Date of Publication
November 4, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

OCTOBER 2025

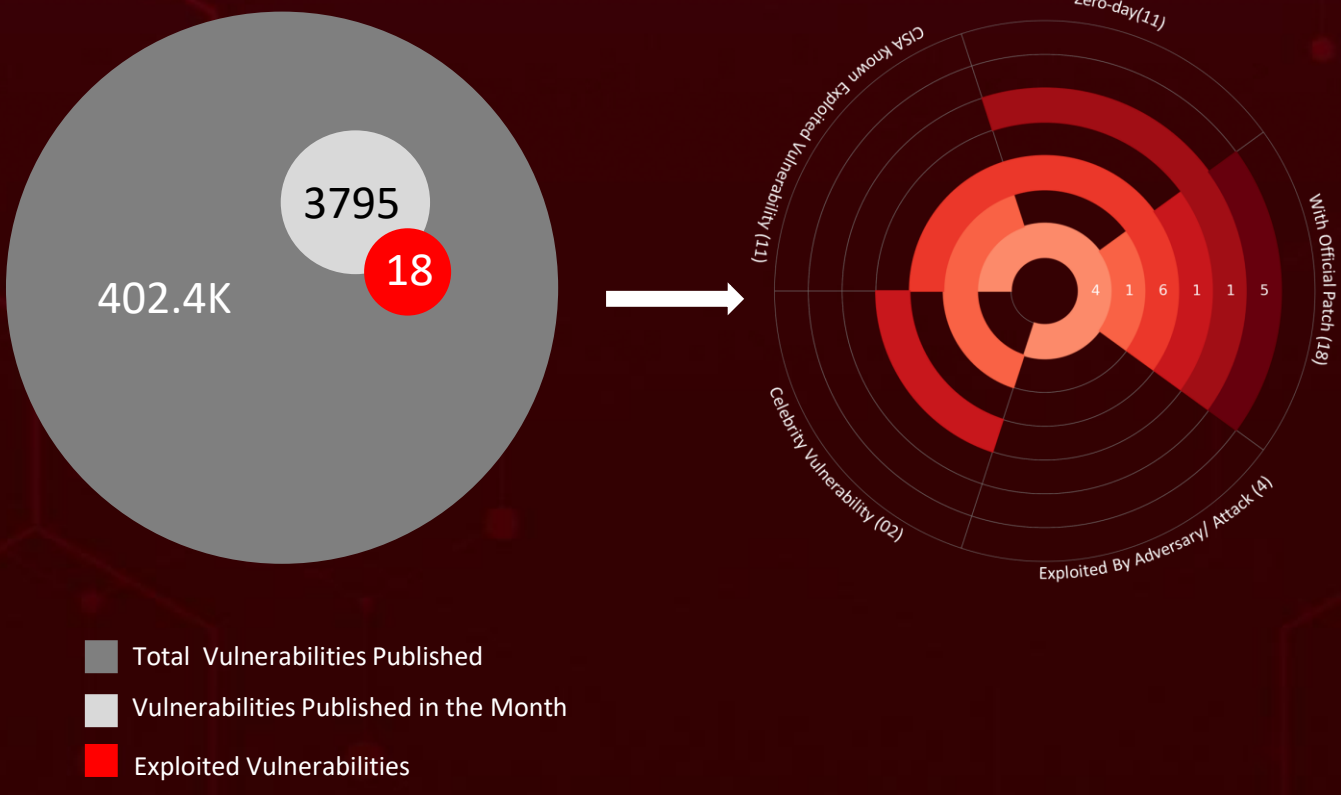
Table Of Contents

Summary

In **October**, the cybersecurity arena drew significant attention due to the active exploitation of **eleven zero-day** vulnerabilities. Among them, **CVE-2025-61932** affects Motex's Lanscope Endpoint Manager (on-premises), allowing remote adversaries to run arbitrary commands on endpoints by sending specially crafted packets, a threat leveraged in real-world attacks since April 2025.

During this period, ransomware attacks surged, with variants such as **FunkLocker, Cl0p, Medusa, and Qilin** aggressively targeting victims. **FunkLocker** is an AI-assisted ransomware from FunkSec that encrypts files with AES-256/RSA-2048, appends .funksec, and demands low ransoms to maximize victim payouts. **CVE-2025-61882**, is an unauthenticated remote code execution flaw in Oracle E-Business Suite (EBS). This weakness has been actively exploited by the **Cl0p ransomware** group since August 2025, with attack frequency surging after a proof-of-concept exploit was leaked in October 2025 by the collective known as **Scattered Lapsus$ Hunters**.

Concurrently, **fourteen** threat actors have engaged in various campaigns. Iran-linked **MuddyWater** has been phishing government and critical infrastructure entities across the Middle East and North Africa, deploying the Phoenix backdoor for intelligence collection. **Water Saci**, which spreads the **SORVEPOTEL** malware through WhatsApp, demonstrating the expanding reach of social engineering tactics. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

In October 2025, a geopolitical cybersecurity landscape unfolds, revealing **Brazil, India, United States, Serbia,** and **Pakistan,** as the top-targeted countries.

Highlighted in **October 2025** is a cyber battleground encompassing the **Defense, Financial, Government, Manufacturing,** and **Cryptocurrency** sectors, designating them as the top industries.

Qilin, aka **Agenda**, cements its place as **2025's** most aggressive ransomware, claiming **700** victims and counting.

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.

Vmware zero-day **CVE-2025-41244** exploited by **UNC5174** for root access and lateral movement.

APT36 pivots to Linux espionage with **DeskRAT**, blending deception, persistence, and precision against Indian defense networks.

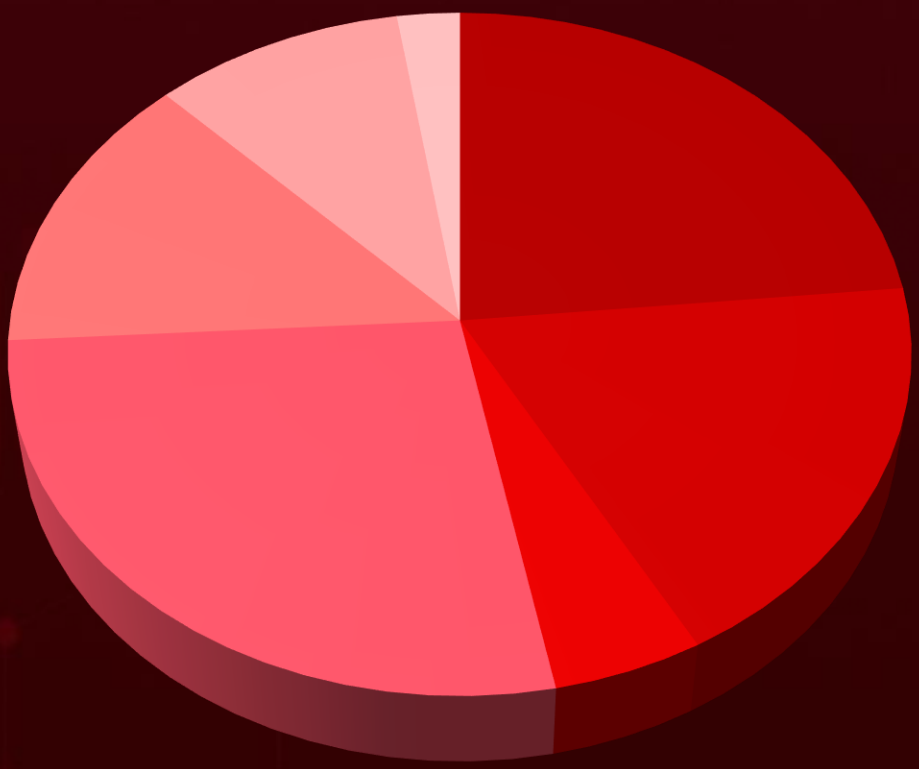
Azure Blob Storage has turned into a goldmine for attackers hunting misconfigurations and exposed data treasure.

Lazarus is expanding **Operation DreamJob** to infiltrate Europe's defense innovators shaping next-gen drone tech.

Cl0p Turns **Oracle E-Business Suite** Flaw Into Enterprise-Scale Ransomware Entry Point.

SessionReaper (CVE-2025-54236) is now being actively weaponized to hijack accounts and seize control of online stores.

Threat Landscape



Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-49844	RediShell	All Versions of Redis with Lua Scripting (Before 8.2.2)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redis:redis:*:*:*:*:*:*:*:*	-
Redis Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	https://github.com/redis/redis/releases/tag/8.2.2, https://redis.io/blog/security-advisory-cve-2025-49844/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-54236</td><td>SessionReaper</td><td rowspan="2">Adobe Commerce Versions: 2.4.9- alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6- p12, 2.4.5-p14, 2.4.4-p15 and earlier
Adobe Commerce B2B Versions: 1.5.3-alpha2, 1.5.2-p2, 1.4.2-p7, 1.3.4-p14, 1.3.3-p15 and earlier
Magento Open Source Versions: 2.4.9-alpha2, 2.4.8-p2, 2.4.7 p7, 2.4.6-p12, 2.4.5-p14 and earlier</td><td rowspan="2">-</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:adobe:commerce:-:*:*:*:*:*:*:*
cpe:2.3:a:adobe:commerce_b2b:-:*:*:*:*:*:*:*
cpe:2.3:a:adobe:magento:-:*:*:open_source:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Adobe Commerce and Magento Improper Input Validation Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1539: Steal Web Session Cookie</td><td>https://helpx.adobe.com/security/products/magento/apsb25-88.html</td></tr>
</table>

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-41244	VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability	VMware Aria Operations and VMware Tools	✓	✓	✓
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	✓	✓	✓
CVE-2025-49844	Redis Remote Code Execution Vulnerability	Redis	✗	✗	✓
CVE-2025-5947	WordPress Service Finder Bookings Plugin Authentication Bypass Vulnerability	WordPress Service Finder Bookings Plugin	✗	✗	✓
CVE-2025-27915	Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	✓	✓	✓
CVE-2025-11371	Gladinet CentreStack and Triofox Unauthenticated Local File Inclusion Vulnerability	Gladinet CentreStack and Triofox	✓	✗	✓
CVE-2025-30406	Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability	Gladinet CentreStack	✓	✓	✓
CVE-2025-59230	Microsoft Windows Improper Access Control Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-47827	IGEL OS Use of a Key Past its Expiration Date Vulnerability	IGEL OS	✓	✓	✓
CVE-2025-24990	Microsoft Windows Untrusted Pointer Dereference Vulnerability	Microsoft Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-53868	F5 BIG-IP SCP and SFTP Appliance Mode Bypass Vulnerability	F5 BIG-IP SCP and SFTP	✗	✗	✓
CVE-2025-10035	Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓
CVE-2025-54236	Adobe Commerce and Magento Improper Input Validation Vulnerability	Adobe Commerce and Magento	✗	✓	✓
CVE-2025-61932	Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability	Motex LANSCOPE Endpoint Manager	✓	✓	✓
CVE-2024-9234	WordPress GutenKit Plugin Unauthenticated Arbitrary File Upload Vulnerability	WordPress GutenKit Plugin	✗	✗	✓
CVE-2024-9707	WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	WordPress GutenKit Plugin	✗	✗	✓
CVE-2024-11972	WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	WordPress GutenKit Plugin	✗	✗	✓
CVE-2025-2783	Google Chromium Mojo Sandbox Escape Vulnerabili	Google Chromium	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Olymp Loader	Loader	-	Windows	-	-
FunkLocker	Ransomware	-	Windows	-	Phishing
WooperStealer	Stealer	-	Windows	-	Spear-phishing
AnonDoor	Backdoor	-	Windows	-	Spear-phishing
SORVEPOTEL	Hybrid Malware	-	Windows	-	Spear-phishing via WhatsApp
Cl0p	Ransomware	CVE-2025-61882	Oracle E-Business Suite	✓	Exploiting vulnerabilities
GOVERSHELL	Stealer	-	Windows	-	Spear-phishing
Ghost RAT	RAT	-	Windows	-	Compromised Web Server
Stealit	Modular stealer	-	Windows	-	-
Astaroth	Banking Trojan	-	Windows	-	Phishing
MonsterV2	Malware-as-a-Service	-	Windows	-	Phishing
Lumma	Information Stealer	-	Windows	-	Phishing
Rhadamanthys	Information Stealer	-	Windows	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Medusa	Ransomware	CVE-2025-10035	GoAnywhere MFT	✓	Phishing
ValleyRAT	RAT	-	Windows	-	Phishing
Phoenix Backdoor v4	Backdoor	-	Windows	-	Phishing
FakeUpdate Loader	Loader	-	Windows	-	Phishing
Chromium_Stealer	Stealer	-	Windows	-	Phishing
ScoringMathTea	RAT	-	-	-	Social Engineering
BinMergeLoader	Loader	-	-	-	Social Engineering
DeskRAT	RAT	-	Linux	-	Phishing
ModuleInstaller	Downloader	-	-	-	Phishing
StealerBot	Toolkit	-	-	-	Phishing
Qilin Ransomware	Ransomware	-	Windows and Linux	-	Phishing
Hijackloader	Loader	-	Windows	-	Phishing
PureHVNC	RAT	-	Windows	-	Phishing
LeetAgent	Spyware	CVE-2025-2783	Google Chrome	✓	Exploiting Vulnerability

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
FunkSec Group	Financial gain	-	CVE-2025-20333 CVE-2025-20362	RayInitiator bootkit, Line Viper loader	Cisco ASA and FTD
Confucius	Information Theft and Espionage	South Asia-based	-	WooperStealer, AnonDoor	Microsoft Windows
Scattered Spider	Financial gain	Suspected UK and US	CVE-2025-61882	-	Oracle E-Business Suite
ShinyHunters	Financial gain	-	CVE-2025-61882	-	Oracle E-Business Suite
LAPSUS$	Financial gain	Brazil	CVE-2025-61882	-	Oracle E-Business Suite
UTA0388	Information Theft and Espionage	China	-	GOVERSHELL	Windows

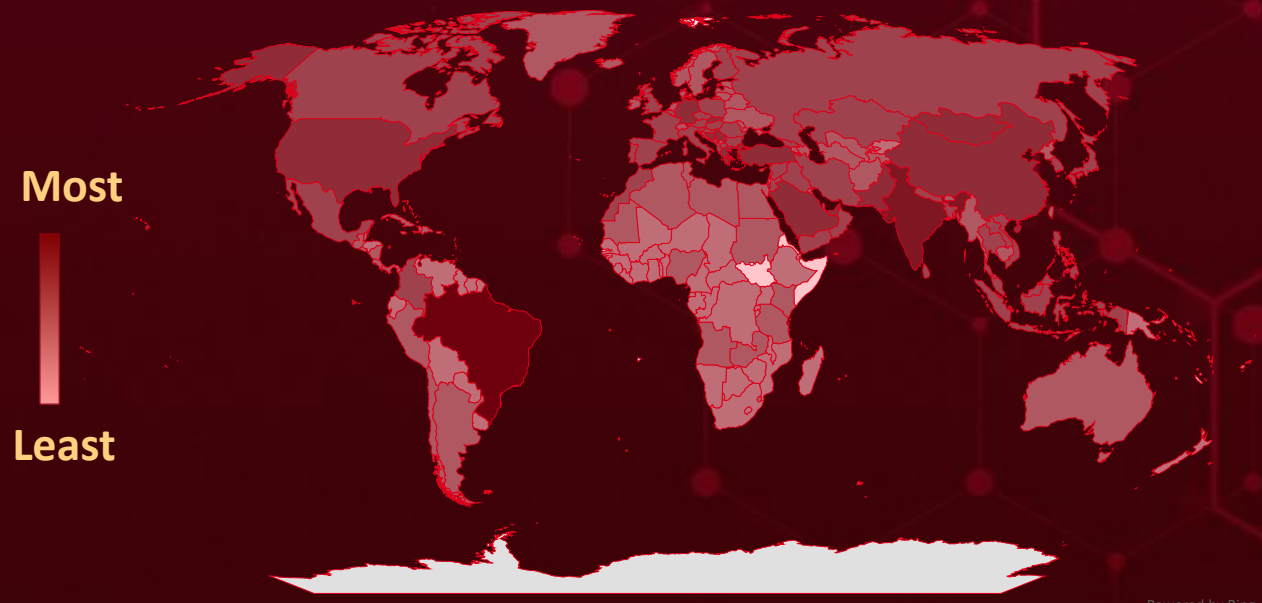
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
TA585	Financial gain	-	-	MonsterV2, Lumma, Rhadamanthys	-
Storm-1175	Financial gain	China	CVE-2025-41244	Medusa ransomware	Fortra GoAnywhere MFT
MuddyWater	Information Theft and Espionage	Iran	-	Phoenix Backdoor v4, FakeUpdate Loader, Chromium_Stealer	-
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	ScoringMathTea, BinMergeLoader	-
Transparent Tribe	Information theft and espionage	Pakistan	-	DeskRAT	-
CL-CRI-1032	Financial gain	Morocco	-	-	-
SideWinder	Information theft and espionage	India	-	ModuleInstaller, StealerBot	-
UNC6229	Financial gain	Vietnam	-	-	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
vmware	Application	VMware Cloud Foundation and VMware vSphere Foundation: VMware Cloud Foundation Operations Version Prior to 9.0.1.0, VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 3.0.5.0, Prior to 13.0.5, Prior to 12.5.4, VMware Cloud Foundation: VMware Aria Operations Version 5.x, 4.x, VMware Aria Operations Version Prior to 8.18.5
ORACLE	Enterprise application software	Oracle E-Business Suite versions 12.2.3-12.2.14
	Plugin	WordPress Service Finder Bookings Plugin Version Prior to 6.1, GutenKit Version Prior to 2.1.1, Hunk Companion Version Before and 1.8.4
zimbra A SYNACOR PRODUCT	Email and collaboration software suite	Zimbra Collaboration (ZCS) 9.0, 10.0, and 10.1
Gladinet	File Server Mobilization	Gladinet CentreStack and Triofox: All versions prior to and including 16.7.10368.56560

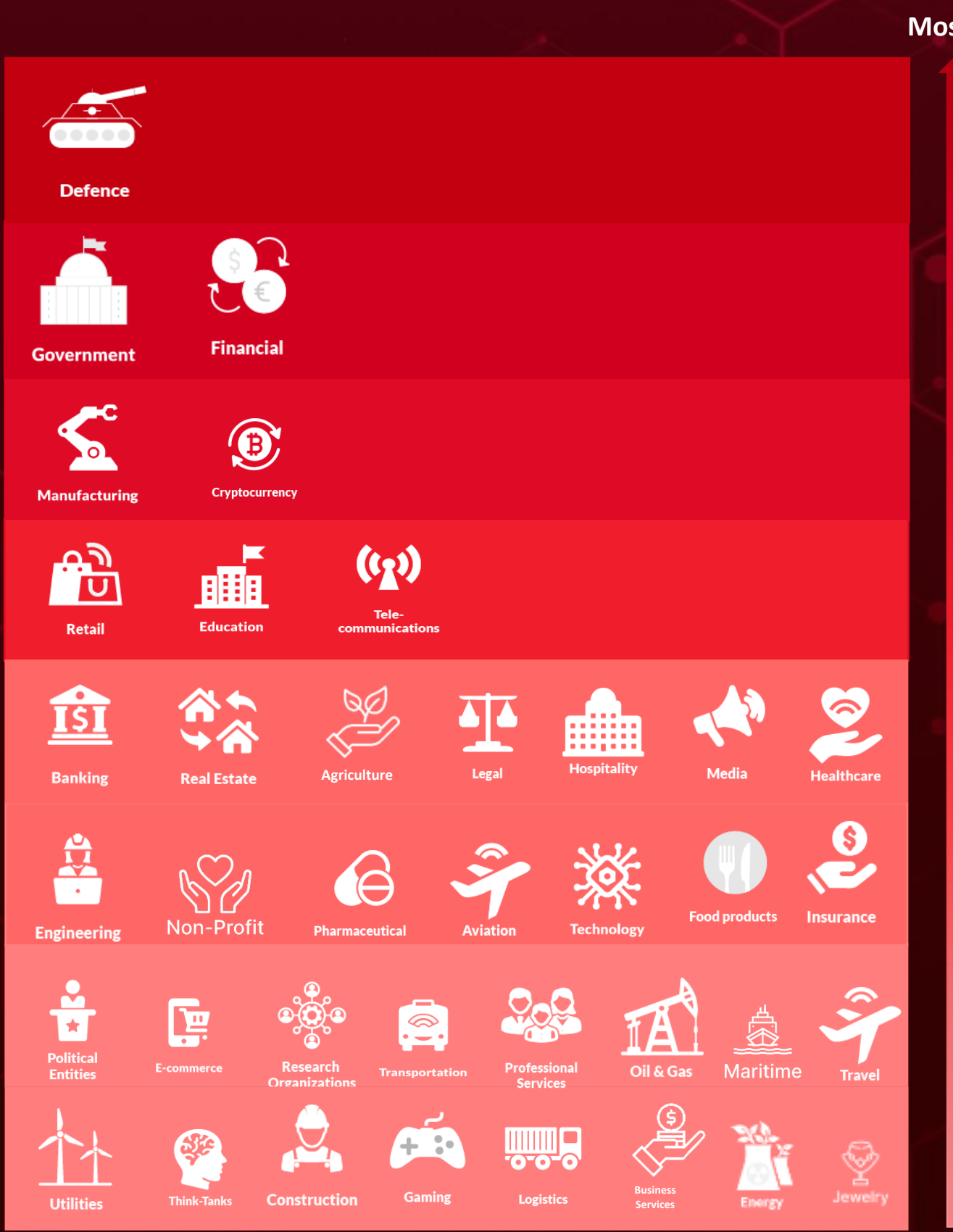
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Microsoft	Operating system	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2
f5	Application Delivery Controller (ADC) and Security	F5 BIG-IP SCP and SFTP OS
FORTRA GoAnywhere Managed File Transfer	Managed File Transfer	Fortra GoAnywhere MFT
LANSCOPE Endpoint Manager Cloud	Endpoint management and security	LANSCOPE Endpoint Manager On-Premise Version 9.4.7.1 and earlier Client Program (MR) Detection Agent (DA)
Chrome	Browser	Google Chrome (Windows) Version Prior to 134.0.6998.178

Targeted Countries



Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	Brazil		Georgia		Thailand		San Marino		Iceland
	India		Philippines		Qatar		Bahamas		Denmark
	United States		Bangladesh		Bulgaria		Trinidad and Tobago		Belize
	Serbia		Singapore		Russia		Algeria		Switzerland
	Pakistan		Belgium		Canada		North Korea		Bermuda
	China		Morocco		Czech Republic		Barbados		Dominica
	United Arab Emirates		Hong Kong		Yemen		Aruba		Bhutan
	Germany		Colombia		Finland		Greenland		Dominican Republic
	Mongolia		Hungary		Malaysia		Curacao		Jamaica
	Greece		Portugal		South Korea		Grenada		Egypt
	Saudi Arabia		Albania		Mexico		Tajikistan		Angola
	Slovakia		Croatia		Sri Lanka		Guadeloupe		Zambia
	Bosnia and Herzegovina		Indonesia		Bahrain		Turks and Caicos Islands		Anguilla
	Israel		Slovenia		France		Guatemala		Nigeria
	Turkey		Iran		Montenegro		Nicaragua		Kenya
	Romania		Syria		Jordan		Haiti		Norway
	North Macedonia		Iraq		United Kingdom		Cayman Islands		Kosovo
	Spain		Nepal		Kazakhstan		Holy See		Panama
			Austria		Vietnam		Armenia		Kuwait
			Oman		Laos		Belarus		Latvia
			Italy		Liechtenstein		Latvia		Puerto Rico
					Lebanon				

Targeted Industries



TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1566** Phishing
T1071 Application Layer Protocol	**T1036** Masquerading	**T1059.001** PowerShell	**T1588.006** Vulnerabilities	**T1041** Exfiltration Over C2 Channel
T1190 Exploit Public-Facing Application	**T1082** System Information Discovery	**T1486** Data Encrypted for Impact	**T1071.001** Web Protocols	**T1105** Ingress Tool Transfer
T1070 Indicator Removal	**T1005** Data from Local System	**T1140** Deobfuscate/Decode Files or Information	**T1068** Exploitation for Privilege Escalation	**T1547.001** Registry Run Keys / Startup Folder
T1083 File and Directory Discovery	**T1543** Create or Modify System Process	**T1562.001** Disable or Modify Tools	**T1203** Exploitation for Client Execution	**T1562** Impair Defenses

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
FunkLocker	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033
Cl0p	SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b
GOVERSHELL	IPv4:Port	80[.]85[.]154[.]48[:]443, 80[.]85[.]157[.]117[:]443, 82[.]118[.]16[.]173[:]443
	IPv4	104[.]194[.]152[.]137, 104[.]194[.]152[.]152, 185[.]144[.]28[.]68, 31[.]192[.]234[.]22, 45[.]141[.]139[.]222, 74[.]119[.]193[.]175, 80[.]85[.]156[.]234, 80[.]85[.]154[.]48, 80[.]85[.]157[.]117, 82[.]118[.]16[.]173
	Hostname	azure-app[.]store, twmoc[.]info, windows-app[.]store, cdn-apple[.]info, sliddeshare[.]online, doccloude[.]info
	URLs	hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ER_XG5FDkURHtsmna8vOQrIBRODKiQBKYJVKnI-kGKwX0A, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ESz4UV9JeOhOp8kiWd0Ie10ByH7eUdSRlBy2NCiNeo2LYw, hxxp[:]//1drv[.]ms/u/c/f9e3b332ce488781/Eap6_fxYFP5Eh1ZKDZaf8lMBjJNcfdba4MVcr4YfKj674w?e=fgNIj4, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ERpeLpJlb7FAkbfyuffpFJYBZ-8u2MmQH6LW5xH86B4M8w,

Attack Name	TYPE	VALUE
GOVERSHELL	URLs	hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/rar, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/zip, hxxp[:]//animated-dango-0fa8c8[.]netlify[.]app/file/Taiwan%20Intro[.]zip, hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/rar hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/zip hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/index/file/[PDF]202507_Please_check_the_document[.]zip hxxp[:]//dainty-licorice-db2b1e[.]netlify[.]app/file/zip hxxp[:]//dulcet-mooncake-36558c[.]netlify[.]app/file/zip hxxp[:]//harmonious-malabi-a8ebfa[.]netlify[.]app/file/Taiwan%20Intro[.]rar hxxp[:]//hllowrodcanlhelipme[.]netlify[.]app/file/zip hxxp[:]//jazzy-biscotti-68241f[.]netlify[.]app/files/Intro-Doc[.]rar hxxp[:]//ln5[.]sync[.]com/4[.]0/dl/100016f90#3d5wrb4z-hfb4iz3m-qmjzsqnq-39rn3vjv hxxp[:]//loveusa[.]netlify[.]app/file/rar hxxp[:]//pulicwordfiledownlos[.]netlify[.]app/file/rar hxxp[:]//spontaneous-selkie-d3346f[.]netlify[.]app/file/zip hxxp[:]//statuesque-unicorn-09420f[.]netlify[.]app/r hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/rar hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/zip hxxp[:]//vocal-crostata-86ebbf[.]netlify[.]app/files/zip wss[:]//api[.]twmoc[.]info/ws wss[:]//onedrive[.]azure-app[.]store/ws wss[:]//outlook[.]windows-app[.]store/ws www[.]twmoc[.]info hxxp[:]//app-site-association[.]cdn-apple[.]info[:]443/updates[.]rss
	SHA256	2ffe1e4f4df34e1aca3b8a8e93eee34bfc4b7876cedd1a0b6ca5d63d89a26301 4c041c7c0d5216422d5d22164f83762be1e70f39fb8a791d758a816cdf3779a9 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040 88782d26f05d82acd084861d6a4b9397d5738e951c722ec5afed8d0f6b07f95e 998e314a8babf6db11145687be18dc3b8652a3dd4b36c115778b7ca5f240aae4 a5ee55a78d420dbba6dec0b87ffd7ad6252628fd4130ed4b1531ede960706d2d ad5718f6810714bc6527cc86d71d34d8c556fe48706d18b5d14f0261eb27d942

Attack Name	TYPE	VALUE
GOVERSHELL	SHA256	fbade9d8a040ed643b68e25e19cba9562d2bd3c51d38693fe4be72e01da39861 7d7d75e4d524e32fc471ef2d36fd6f7972c05674a9f2bac909a07dfd3e19dd18 0414217624404930137ec8f6a26aebd8a3605fe089dbfb9f5aaaa37a9e2bad2e 126c3d21a1dae94df2b7a7d0b2f0213eeeec3557c21717e02ffaed690c4b1dbd, 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040
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
MonsterV2	SHA256	ccac0311b3e3674282d87db9fb8a151c7b11405662159a46dda71039f2200a67
Medusa	SHA256	6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da
Phoenix Backdoor v4	SHA256	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839, 1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56, 3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3, 76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75, 3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
DeskRAT	SHA256	567dfbe825e155691329d74d015db339e1e6db73b704b3246b3f015ffd9f0b33
Qilin Ransomware	SHA1	c150e4ab20d59affc62b916c2c90686f43040a9f
	SHA256	cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-41244	✗	VMware Cloud Foundation and VMware vSphere Foundation: VMware Cloud Foundation Operations Version Prior to 9.0.1.0, VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 3.0.5.0, Prior to 13.0.5, Prior to 12.5.4, VMware Cloud Foundation: VMware Aria Operations Version 5.x, 4.x, VMware Aria Operations Version Prior to 8.18.5	UNC5174 (aka Uteus)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vmware_cloud_foundation_operations:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_tools:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:*:*	-
VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-267	T1068: Exploitation for Privilege Escalation, T1036.005 Masquerading: Match Legitimate Resource Name or Location	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-61882</td><td>  </td><td rowspan="2">Oracle E-Business Suite versions 12.2.3-12.2.14</td><td rowspan="2">Scattered Spider, ShinyHunters, and LAPSUS$</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:oracle:concurrent_processing:*:*:*:*:*:*:*:*</td><td rowspan="2">Cl0p Ransomware</td></tr>
<tr><td rowspan="3">Oracle E-Business Suite Unspecified Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-22
CWE-444</td><td>T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter</td><td>https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/rs?type=doc&id=3106344.1</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-5947	✗	WordPress Service Finder Bookings Plugin Version Prior to 6.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:service_finder_bookings_plugin:service_finder_bookings_plugin:*:*:*:*:*:*:*:*	-
WordPress Service Finder Bookings Plugin Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-639	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://themeforest.net/item/service-finder-service-and-business-listing-wordpress-theme/15208793?srsltid=AfmBOoq5ifHWqLc8b5o0Q7gjSz6HEpbHfquXWh-KhP0FWnFBTCFLaBzH

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-27915	✗	Zimbra Collaboration (ZCS) 9.0, 10.0, and 10.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.13, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.5, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P44

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	https://www.centrestack.com/p/gce_latest_release.html

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

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

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-61932</td><td>  </td><td rowspan="2">LANSCOPE Endpoint Manager On-Premise Version 9.4.7.1 and earlier Client Program (MR) Detection Agent (DA)</td><td rowspan="2">-</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:motex:lanscope_endpoint_manager:*:*:*:*:on-premise:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-940</td><td>T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services; T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution</td><td>https://www.motex.co.jp/news/notice/2025/release251020/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9234	✗	GutenKit Version Prior to 2.1.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wpmet:gutenkit:*:*:	-
WordPress GutenKit Plugin Unauthenticated Arbitrary File Upload Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://wordpress.org/plugins/gutenkit-blocks-addon/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9707	✗	Hunk Companion Version Before and 1.8.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:themehunk:hunk_companion:*:*:*:*:*:wordpress:*:*	-
WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://wordpress.org/plugins/hunk-companion/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11972	✗	Hunk Companion Version Before and 1.8.5	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:themehunk:hunk_companion:*:*:*:*:*:wordpress:*:*	-
WordPress Hunk Companion Plugin Unauthenticated Arbitrary Plugin Activation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://wordpress.org/plugins/hunk-companion/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2783	✗	Google Chrome (Windows) Version Prior to 134.0.6998.178	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	LeetAgent
Google Chromium Mojo Sandbox Escape Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting; T1497: Virtualization/Sandbox Evasion	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Olymp Loader	Olymp Loader is an emerging Malware-as-a-Service (MaaS), heavily advertised as "fully undetectable" (FUD) and notably written entirely in assembly language. It functions primarily as a versatile loader to stealthily deliver second-stage malware, such as credential stealers (e.g., LummaC2) and Remote Access Trojans.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FunkLocker	FunkLocker is an AI-assisted ransomware strain developed by the FunkSec group, which operates under a ransomware-as-a-service model. The group blends cybercrime and hacktivism, targeting a wide range of public and private sector organizations worldwide. Ransom demands are relatively low typically around 0.1 Bitcoin, encouraging faster payments and increasing the number of victims.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data encryption, Data Exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
FunkSec Group			-

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
WooperStealer	WooperStealer is a type of information-stealing malware that is configured to enumerate and collect files with specific extensions across an infected host. After gathering this data, it transmits the stolen files to a designated remote endpoint	Spear-phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Exfiltration and Confidentiality Loss	Windows
Stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
Confucius			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AnonDoor	AnonDoor is a Python-based persistent backdoor that also serves as a centralized loader for modular payloads. It facilitates sustained access and detailed host profiling, including screenshots and enumeration of files and disk volumes. Heavier operations are throttled to run no more than once every six minutes, minimizing observable activity and redundant data transfers.	Spear-phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Sustained Remote Access, Host Profiling & Reconnaissance	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Confucius			-

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
SORVEPOTEL	Water Saci is a malicious campaign that spreads SORVEOTEL, a hybrid malware. It uses deceptive messages with ZIP attachments that execute PowerShell commands to load additional payloads directly into memory. SORVEOTEL can hijack active WhatsApp Web sessions to propagate infected files to contacts and deploy convincing banking overlays to harvest credentials.	Spear-phishing via WhatsApp	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential Theft, Financial Loss	Windows
Hybrid Malware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Cl0p	The Cl0p ransomware group has escalated its attacks, particularly after the October 2025 leak of a proof-of-concept exploit for an Oracle EBS zero-day. The group has been involved in campaigns that combine data theft with double extortion tactics. Key indicators of compromise include unauthorized web shells, outbound command-and-control traffic, and stolen application credentials.	Exploiting vulnerabilities	CVE-2025-61882
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	Oracle E-Business Suite
Ransomware			
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/ https://support.oracle.com/rs?type=doc&id=3106344.1

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
GOVERSHELL	GOVERSHELL is a sophisticated backdoor malware that leverages search-order hijacking to deploy itself through malicious archives. Once executed, it establishes persistent access to compromised systems, allowing attackers to control the target remotely.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Remote Access, Data Exfiltration	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UTA0388			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Ghost RAT	The Ghost RAT attack began when a phpMyAdmin panel was accidentally exposed online due to a DNS misconfiguration. The attacker, using an AWS IP from Hong Kong, quickly changed the interface to Simplified Chinese and executed SQL commands. They exploited a logging misconfiguration and directory traversal flaw to inject a PHP web shell into the MariaDB logs, creating a hidden backdoor. The malware used multiple stages to evade detection and maintained persistence by masquerading as a Windows service called SQLite.	Compromised Web Server	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Sustained Remote Access, Operational Disruption	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
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**
-			-

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**
-			-

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
MonsterV2	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.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Malware-as-a-Service		Data theft, remote control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
TA585			-

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			-

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			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ValleyRAT	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.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
Phoenix Backdoor v4	Phoenix is a compact, stealthy backdoor linked to MuddyWater that fingerprints infected Windows hosts, attempts to create a mutex named sysprocupdate.exe, and installs a copy to maintains persistence by altering the current user's registry autostart and reaches out to its operators over WinHTTP to fetch and execute commands. This observed v4 sample also contains an embedded Portable Executable inside the binary that was not dropped or run during normal operation, implying a dormant capability the operator could enable later.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FakeUpdate Loader	FakeUpdate is an injector-style loader that uses AES at runtime to decrypt an embedded second-stage payload and then injects the decrypted code into its own process for execution. It operates as a covert bootstrap, remaining quiet on disk and exposing the payload only after in-memory decryption and self-injection.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Loads Malware	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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
Chromium_Stealer	Chromium_Stealer is a custom credential-harvesting tool that masquerades as a harmless calculator-style app to evade detection. Its primary purpose is to locate browser profiles, extract the browser master key, and then read the profile's Login Data databases to retrieve stored credentials. To ensure it can access locked files, it will terminate running browser processes, decrypt stored passwords in memory using the recovered master key, and write the results into a local staging file. The credentials in that file are stored in an encrypted form. After harvesting, the malware attempts to restart the browser from its previous state to reduce user suspicion.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ScoringMathTea	ScoringMathTea is a remote-access trojan first observed in late 2022 that gives operators near-complete control of infected hosts. It was quickly adopted by Lazarus during Operation DreamJob and has remained their go-to post-compromise payload for about three years, reappearing across multiple campaigns. The RAT talks to command-and-control infrastructure hosted on compromised servers; investigators often find the server-side components concealed inside WordPress sites, typically buried in theme or plugin directories to hide in plain sight. Its combination of reliable remote-control features and a stealthy C2 hosting approach makes it well-suited for long-term access and follow-up operations.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

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
BinMergeLoader	BinMergeLoader is a lightweight loader in the same family as MISTPEN that abuses legitimate Microsoft cloud tooling to blend in. It authenticates with Microsoft API tokens and uses the Microsoft Graph API as its command-and-control and delivery channel, giving operators a stealthy, high-privilege pathway into Microsoft 365 resources and endpoints.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Loads Malware	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DeskRAT	DeskRAT is a custom Golang-built Remote Access Trojan engineered to compromise Linux environments with surgical stealth: it chains dropper scripts, convincing decoy PDFs, and multiple Linux-specific startup mechanisms to gain persistent, long-term access, quietly exfiltrate files, and maintain remote control. Notably tailored to target systems running the BOSS Linux distribution, widely used within some Indian government organizations, DeskRAT blends social-engineering lures with platform-aware persistence tricks to evade detection and ensure the attacker's foothold endures.	Spear-phishing attacks	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
RAT		System Compromise	Linux (Specifically BOSS distributions)
ASSOCIATED ACTOR			**PATCH LINK**
Transparent Tribe			-

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
StealerBot	StealerBot is a private post-exploitation toolkit, designed for espionage and stealthy data theft. Developed in .NET, it operates as a modular implant, avoiding traditional file-based execution by loading its components directly into memory via ModuleInstaller, a backdoor loader named by the attackers. StealerBot features multiple modules for deploying additional malware, capturing screenshots, logging keystrokes, stealing browser passwords and files, phishing Windows credentials, and escalating privileges by bypassing UAC, making it a versatile tool for persistent access and data exfiltration.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise, Data Theft	-
Toolkit			
ASSOCIATED ACTOR			**PATCH LINK**
SideWinder			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Qilin Ransomware	Qilin, also known as Agenda, is a prolific Ransomware-as-a-Service operation that supplies its encryption toolkit to affiliate actors, who commonly employ double-extortion tactics: they both encrypt victims' files and steal sensitive data to threaten public release unless a ransom is paid. Beyond the usual RaaS playbook, a major 2025 evolution lets affiliates run a Linux ransomware variant on Windows hosts by abusing legitimate remote-management and file-transfer tools such as AnyDesk, ScreenConnect, and Splashtop; this cross-platform trick evades many Windows-focused detection controls and improves stealth inside mixed-OS environments, making Qlin/Agenda attacks harder to spot and more damaging when they succeed.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise, Encrypt Data	Windows and Linux
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
Hijackloader	Hijackloader is a stealthy loader first seen in July 2023 that serves as a delivery platform for a variety of follow-on malware; it combines sophisticated evasion and abuse of Windows internals, using Process Doppelgänging to run from altered in-memory images, Heaven's Gate to flip between 32- and 64-bit contexts, and DLL search-order/DLL side-loading tricks so attacker libraries are loaded instead of legitimate ones, making detection and forensic analysis difficult.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Loads other payloads	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PureHVNC	PureHVNC is a customized Remote Access Trojan (RAT) that gives attackers full Control over the infected systems. Often obfuscated with .NET Reactor, it enables keylogging, data theft, and remote desktop access for surveillance and system control.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
LeetAgent	LeetAgent is the spyware deployed in the Operation ForumTroll campaign; its name reflects the quirks of the codebase, where command names are written in leetspeak. The implant reads a configuration to contact one of several hardcoded C2 servers over HTTPS, then receives numeric command identifiers it maps to actions and executes them remotely. Built-in traffic-obfuscation options and a polished command/response design suggest LeetAgent may be a commercial or commoditized tool.	Exploiting Vulnerability	CVE-2025-2783
		IMPACT	AFFECTED PRODUCT
TYPE		Data spying, Data theft	Google Chrome
Spyware			
ASSOCIATED ACTOR			PATCH LINK
-			https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ModuleInstaller	ModuleInstaller is a stealthy downloader that establishes and sustains an attacker's foothold on compromised systems: it retrieves configuration files that tell it which components to fetch, usually a seemingly legitimate application alongside a malicious DLL, and then uses that DLL as the loader for the final-stage payload, enabling persistent execution and further payload delivery.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Load other payloads	-
Downloader			
ASSOCIATED ACTOR			PATCH LINK
SideWinder			-

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 FunkSec Group	-	Government, Defense, Finance, Higher Education	United States, India, Spain, Mongolia, Italy, Brazil, Israel
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-20333 CVE-2025-20362	RayInitiator bootkit, Line Viper loader	Cisco ASA and FTD
TTPs			
TA0001: Initial Access; TA0005: Defense Evasion; T1190: Exploit Public-Facing Application; T1543: Create or Modify System Process; T1068; TA0002: Execution; TA0040: Impact; T1078: Valid Accounts; T1562; TA0003: Persistence; TA0004: Privilege Escalation; TA0042: Resource Development; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1569: System Services; T1569.002: Service Execution; T1529: System Shutdown/Reboot; T1542.001: System Firmware; T1070: Impair Defenses; T1588.006: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1486 : Data Encrypted for Impact; T1588: Obtain Capabilities			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="3"> 
Confucius (aka G0142)</td><td>South Asia-based</td><td rowspan="3">Government Agencies, Military Organizations, Defense Contractors, Critical Infrastructures</td><td rowspan="3">Pakistan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td rowspan="2"></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>WooperStealer, AnonDoor</td><td>Microsoft Windows</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; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1041: Exfiltration Over C2 Channel; T1112: Modify Registry; T1005: Data from Local System; T1083: File and Directory Discovery; T1087: Account Discovery; T1113: Screen Capture; T1027: Obfuscated Files or Information</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)</td><td>Suspected UK and US</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61882</td><td>-</td><td>Oracle E-Business Suite</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
ShinyHunters</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61882</td><td>-</td><td>Oracle E-Business Suite</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
LAPSUS$ (aka DEV-0537, Strawberry Tempest, Slippy Spider, G1004)</td><td>Brazil</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61882</td><td>-</td><td>Oracle E-Business Suite</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0007: Discovery; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1505: Server Software Component; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts; T1210: Exploitation of Remote Services; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UTA0388 (aka UNK_DropPitch)</td><td>China</td><td rowspan="3">Manufacturing, Investment firms, Semiconductor</td><td rowspan="3">North America, Asia, and Europe</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>GOVERSHELL</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0011: Command and Control; TA0005: Defense Evasion; TA0040: Impact; T1574.001: DLL Search Order Hijacking; T1574: Hijack Execution Flow; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1036: Masquerading; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1071.004: DNS; T1203: Exploitation for Client Execution; T1588.007: Artificial Intelligence; T1588: Obtain Capabilities; T1598.003: Spearphishing Link; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1486: Data Encrypted for Impact; T1059: Command and Scripting Interpreter</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="4"> 
TA585</td><td>-</td><td rowspan="3">Finance, Accounting</td><td rowspan="3">United States</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>MonsterV2, Lumma, Rhadamanthys</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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</td></tr>
</table>

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			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)</td><td>Iran</td><td rowspan="2">Government, Diplomatic, Foreign Affairs Ministries and Consulates, Telecommunications, International Organizations</td><td rowspan="2">Middle East and North Africa (MENA)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Phoenix Backdoor v4, FakeUpdate Loader, Chromium_Stealer</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0009: Collection; TA0006: Credential Access; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1547.001: Registry Run Keys / Startup Folder; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1219: Remote Access Software; T1027: Obfuscated Files or Information; T1586: Compromise Accounts; T1564.001: Hidden Files and Directories; T1564: Hide Artifacts; T1555: Credentials from Password Stores; T1082: System Information Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1555.003: Credentials from Web Browsers; T1090.002: External Proxy; T1090: Proxy; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1059.005: Visual Basic; T1059.001: PowerShell; T1547.004: Winlogon Helper DLL; T1546.015: Component Object Model Hijacking; T1546: Event Triggered Execution; T1055: Process Injection; T1055.002: Portable Executable Injection; T1140: Deobfuscate/Decode Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1112: Modify Registry; T1027.002: Software Packing; T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Lazarus (aka 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, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, G0032)	North Korea	Engineering, Manufacturer of Aircraft Components, Defense Company	Southeastern and Central Europe
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	ScoringMathTea, BinMergeLoader	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1584: Compromise Infrastructure; T1584.004: Server; T1587: Develop Capabilities; T1587.001: Malware; T1106: Native API; T1129: Shared Modules; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.001: DLL; T1134: Access Token Manipulation; T1134.002: Create Process with Token; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1620: Reflective Code Loading; T1055: Process Injection; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel; T1036: Masquerading; T1566: Phishing

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Transparent Tribe (aka Mythic Leopard, APT36, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, C-Major)	Pakistan	Military, Defense, and Government Organizations	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	DeskRAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0009: Collection; TA0011: Command and Control; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1140: Deobfuscate/Decode Files or Information; T1204.002: Malicious File; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1027: Obfuscated Files or Information; T1041: Exfiltration Over C2 Channel; T1082: System Information Discovery; T1005: Data from Local System; T1564.001: Hidden Files and Directories; T1564: Hide Artifacts			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 CL-CRI-1032	Morocco	Retail, Consumer Services	Worldwide
	MOTIVE		
	Financial Theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	-	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0040: Impact; TA0043: Reconnaissance; TA0042: Resource Development; T1589: Gather Victim Identity Information; T1564: Hide Artifacts; T1564.008: Email Hiding Rules; T1070: Indicator Removal; T1070.008: Clear Mailbox Data; T1586: Compromise Accounts; T1078: Valid Accounts; T1078.002: Domain Accounts; T1530: Data from Cloud Storage; T1566.002: Spearphishing Link; T1566: Phishing; T1078.004: Cloud Accounts; T1057: Process Discovery; T1087.003: Email Account; T1087: Account Discovery; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1098: Account Manipulation; T1036: Masquerading; T1496: Resource Hijacking; T1591: Gather Victim Org Information; T1598: Phishing for Information; T1588: Obtain Capabilities; T1189: Drive-by Compromise; T1199: Trusted Relationship; T1531: Account Access Removal

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 SideWinder (aka Rattlesnake, Razor Tiger, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21, G0121)	India	Diplomats	Sri Lanka, Pakistan, Bangladesh, India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	ModuleInstaller, StealerBot	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1087: Account Discovery; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.008: Stripped Payloads; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1027.016: Junk Code Insertion; T1218: System Binary Proxy Execution; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1083: File and Directory Discovery; T1012: Query Registry; T1652: Device Driver Discovery; T1005: Data from Local System; T1119: Automated Collection; T1560: Archive Collected Data; T1560.002: Archive via Library; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1105: Ingress Tool Transfer; T1090: Proxy; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6229	Vietnam	Digital Advertising, Marketing	Worldwide
	MOTIVE		
	Financial Theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0040: Impact; TA0043: Reconnaissance; TA0042: Resource Development; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1212: Exploitation for Credential Access; T1078: Valid Accounts; T1219: Remote Access Software; T1036: Masquerading; T1608: Stage Capabilities; T1608.004: Drive-by Target; T1098: Account Manipulation; T1199: Trusted Relationship; T1586: Compromise Accounts; T1586.001: Social Media Accounts; T1657: Financial Theft; T1531: Account Access Removal; T1667: Email Bombing; T1589: Gather Victim Identity Information; T1589.001: Credentials			

MITRE ATT&CK TTPS

Tactic	Technique	Sub_Technique
TA0001: Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1195: Supply Chain Compromise	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1203: Exploitation for Client Execution	
	T1651: Cloud Administration Command	
	T1106: Native API	
	T1129: Shared Modules	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution

Tactic	Technique	Sub_Technique
TA0003: Persistence	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1098: Account Manipulation	
	T1112: Modify Registry	
	T1136: Create Account	T1136.001: Local Account
		T1136.003: Cloud Account
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1484.001: Group Policy Modification

Tactic	Technique	Sub_Technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.003: CMSTP
		T1218.005: Mshta
		T1218.007: Msiexec
		T1218.011: Rundll32
	T1497: Virtualization/Sandbox Evasion	
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1620: Reflective Code Loading	
	T1656: Impersonation	T1484.001: Group Policy Modification
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
		T1003.003: NTDS

Tactic	Technique	Sub_Technique
TA0006: Credential Access	T1056: Input Capture	T1056.001: Keylogging
		T1056.001: Keylogging
	T1110: Brute Force	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
		T1087.004: Cloud Account
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	T1518.001: Security Software Discovery
		T1614.001: System Language Discovery

Tactic	Technique	Sub_Technique
TA0009: Collection	T1530: Data from Cloud Storage	
	T1185: Browser Session Hijacking	
	T1115: Clipboard Data	
	T1056: Input Capture	T1056.001: Keylogging
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1119: Automated Collection	
	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1011: Exfiltration Over Other Network Medium	
	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1537: Transfer Data to Cloud Account	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1568.003: DNS Calculation

Tactic	Technique	Sub_Technique
TA0040: Impact	T1489: Service Stop	
	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.002: External Defacement
	T1498: Network Denial of Service	
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.005: Botnet
		T1583.006: Web Services
	T1584: Compromise Infrastructure	
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.004: Digital Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
TA0043: Reconnaissance	T1591: Gather Victim Org Information	T1591.001: Determine Physical Locations
	T1592: Gather Victim Host Information	
	T1598: Phishing for Information	T1598.001: Spearphishing Service
		T1598.002: Spearphishing Attachment
		T1598.004: Spearphishing Voice
		T1590.002: DNS
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1568.003: DNS Calculation

Tactic	Technique	Sub_Technique
TA0008: Lateral Movement	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
		T1550.002: Pass the Hash
	T1570: Lateral Tool Transfer	
	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1072: Software Deployment Tools	
	T1210: Exploitation of Remote Services	

Top 5 Takeaways

#1 In October, there were seven zero-day vulnerabilities, with the standout "**celebrity**" vulnerability, **RediShell**, taking center stage. Meanwhile, SessionReaper (CVE-2025-54236) in Adobe Commerce and Magento Open Source enables unauthenticated attackers to hijack customer accounts and potentially execute malicious code on targeted systems.

#2 Ransomware is on the rise, with relentless variants like **FunkLocker, Cl0p, Medusa, and Qilin,** claiming new victims. As attacks grow more sophisticated, organizations must act fast strengthening defenses, securing backups, and refining disaster recovery plans to stay ahead of the threat.

#3 Cyberattacks hit **223** countries in October, with **Brazil, India, United States, Serbia, and Pakistan,** facing the brunt of the threats. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region was immune as adversaries expanded their reach globally.

#4 The **Defense, Financial, Government, Manufacturing, and Cryptocurrency** sectors were prime targets, with ransomware, data theft, and espionage campaigns wreaking havoc. As attackers refine their tactics, organizations in these industries must stay ahead with proactive security measures.

#5 A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **GOVERSHELL, Ghost RAT, MonsterV2, Medusa, Phoenix Backdoor v4.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **18 significant vulnerabilities** and block the indicators related to the **14 active threat actors, 27 active malware,** and **215 potential MITRE TTPs.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

• Running a scan to discover the assets impacted by the **18 significant vulnerabilities.**

• Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

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 malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Social engineering: is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

Supply chain attack: Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

Eavesdropping: Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
CVE - Common Vulnerabilities and Exposures
CPE - Common Platform Enumeration
CWE - Common Weakness Enumeration

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Olymp Loader	SHA256	7bc217f0ee12266d42812af436f494caf599c0705242457a581f64d4eb508904, d36da9c3e5e78aa87bcdcd7fc8d3499d85a60b9dd107bf775d759940fc2f2489, D167a0c6fdba1175b67f10daf4be218b4d8adf2f81280ba5d1510228a4321bca, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23, ff1e159c4c6fcb97c9cb1885796fa4557e1afb92c82ada00f24ae994bffd63e4, 9464a2a1fb53b3a8c783ee4b55bba69cbb74a841f0d06f0cef86a93d607be5ae, 59b143fd884f8450cf5161954ebf38dbd9c951ecdb13de5e1f6aea01a9f92201, 60fec45a29a89c1cb10fd793065e8fc39bdae15daf813e3438e8ff6558fb7e2d, 561809b0c9c67b7d48712ab9e53cf5cc137b94d5a2d8bc65314a2db4c23df99d, 9d5d474791793300a273c5b6e522c7c3acd6fbb26c4da0421d4ef695c82f3fa5, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23, 14e4884288c1740d5a4b67ac83a890000c3b92f945139b2433bf9746acd14f9b, 01562cd36b61d517959fdbe5beaef9e1e9462be292c74a49b36a30057d09bc2c, 60f8b5a6c8621e07124fbec4b9253b913056d1279d6c42fdd99a8b6b14c33e9a, 048701ffc9b7ccfe4228bfaaa0b98a0518f02c6325c7f59365f863eccb65aa6d, c465c1ac750e80ffb4020ec085528ca520b4fca587710ae1a5937bc88e5ad22c, dbe4aaef628f4d392fd25946643424334af4ecb9eb2589884112b465f508ca33, 02eb774341d84b8c83b448186f3de8db139c52bea2376fec0ac88c7112186fd2, Ee1e27a01b884099a614b8eee78cdb1dd02ffecd6ed9f6a54b7b567b9eab979f

Attack Name	TYPE	VALUE
FunkLocker	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, e29d95bfb815be80075f0f8bef4fa690abcc461e31a7b3b73106bfcd5cd79033
WooperStealer	SHA256	8603b9fa8a6886861571fd8400d96a705eb6258821c6ebc679476d1b92dcd09e
AnonDoor	SHA256	abefd29c85d69f35f3cf8f5e6a2be76834416cc43d87d1f6643470b359ed4b1b
Cl0p	SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b
GOVERSHELL	IPv4:Port	80[.]85[.]154[.]48[:]443, 80[.]85[.]157[.]117[:]443, 82[.]118[.]16[.]173[:]443
	IPv4	104[.]194[.]152[.]137, 104[.]194[.]152[.]152, 185[.]144[.]28[.]68, 31[.]192[.]234[.]22, 45[.]141[.]139[.]222, 74[.]119[.]193[.]175, 80[.]85[.]156[.]234, 80[.]85[.]154[.]48, 80[.]85[.]157[.]117, 82[.]118[.]16[.]173
	Hostname	azure-app[.]store, twmoc[.]info, windows-app[.]store, cdn-apple[.]info, sliddeshare[.]online, doccloude[.]info

Attack Name	TYPE	VALUE
GOVERSHELL	URLs	hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ER_XG5FDkURHtsmna8vOQrIBRODKiQBKYJVKnI-kGKwX0A, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ESz4UV9JeOhOp8kiWd0Ie10ByH7eUdSRlBy2NCiNeo2LYw, hxxp[:]//1drv[.]ms/u/c/f9e3b332ce488781/Eap6_fxYFP5Eh1ZKDZaf8lMBjJNcfdba4MVcr4YfKj674w?e=fgNIj4, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ERpeLpJlb7FAkbfyuffpFJYBZ-8u2MmQH6LW5xH86B4M8w, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/rar, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/zip, hxxp[:]//animated-dango-0fa8c8[.]netlify[.]app/file/Taiwan%20Intro[.]zip, hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/rar hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/zip hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/index/file/[PDF]202507_Please_check_the_document[.]zip hxxp[:]//dainty-licorice-db2b1e[.]netlify[.]app/file/zip hxxp[:]//dulcet-mooncake-36558c[.]netlify[.]app/file/zip hxxp[:]//harmonious-malabi-a8ebfa[.]netlify[.]app/file/Taiwan%20Intro[.]rar hxxp[:]//hllowrodcanlhelipme[.]netlify[.]app/file/zip hxxp[:]//jazzy-biscotti-68241f[.]netlify[.]app/files/Intro-Doc[.]rar hxxp[:]//ln5[.]sync[.]com/4[.]0/dl/100016f90#3d5wrb4z-hfb4iz3m-qmjzsqnq-39rn3vjv hxxp[:]//loveusa[.]netlify[.]app/file/rar hxxp[:]//pulicwordfiledownlos[.]netlify[.]app/file/rar hxxp[:]//spontaneous-selkie-d3346f[.]netlify[.]app/file/zip hxxp[:]//statuesque-unicorn-09420f[.]netlify[.]app/r hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/rar hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/zip hxxp[:]//vocal-crostata-86ebbf[.]netlify[.]app/files/zip wss[:]//api[.]twmoc[.]info/ws wss[:]//onedrive[.]azure-app[.]store/ws wss[:]//outlook[.]windows-app[.]store/ws www[.]twmoc[.]info hxxp[:]//app-site-association[.]cdn-apple[.]info[:]443/updates[.]rss

Attack Name	TYPE	VALUE
GOVERSHELL	SHA256	2ffe1e4f4df34e1aca3b8a8e93eee34bfc4b7876cedd1a0b6ca5d63d89a26301 4c041c7c0d5216422d5d22164f83762be1e70f39fb8a791d758a816cdf3779a9 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040 88782d26f05d82acd084861d6a4b9397d5738e951c722ec5afed8d0f6b07f95e 998e314a8babf6db11145687be18dc3b8652a3dd4b36c115778b7ca5f240aae4 a5ee55a78d420dbba6dec0b87ffd7ad6252628fd4130ed4b1531ede960706d2d ad5718f6810714bc6527cc86d71d34d8c556fe48706d18b5d14f0261eb27d942 fbade9d8a040ed643b68e25e19cba9562d2bd3c51d38693fe4be72e01da39861 7d7d75e4d524e32fc471ef2d36fd6f7972c05674a9f2bac909a07dfd3e19dd18 0414217624404930137ec8f6a26aebd8a3605fe089dbfb9f5aaaa37a9e2bad2e 126c3d21a1dae94df2b7a7d0b2f0213eeeec3557c21717e02ffaed690c4b1dbd, 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040
Ghost RAT	SHA256	7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958
	File Path	C:\Windows\Cursors\x.exe
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

Attack Name	TYPE	VALUE
Lumma	SHA256	e17bf83e09457d8cecd1f3e903fa4c9770e17e823731650a453bc479591ac511, 0f6481dabf7871823f259eb95f3b85c37d1de8a7d1884ac77a97d887cf96f75d, 8d7f3d4905f17b6e488d485169fe6ace11a2f2771f432ebf25425179312fbb50, 6d41d871f00a12249ee90afb22a1da514b0ee0b16a0943a60e481d44f9b57be7, c7196ff93362110d20441bb1548884eff42deda49e759dc3e8a943a310f2b170
Rhadamanthys	SHA256	9007661e48e9d4b325029b08a941aa99d315e33be6496380dacf238f0b95ccf3, 805f2fec37ed73461b715ba2ce6671213674ada9076ef24de833ec0d33a18c01,
Phoenix Backdoor v4	SHA256	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839, 1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56, 3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3, 76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75, 3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
ScoringMathTea	SHA256	c39ecc7d9f1e225a37304345731fffe72cdb95b21aeb06aa6022f6d338777012
	SHA1	71D0DDB7C6CAC4BA2BDE679941FA92A31FBEC1FF, E670C4275EC24D403E0D4DE7135CBCF1D54FF09C, AC16B1BAEDE349E4824335E0993533BF5FC116B3, 086816466D9D9C12FCADA1C872B8C0FF0A5FC611
	IPv4	23[.]111[.]133[.]162, 104[.]21[.]80[.]1, 70[.]32[.]24[.]131, 185[.]148[.]129[.]24, 66[.]29[.]144[.]75, 108[.]181[.]92[.]71, 104[.]247[.]162[.]67, 193[.]39[.]187[.]165, 172[.]67[.]193[.]139, 77[.]55[.]252[.]111, 45[.]148[.]29[.]122, 75[.]102[.]23[.]3, 152[.]42[.]239[.]211, 95[.]217[.]119[.]214

Attack Name	TYPE	VALUE
ScoringMathTea	Domains	coralsunmarine[.]com, kazitradebd[.]com, oldlinewoodwork[.]com, www[.]mnmathleague[.]org, pierregems[.]com, www[.]scgestor.com[.]br, galaterrace[.]com, ecudecode[.]mx, www[.]anvil.org[.]ph,partnerls[.]pl, trainingpharmacist[.]co[.]uk, mediostresbarbas[.]com[.]ar, www[.]bandarpowder[.]com, spaincaramoon[.]com
	URLs	hxxps[:]//coralsunmarine[.]com/wp-content/themes/flatsome/inc/functions/function-hand[.]php, hxxps[:]//kazitradebd[.]com/wp-content/themes/hello-elementor/includes/customizer/customizer-hand[.]php, hxxps[:]//oldlinewoodwork[.]com/wp-content/themes/zubin/inc/index[.]php, hxxps[:]//www[.]mnmathleague[.]org/ckeditor/adapters/index[.]php, hxxps[:]//pierregems[.]com/wp-content/themes/woodmart/inc/configs/js-hand[.]php, hxxps[:]//www[.]scgestor[.]com[.]br/wp-content/themes/vantage/inc/template-headers[.]php, hxxps[:]//galaterrace[.]com/wp-content/themes/hello-elementor/includes/functions[.]php, hxxps[:]//ecudecode[.]mx/redsocial/wp-content/themes/buddyx/inc/Customizer/usercomp[.]php, hxxps[:]//www[.]anvil[.]org[.]ph/list/images/index[.]php, hxxps[:]//partnerls[.]pl/wp-content/themes/public/index[.]php, hxxps[:]//trainingpharmacist[.]co[.]uk/bootstrap/bootstrap[.]php, hxxps[:]//mediostresbarbas[.]com[.]ar/php_scrip/banahosting/index[.]php, hxxps[:]//www[.]bandarpowder[.]com/public/assets/buttons/bootstrap[.]php, hxxps[:]//spaincaramoon[.]com/realestate/wp-content/plugins/gravityforms/forward[.]php
BinMergeLoader	SHA1	26AA2643B07C48CB6943150ADE541580279E8E0E

Attack Name	TYPE	VALUE
Medusa	SHA256	6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da
ValleyRAT	SHA256	14bf52de60e60a526141ffe61ef5afc2a3bc7d60d4086e644ec80e67513d2684, b14996c4a93ff7d09795b113fb916c9588eb7efb4d64a1dbe190cfe937912209
DeskRAT	SHA256	567dfbe825e155691329d74d015db339e1e6db73b704b3246b3f015ffd9f0b33
Qilin Ransomware	SHA1	c150e4ab20d59affc62b916c2c90686f43040a9f
	SHA256	cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f
Hijackloader	SHA256	14becb3a9663128543e1868d09611bd30a2b64c655dfb407a727a7f2d0fb8b7e, 57c49cff3e71bc75641c78a5a72d8509007a18032510f607c042053c9d280511, 7c3d9ad3f1bd890e3552dc67093e161395d4e1fab79ec745220af1e19a279722, ce42377d3d26853fd1718f69341c0631208138490decc8e71a5622df5e9e1f59, a0e4979b4e4a706286438d48f0e21b0d92cc7bd40c1c3ea5b9872089aaec0124, 6d93a486e077858b75eb814e9a7bda181189d5833adce7cec75775cfda03f514, bdca9849d7263d508b7ed4dbbf86bd628932b117b45933cb28a7e78171d05cdd, 1ae61edf35127264d329b7c0e2bddb7077e34cc5f9417de86ab6d2d65bad4b4f, 2ec31a8a36d73fa8354a7ac0c39506dbe12638a0dc1b900f57620b8d53ae987f, 776bbaa44c7788e0ccd5945d583de9473b6246c44906692cb0a52e6329cb213a,

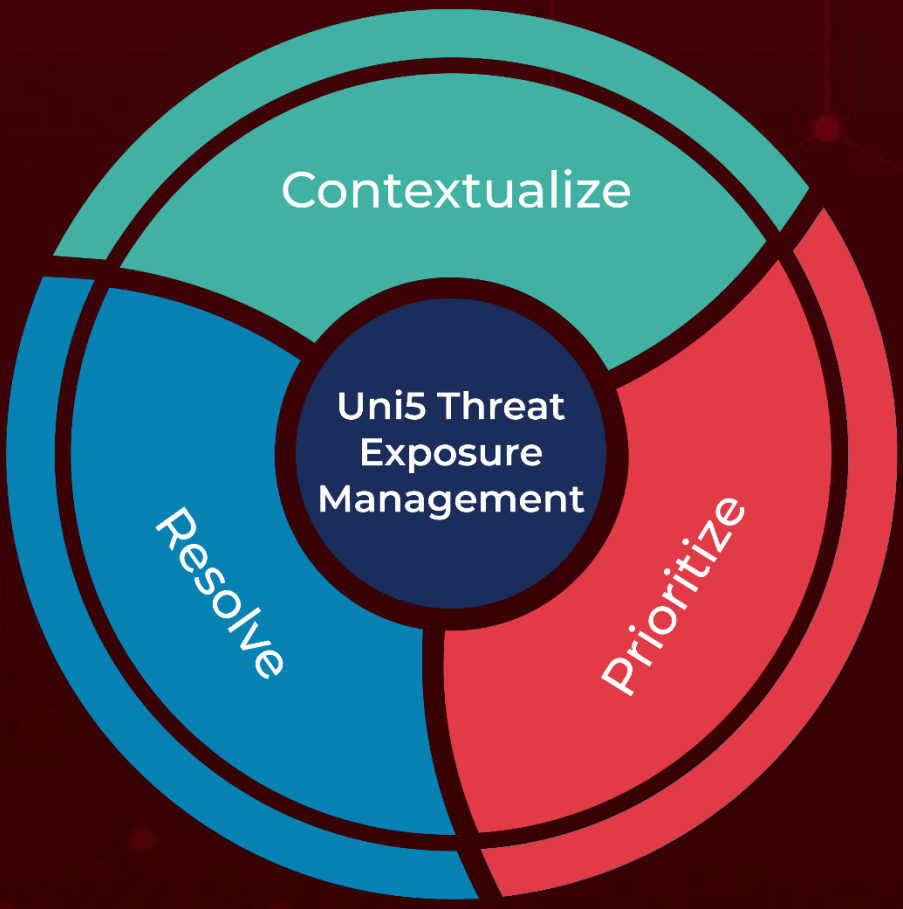
Attack Name	TYPE	VALUE
Hijackloader	SHA256	9e9997b54da0c633ffcf0a4fb94e67b482cf7a89522d1b254778d0c6c22c70ee, b2f733b67f1ef06d9e5ce76d3cc848f6e7e3ec2d0c363c76d5175c6cf85f979b, c93e70d20ba2948a6a8a013df68e5c4d14d59e5f549417d1a76833bd1c8efd22, d550a2a327394148c0c3d05df2fe0156783fc313b4038e454f9aa2cb2f0f2090, e668ca17fcdfa818aac35f12064d10a0288d7d9c6b688966b695125b760567d6, fe6d0ee45a70359008b2916e5116c411a955978b5694cc457683ab7b26590e47, 977f2f18ff13c93406c5702f83c04a9412760e02028aefc7c1cb7d6f2797a9b5, 768ca38878c5bb15650343ce49292315a9834eaf62fad14422d52510c3787228, 47245b7d2d8cb6b92308deb80399e0273193d5bca39da85a6b2a87a109d18d85, 4484b0ac51536890301a0e6573b962e069e31abc4c0c6f0f6fc1bf66bf588a93, 0113d9f3d93069a29458b3b4c33610aae03961014df60a9e859f3104086d886a, 22d474e729d600dcd84ce139f6208ce3e3390693afa7b52b0615174fca6d0fe2, 2cbfc482e27a2240a48d2fb6f6f740ff0f08598f83ae643a507c6f12a865dc28, 96ee786c5b6167c0f0f770efbace25e97d61e127ef7f58a879b6cf4b57e202c3, a70978d0cb43ca85b2f91ca022f678d38ec04b8ddef895355c934777e1c7c673
PureHVNC	SHA256	33d0c63777882c9ec514be062612a56fdb1f291fcb6676c49480d3cd4501c508, afecefa6d9bd1e6d1c92144209eda320e1fe0f196ffa8e8bc114e7d3a25503f6, 85641c8fb94e8e4c5202152dcbb2bb26646529290d984988ecb72e18d63c9bc5, 1bf3a1cf9bc7eded0b8994d44cf2b801bf12bc72dc23fb337ddd3a64ac235782
LeetAgent	MD5	33bb0678af6011481845d7ce9643cedc
	SHA1	8390e2ebdd0db5d1a950b2c9984a5f429805d48c
	SHA256	388a8af43039f5f16a0673a6e342fa6ae2402e63ba7569d20d9ba4894dc0ba59

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 4, 2025 • 9:00 AM

More at www.hivepro.com