99d315e33be6496380dacf238f0b95ccf3, 805f2fec37ed73461b715ba2ce6671213674ada9076ef24de833ec0d33a18c01, 07af486a9071194cb462bd6daa0634998861a99f342513b14ce702824e8c6dd1, 9007661e48e9d4b325029b08a941aa99d315e33be6496380dacf238f0b95ccf3, 06a9bf9c5f8039d2c7e180c218ac281139fb128e6fba020132d5f61b95040388		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Medusa	Medusa ransomware employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non-compliant organizations. Operating as a ransomware-as-a-service approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.	Phishing	CVE-2025-10035
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data theft	GoAnywhere MFT
ASSOCIATED ACTOR			**PATCH LINK**
Storm-1175			https://www.fortra.com/security/advisories/product-security/fi-2025-012
IOC TYPE	**VALUE**		
SHA256	6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da		

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>ValleyRAT</td><td rowspan="6">ValleyRAT is a multi-stage Remote Access Trojan (RAT) primarily targeting Chinese-speaking users via phishing campaigns. It conducts extensive system fingerprinting, captures screenshots and clipboard data, and includes routines to disrupt security products.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>RAT</td><td rowspan="4">Remote control</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">14bf52de60e60a526141ffe61ef5afc2a3bc7d60d4086e644ec80e67513d2684, b14996c4a93ff7d09795b113fb916c9588eb7efb4d64a1dbe190cfe937912209</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 PRODUCTS	ASSOCIATED ACTOR
CVE-2025-11371	✗	Gladinet CentreStack and Triofox: All versions prior to and including 16.7.10368.56560	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:* cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	-
Gladinet CentreStack and Triofox Unauthenticated Local File Inclusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-552	T1190 : Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalationn	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30406	✗	Gladinet CentreStack through 16.1.10296.56315	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:*	-
Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-321	T1552.004 Unsecured Credentials: Private Keys; T1190 : Exploit Public-Facing Application	https://www.centrestack.com/p/gce_latest_release.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-59230	✗	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-47827	✗	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
IGEL OS Use of a Key Past its Expiration Date Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-324	T1068: Exploitation for Privilege Escalation, T1547 : Boot or Logon Autostart Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-47827

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24990	✗	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Untrusted Pointer Dereference Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-822	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-24990

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53868	✗	F5 BIG-IP SCP and SFTP OS	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
F5 BIG-IP SCP and SFTP Appliance Mode Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://my.f5.com/manage/s/article/K000151902

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-10035</td><td>  </td><td rowspan="2">Fortra GoAnywhere MFT</td><td rowspan="2">Storm-1175</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*</td><td rowspan="2">Medusa ransomware</td></tr>
<tr><td rowspan="3">Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77
CWE-502</td><td>T1190: Exploit Public-Facing Application</td><td>https://www.fortra.com/security/advisories/product-security/fi-2025-012</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 TA585	-	Finance, Accounting	United States
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	MonsterV2, Lumma, Rhadamanthys	-

TTPs
TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; T1566.002: Spearphishing Link; T1199: Trusted Relationship; T1189: Drive-by Compromise; T1562: Impair Defenses; T1113: Screen Capture; T1071; TA0002: Execution; TA0040: Impact; TA0008: Lateral Movement; T1566: Phishing; T1547: Boot or Logon Autostart Execution; T1027: Obfuscated Files or Information; T1036; TA0003: Persistence; TA0010: Exfiltration; TA0011: Command and Control; T1204: User Execution; TA0007: Discovery; TA0009: Collection; T1053: Scheduled Task/Job; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1056: Masquerading; T1005: Data from Local System; T1071.001: Application Layer Protocol; T1021: Remote Services: Web Protocols: Input Capture; T1105: Ingress Tool Transfer; T1564.003: Hidden Window; T1059.001: PowerShell; T1562.001: Disable or Modify Tools; T1056.001: Keylogging; T1041: Exfiltration Over C2 Channel; T1564: Hide Artifacts

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Storm-1175	China	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-41244	Medusa ransomware	Fortra GoAnywhere MFT
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0010: Exfiltration; TA0040: Impact; TA0011: Command and Control; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1059: Command and Scripting Interpreter; T1133: External Remote Services; T1505.003: Web Shell; T1213: Data from Information Repositories; T1082: System Information Discovery; T1046: Network Service: Discovery; T1021.001: Remote Desktop: Protocol; T1090: Proxy: T1133: External Remote: Services; T1567.002: Exfiltration to Cloud: Storage; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for: Impact			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actor **TA585, Storm-1175** and malware **Stealit, Astaroth, MonsterV2, Lumma, Rhadamanthys, Medusa, ValleyRAT.**

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 **seven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to malware **Stealit, Astaroth, MonsterV2, ValleyRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Stealit’s New Trick: Packing Malware Inside Node.js Single Executables Inbox

CVE-2025-11371: Unpatched Gladinet Flaw Actively Exploited in the Wild

Astaroth Targets Brazil Using GitHub Infrastructure

TA585 Leverages ClickFix Technique and MonsterV2 Malware

Microsoft’s October 2025 Patch Tuesday

F5 BIG-IP Breach: Nation-State Hackers Expose Source Code and Undisclosed Flaws

Storm-1175's Masterstroke Exploits CVE-2025-10035 in GoAnywhere MFT

Operation Silk Lure Scam: When Job Hunts Leads to Malware

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
Stealit	SHA256	554b318790ad91e330dced927c92974d6c77364ceddfb8c2a2c830d8b58e203c
	URLs	https[:]//root[.]stealituptaded[.]lol/download/save_data, https[:]//root[.]stealituptaded[.]lol/download/stats_db, https[:]//root[.]stealituptaded[.]lol/download/game_cache
Astaroth	SHA256	251cde68c30c7d303221207370c314362f4adccdd5db4533a67bedc2dc1e6195
MonsterV2	SHA256	ccac0311b3e3674282d87db9fb8a151c7b11405662159a46dda71039f2200a67
Lumma	SHA256	e17bf83e09457d8cecd1f3e903fa4c9770e17e823731650a453bc479591ac511, 0f6481dabf7871823f259eb95f3b85c37d1de8a7d1884ac77a97d887cf96f75d, 8d7f3d4905f17b6e488d485169fe6ace11a2f2771f432ebf25425179312fbb50, 6d41d871f00a12249ee90afb22a1da514b0ee0b16a0943a60e481d44f9b57be7, c7196ff93362110d20441bb1548884eff42deda49e759dc3e8a943a310f2b170
Rhadamanthys	SHA256	9007661e48e9d4b325029b08a941aa99d315e33be6496380dacf238f0b95ccf3, 805f2fec37ed73461b715ba2ce6671213674ada9076ef24de833ec0d33a18c01,

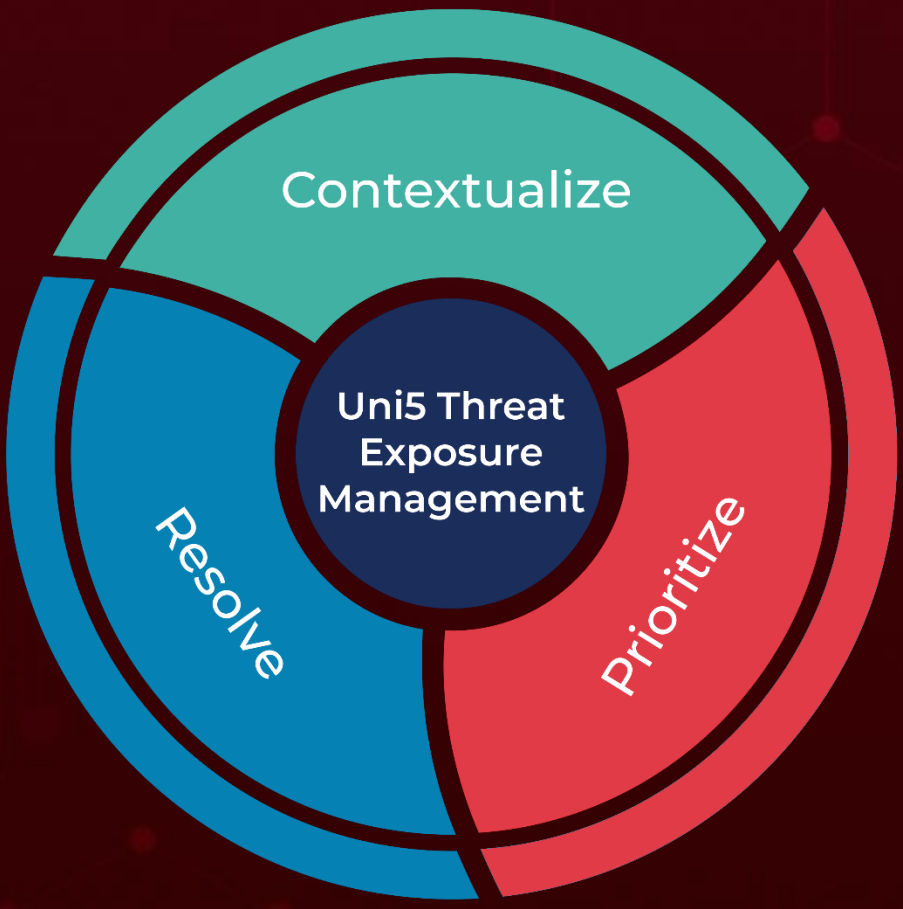
Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	07af486a9071194cb462bd6daa0634998861a99f342513b14ce702824e8c6dd1, 9007661e48e9d4b325029b08a941aa99d315e33be6496380dacf238f0b95ccf3, 06a9bf9c5f8039d2c7e180c218ac281139fb128e6fba020132d5f61b95040388
Medusa	SHA256	6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da
ValleyRAT	SHA256	14bf52de60e60a526141ffe61ef5afc2a3bc7d60d4086e644ec80e67513d2684, b14996c4a93ff7d09795b113fb916c9588eb7efb4d64a1dbe190cfe937912209

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

October 21, 2025 . 11:30 PM

More at www.hivepro.com