Date of Publication
December 16, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

8 to 14 DECEMBER 2025

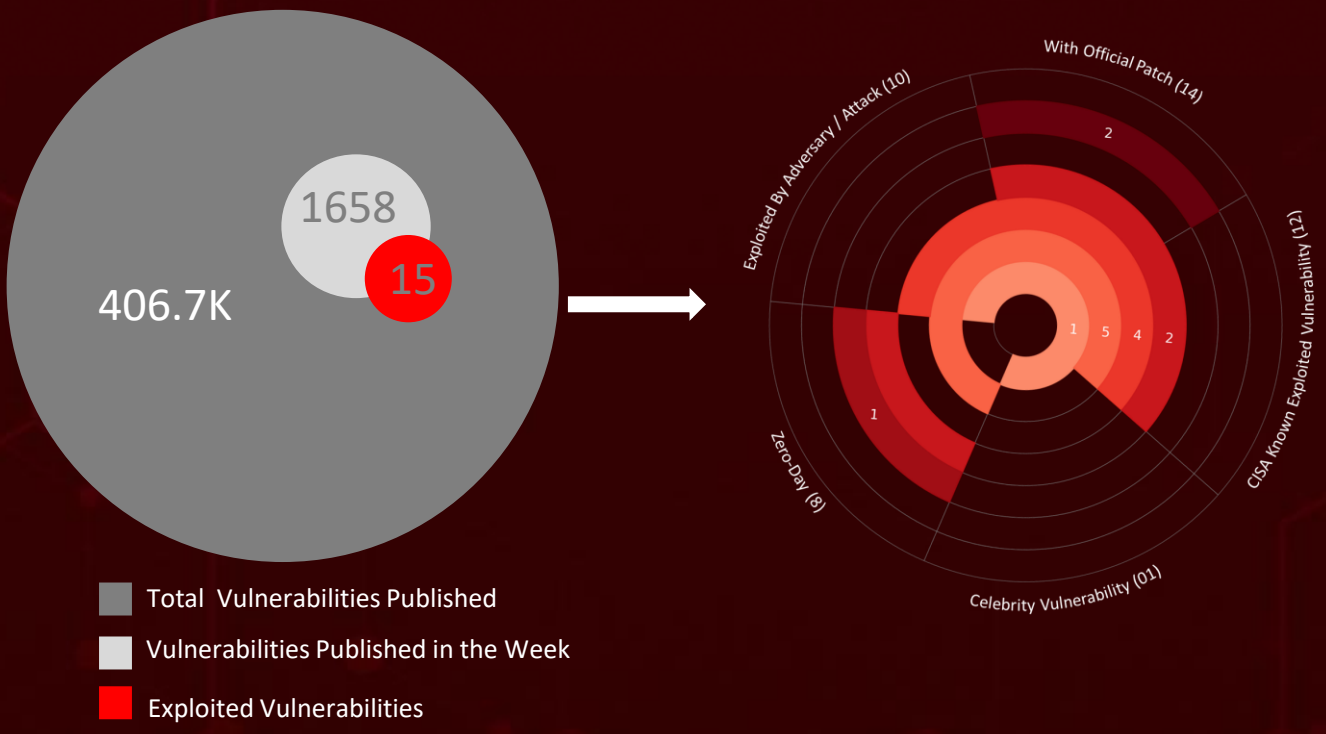
Table Of Contents

Summary

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

Much of this surge is being fueled by the rapid weaponization of newly disclosed and zero-day vulnerabilities. **CVE-2025-55182**, known as **React2Shell**, is a critical unauthenticated remote code execution flaw in React Server Components caused by unsafe deserialization in the Flight protocol. The flaw was exploited within days of disclosure by multiple threat actors observed leveraging the vulnerability to deploy cryptominers, web shells, and persistent backdoors during mass scanning campaigns. At the same time, multiple zero-days remain under active exploitation: **CVE-2025-62221** enables privilege escalation on Windows systems via the Cloud Files Mini Filter Driver; **CVE-2025-14174** targets Google Chromium through an out-of-bounds memory access flaw in the ANGLE graphics engine; and **CVE-2025-8110** exposes Gogs deployments to authenticated remote code execution due to improper symbolic-link handling. With fixes incomplete or still pending, hundreds of environments remain exposed to live attacks.

Beyond vulnerability exploitation, state-aligned threat activity continues to intensify. China-linked operators deploy **BRICKSTORM**, a stealthy Go-based ELF backdoor designed for long-term persistence and deep system control. The malware has also been used by the **WARP PANDA** threat group during intrusions against U.S. organizations in 2025. Together, these developments underscore the need for timely patching, continuous monitoring, and sustained defensive vigilance as attackers refine and diversify their intrusion strategies.



High Level Statistics

10
Attacks Executed

15
Vulnerabilities Exploited

8
Adversaries in Action

- XMRig
- Sliver
- PeerBlight
- EtherRAT
- UDPGangster
- MetaRAT
- Talisman PlugX
- BRICKSTORM
- Pteranodon
- GamaWiper

- CVE-2025-55182
- CVE-2024-21893
- CVE-2024-21887
- CVE-2025-62221
- CVE-2025-54100
- CVE-2025-64671
- CVE-2025-14174
- CVE-2025-8110
- CVE-2023-46805
- CVE-2024-38812
- CVE-2023-46747
- CVE-2023-34048
- CVE-2021-22005
- CVE-2025-8088
- CVE-2025-6218

- ShadyPanda
- Earth Lamia
- Jackpot Panda
- UNC5174
- MuddyWater
- WARP PANDA
- Gamaredon
- APT-C-08

Insights

Google Chrome emergency update fixes zero-day **CVE-2025-14174** and two other flaws actively exploited in the wild.

CVE-2025-55182 (React2Shell): From disclosure to domination- RCE swiftly hijacked to drop miners and backdoors.

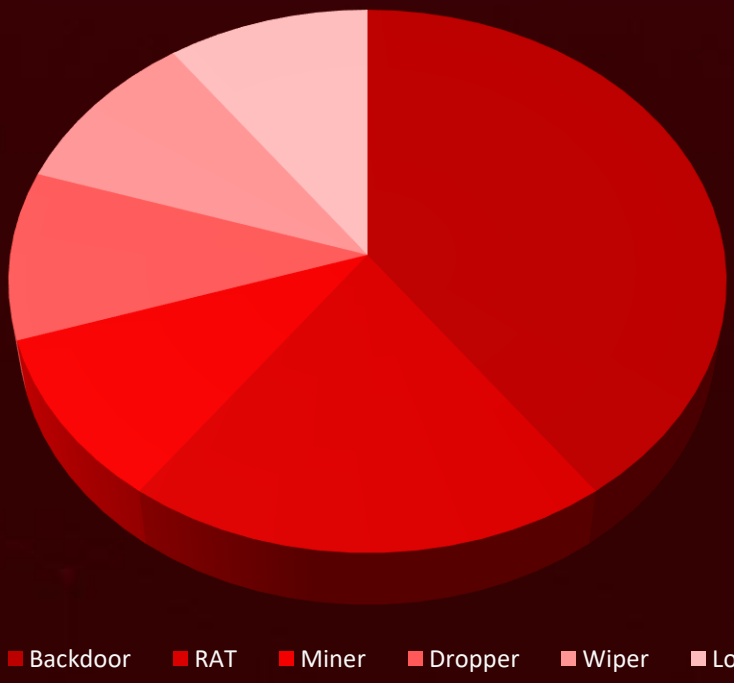
Ivanti zero-days, **CVE-2024-21893** and **CVE-2024-21887**, opened Japan's shipping networks to China-linked PlugX intrusions.

Microsoft Dec 2025 Patch: 57 fixes, spotlight on actively exploited zero-day CVE-2025-62221.

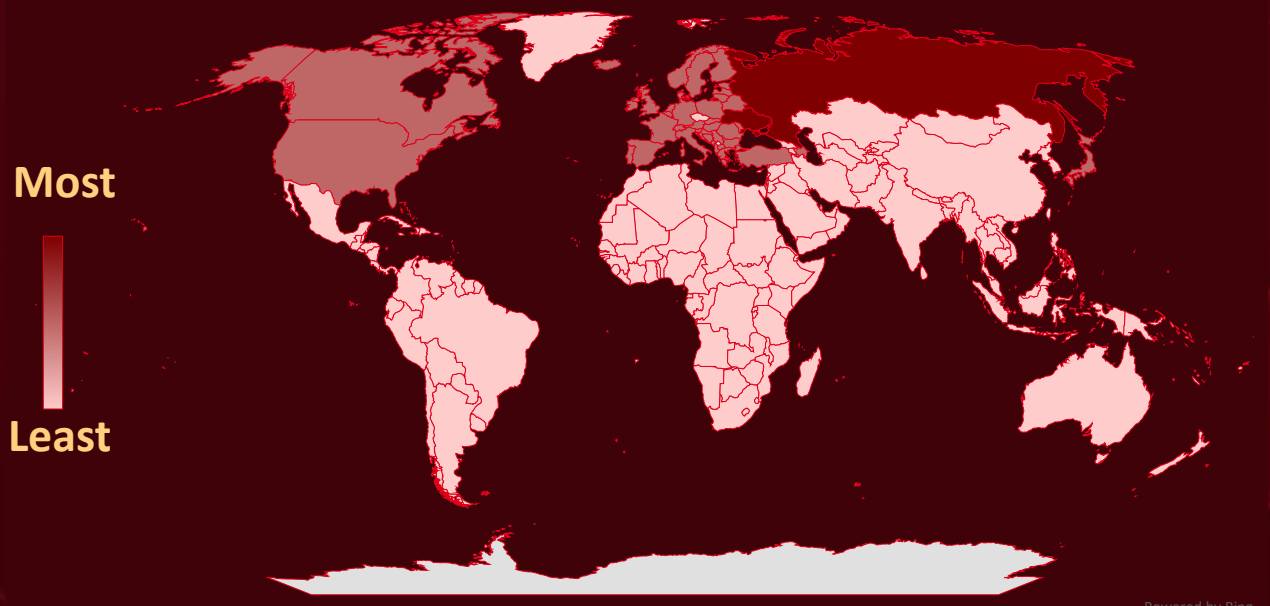
WARP PANDA deploys BRICKSTORM, a stealthy Go-based ELF backdoor driving China-linked intrusions into U.S. targets.

CVE-2025-8110: New Gogs zero-day enables authenticated RCE, sidesteps prior patch, and compromises over 700 instances via Supershell C2.

Threat Distribution

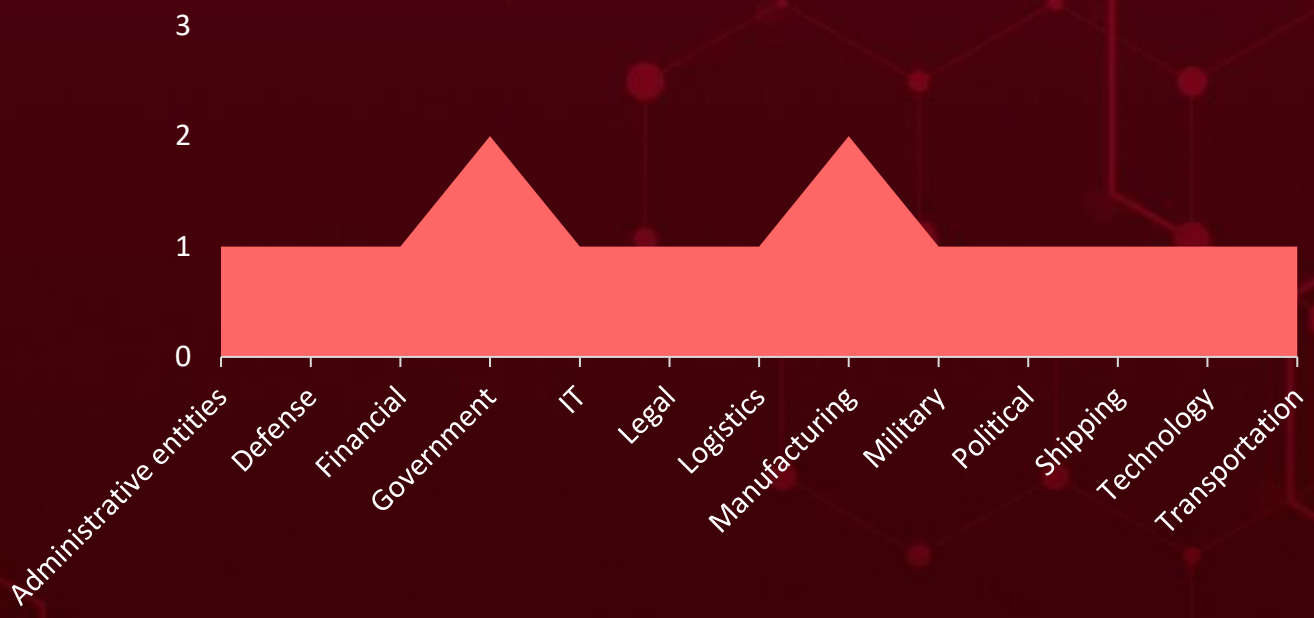


Targeted Countries



Countries	Countries	Countries	Countries
Russia	France	Egypt	Ghana
Ukraine	Montenegro	Paraguay	Niger
Norway	Germany	El Salvador	Argentina
Lithuania	North Macedonia	Costa Rica	Chad
Slovenia	Greece	Equatorial Guinea	Grenada
Austria	Poland	Suriname	Panama
Monaco	Holy See	Eritrea	Guatemala
Azerbaijan	Romania	Bahamas	Philippines
Albania	Hungary	Bahrain	Guinea
Belarus	San Marino	New Zealand	Colombia
Andorra	Iceland	Eswatini	Guinea-Bissau
Belgium	Slovakia	Pakistan	Saint Lucia
Malta	Ireland	Ethiopia	Guyana
Bosnia and Herzegovina	Spain	China	Saudi Arabia
Netherlands	Israel	Fiji	Haiti
Bulgaria	Switzerland	Congo	Sierra Leone
Portugal	Turkey	Bangladesh	Belize
Canada	United Kingdom	Côte d'Ivoire	Solomon Islands
Serbia	Italy	Barbados	Honduras
Croatia	United States	Sri Lanka	South Sudan
Sweden	Japan	Gabon	Benin
Denmark	Latvia	Tajikistan	State of Palestine
Liechtenstein	Togo	Gambia	Bhutan
Estonia	Rwanda	Georgia	Czech Republic
Luxembourg	North Korea	Uruguay	India
Finland	South Africa	Antigua and Barbuda	Thailand
Moldova	Ecuador		Indonesia
	Namibia	Nepal	Trinidad and Tobago

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1071.001** Web Protocols
T1027 Obfuscated Files or Information	**T1059.007** JavaScript	**T1071** Application Layer Protocol	**T1041** Exfiltration Over C2 Channel	**T1505** Server Software Component
T1068 Exploitation for Privilege Escalation	**T1082** System Information Discovery	**T1036** Masquerading	**T1095** Non-Application Layer Protocol	**T1005** Data from Local System
T1189 Drive-by Compromise	**T1566** Phishing	**T1543** Create or Modify System Process	**T1204.002** Malicious File	**T1033** System Owner/User Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
XMRig	XMRig is a legitimate open-source cryptocurrency miner that is often embedded in malware. Threat actors use it to hijack system CPU/GPU resources for unauthorized mining. It typically runs silently to avoid detection and maximize profit.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	**AFFECTED PLATFORM**
TYPE		Resource Drain, Potential for Data Theft	Meta React Server Components
Miner			**PATCH LINK**
ASSOCIATED ACTOR			https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r
-			
IOC TYPE	**VALUE**		
SHA1	59de54c4cb7ccc1602c90d8afe2efc071751d9ae		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Sliver	Sliver is an advanced malware framework used in cyberattacks, leveraging DLL sideloading and proxying techniques for persistence and stealth. It targets organizations, enabling data exfiltration and espionage while evading detection.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data exfiltration and Espionage	Meta React Server Components
Dropper			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r
IOC TYPE	**VALUE**		
SHA256	2cd41569e8698403340412936b653200005c59f2ff3d39d203f433adb2687e7f, cb5524b6605af240a7385f8f875c6af0b5009d5bcba4a3cc7c3e399057c7c644		

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
PeerBlight	PeerBlight is a Linux-based backdoor that leverages the BitTorrent DHT network as a fallback command-and-control (C2) channel, enhancing its resilience against conventional domain takedowns. Upon execution, it manipulates in-memory data to conceal its original file path and persistently masquerades its identity across system monitoring tools.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCT
TYPE		Unauthorized remote access	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r
IOC TYPE	VALUE		
SHA256	a605a70d031577c83c093803d11ec7c1e29d2ad530f8e95d9a729c3818c7050d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EtherRAT	EtherRAT uses Ethereum smart contracts to resolve its command-and-control (C2) infrastructure, reducing the effectiveness of traditional domain or IP blocking. It deploys multiple Linux persistence mechanisms and downloads a legitimate Node.js runtime to evade detection.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCT
TYPE			Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r
IOC TYPE	VALUE		
IPv4:PORT	193[.]24[.]123[.]68[:]3001		

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
UDPGangster	UDPGangster is a stealthy UDP-based backdoor used in MuddyWater's latest espionage campaigns. Once activated, it quietly deploys itself, evades virtual analysis, and collects system details while hiding behind decoy images and layered obfuscation. The malware establishes persistence, communicates with its C2 server over UDP, and supports commands for file theft, remote execution, and payload delivery.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Stealthy long-term persistence, Espionage	Microsoft Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

IOC TYPE	VALUE
SHA256	028dcda69ba17f9c0d492fe2e0aa0b1bbb5154266c52840bd49f51ce11c934d4, 863f94873b7535f49a03784abf74a8a29b792b97dadc5361a379c7ae29d0ba4c, a35e0fccee6d9cf10a806c5134a85a1dadc0301312bbd9ae92af2fe1fbb77d24

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MetaRAT	MetaRAT is a modernized iteration featuring enhanced obfuscation, modularity, and encrypted C2 communications. It relies on DLL side-loading, custom shellcode, layered decryption, and reflective loading to unpack itself directly into memory. The malware supports multiple communication protocols.	Exploiting Vulnerabilities	CVE-2024-21893 CVE-2024-21887
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data theft and command execution	Ivanti Connect Secure
RAT			**PATCH LINK**
ASSOCIATED ACTOR			https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US, https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
-			

IOC TYPE	VALUE
SHA256	aba6f7611291433983ba9c65654b04745a050530329d3ad329cc859c1ce12c44

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Talisman PlugX</td><td rowspan="6">Talisman PlugX is a side-loading variant capable of executing multiple plugins for tasks such as keylogging, file manipulation, and command execution. It follows an execution flow, loading an encrypted payload, decrypting and decompressing embedded components, and injecting itself into legitimate processes to blend into normal system activity.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-21893
CVE-2024-21887</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="4">Credential theft, Long-term persistence</td><td>Ivanti Connect Secure</td></tr>
<tr><td>RAT</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US, https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">78c3eb67fdc59fd09cba6388d6e31c428ed3c227f04b9cd739e8c36a8f1a182e</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
BRICKSTORM	BRICKSTORM is a Go-based ELF backdoor built for stealth, durability, and deep system control. It begins by performing integrity and environment checks, then anchors itself with a self-monitoring mechanism that automatically reinstalls or restarts if interrupted. The malware configures environment variables to match the compromised host, enabling stable operation.	Exploiting vulnerabilities	CVE-2023-46805 CVE-2024-21887
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Stable long-term foothold	Ivanti, VMware, F5 BIG-IP, VMware vCenter
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
WARP PANDA			-
IOC TYPE	**VALUE**		
SHA256	aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38, 013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf, 57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Pteranodon	Pteranodon acts as the core loader in a multi-stage infection chain, enabling long-term espionage, internal movement, and data theft through a resilient C2 setup.	Exploiting vulnerabilities	CVE-2025-8088
		IMPACT	**AFFECTED PRODUCT**
TYPE		Long-term espionage, Data exfiltration	RARLAB WinRAR
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
Gamaredon			https://www.win-rar.com/download.html?&L=0
IOC TYPE	**VALUE**		
SHA256	18b2956ceea0e45e2183dc1590fb306f9431943ed612e110af508d819d2ffd67, f08ea988890f33b18ae15d6d3466be0d60e974dece876450f16a0c82bf8469a7		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">GamaWiper</td><td rowspan="5">Gamawiper is a newly discovered destructive malware. Once executed, it systematically overwrites files and corrupts the Master Boot Record (MBR), rendering the infected system unbootable and data unrecoverable. Gamawiper is designed solely to permanently destroy data.</td><td>Exploiting vulnerabilities</td><td>CVE-2025-8088</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="3">Data Destruction</td><td rowspan="2">RARLAB WinRAR</td></tr>
<tr><td>TYPE</td></tr>
<tr><td>Wiper</td><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Gamaredon</td><td colspan="2">https://www.win-rar.com/download.html?&L=0</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">d4ce4776bdad9b741a1e8345b41737245b80f4cf8d361ebb1ae5415c7a4fe1eb,
9a39423ec90dc06a3058279cd744c08d83252d1c7096633b9853e435cc205755</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55182	React2Shell	react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack versions: 19.0.0, 19.1.0, 19.1.1, 19.2.0 Next.js versions: 14.3.0-canary.77+, 15.x, 16.x (before 16.0.7) React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc	Earth Lamia, Jackpot Panda and UNC5174
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:* cpe:2.3:a:remix:react_router:*:*:*:*	XMRig, Sliver, PeerBlight and EtherRAT
Meta React Server Components Remote Code Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-502	T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter	https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-21893	✗	Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	MetaRAT, Talisman PlugX
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-918	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-21887	✗	Ivanti Connect Secure and Policy Secure	WARP PANDA
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	MetaRAT, Talisman PlugX, BRICKSTORM Backdoor
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-77	T1059: Command and Scripting Interpreter; T1133: External Remote Service	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-62221	✗	Windows Server 2022, 2025; Windows 11 Version 25H2; Windows 10 Version 1809	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-62221

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-54100	✗	Windows Server 2025, 2012, 2008, 2016; Windows 10 Version 1607	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
PowerShell Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059.001: PowerShell, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-54100

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-64671	✗	GitHub Copilot Plugin for JetBrains IDEs	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:github_copilot:*:*:*:*:*:jetbrains:*:*	-
GitHub Copilot for Jetbrains Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-64671

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-14174	✗	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium Out of Bounds Memory Access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8110	✗	Gogs (Prior to 0.13.4, all versions through 0.13.3)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	-
Gogs Symlink Bypass Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505: Server Software Component	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-46805	✗	Ivanti Connect Secure and Policy Secure	WARP PANDA
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	BRICKSTORM
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-38812	✗	VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x	WARP PANDA
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	-
VMware vCenter Server Heap-Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow, T1021.003: Distributed Component Object Model	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-46747	✗	F5 BIG-IP Configuration Utility	WARP PANDA
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	-
F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306 CWE-288	T1190: Exploit Public-Facing Application	https://my.f5.com/manage/s/article/K000137353

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-34048	✗	VMware vCenter Server	WARP PANDA
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	-
VMware vCenter Server Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2021-22005	✗	VMware vCenter Server: 6.7 - 7.0.0	WARP PANDA
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	-
VMware vCenter Server File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1505.003: Web Shell, T1505: Server Software Component, T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23611

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8088	✗	WinRAR versions before 7.13	Gamaredon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Pteranodon, GamaWiper
RARLAB WinRAR Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-6218	✗	WinRAR Version Prior to 7.12	APT-C-08
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*	-
RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShadyPanda	China	All	Worldwide
	MOTIVE		
	Information theft, Financial gain, and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	-	Chrome, Edge
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1189: Drive-by Compromise; T1176: Software Extensions; T1176.001: Browser Extensions; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1027: Obfuscated Files or Information; T1480: Execution Guardrails; T1036: Masquerading; T1539: Steal Web Session Cookie; T1185: Browser Session Hijacking; T1005: Data from Local System; T1056: Input Capture; T1056.004: Credential API Hooking; T1041: Exfiltration Over C2 Channel; T1217: Browser Information Discovery; T1567: Exfiltration Over Web Service; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1557: Adversary-in-the-Middle			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Earth Lamia	China	All	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	-	Meta React Server Components
TTPs			
TA0010: Exfiltration; TA0042 : Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057 : Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Jackpot Panda	China	All	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	-	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042 : Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057 : Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC5174 (aka Uteus, CL-STA-1015)	China	All	Worldwide
	MOTIVE		
	Financial gain, Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	-	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042 : Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057 : Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, G0069)	Iran	All	Turkey, Israel, Azerbaijan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	UDPGangster	Microsoft Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1497: Virtualization/Sandbox Evasion; T1027: Obfuscated Files or Information; T1036: Masquerading; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1083: File and Directory Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 WARP PANDA	China	Government, IT, Legal, Technology, Manufacturing	United States
	MOTIVE		
	Espionage, Information Theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2024-21887 CVE-2023-46805 CVE-2024-38812 CVE-2023-46747 CVE-2023-34048 CVE-2021-22005	BRICKSTORM Backdoor	Ivanti Connect Secure and Policy, VMware, F5 BIG-IP

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1037: Boot or Logon Initialization Scripts; T1574: Hijack Execution Flow; T1574.007: Path Interception by PATH Environment Variable; T1505: Server Software Component; T1505.003: Web Shell; T1548: Abuse Elevation Control Mechanism; T1548.003: Sudo and Sudo Caching; T1036: Masquerading; T1078: Valid Accounts; T1083: File and Directory Discovery; T1003: OS Credential Dumping; T1003.003: NTDS; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1090: Proxy; T1090.001: Internal Proxy; T1041: Exfiltration Over C2 Channel; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1583.007: Serverless; T1584: Compromise Infrastructure; T1584.008: Network Devices; T1588: Obtain Capabilities; T1588.001: Malware; T1608: Stage Capabilities; T1608.003: Install Digital Certificate; T1190: Exploit Public-Facing Application; T1078.004: Cloud Accounts; T1078.001: Default Accounts; T1098.001: Additional Cloud Credentials; T1036.004: Masquerade Task or Service; T1070.004: File Deletion; T1070.006: Timestomp; T1564.006: Run Virtual Instance; T1021.004: SSH; T1550.001: Application Access Token; T1114.002: Remote Email Collection; T1213: Data from Information Repositories; T1213.002: Sharepoint; T1530: Data from Cloud Storage; T1560.001: Archive via Utility; T1071.004: DNS; T1090.003: Multi-hop Proxy; T1095: Non-Application Layer Protocol; T1572: Protocol Tunneling; T1573.002: Asymmetric Cryptography; T1098: Account Manipulation; T1573: Encrypted Channel; T1560: Archive Collected Data; T1114: Email Collection; T1550: Use Alternate Authentication Material; T1021: Remote Services; T1564: Hide Artifacts; T1070: Indicator Removal

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Gamaredon (aka Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard, UNC530, G0047)	Russia	Financial, Manufacturing, Defense, Logistics, Government, Political, Military, Administrative entities	Europe, Canada, Russia, Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-8088	Pteranodon, GamaWiper	RARLAB WinRAR

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; 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; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036: Masquerading; T1036.001: Invalid Code Signature; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Browser Session Hijacking; T1005: Data from Local System; T1114: Email Collection; T1114.001: Local Email Collection; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1658: Exploitation for Client Execution; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol; T1574: Hijack Execution Flow; T1574.001: DLL; T1137: Office Application Startup; T1137.001: Office Template Macros

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 APT-C-08 (aka Bitter, T-APT-17, TA397, G1002, Manlinghua)	-	Financial, Manufacturing, Defense, Logistics, Government, Political, Military, Administrative entities	Europe, Canada, Russia, Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-6218	-	RARLAB WinRAR

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; 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; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036: Masquerading; T1036.001: Invalid Code Signature; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Browser Session Hijacking; T1005: Data from Local System; T1114: Email Collection; T1114.001: Local Email Collection; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1658: Exploitation for Client Execution; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol; T1574: Hijack Execution Flow; T1574.001: DLL; T1137: Office Application Startup; T1137.001: Office Template Macros

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **fifteen exploitable vulnerabilities** and block the indicators related to the threat actors **ShadyPanda, Earth Lamia, Jackpot Panda, UNC5174, MuddyWater, WARP PANDA, Gamaredon, APT-C-08,** and malware **XMRig, Sliver, PeerBlight, EtherRAT, UDPGangster, MetaRAT, Talisman PlugX, BRICKSTORM, Pteranodon,** and **GamaWiper.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **fifteen exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **ShadyPanda, Earth Lamia, Jackpot Panda, UNC5174, MuddyWater, WARP PANDA, Gamaredon, APT-C-08,** and malware **Sliver, PeerBlight, UDPGangster, MetaRAT, Talisman PlugX,** and **BRICKSTORM** in Breach and Attack Simulation(BAS).

Threat Advisories

ShadyPanda's Seven-Year Operation Built a Browser Extension Spy Empire

React2Shell Flaw in React Server Components Under Active Attack

Echoes Over UDP: MuddyWater’s Covert Backdoor Strikes

China-Linked Operators Breach Japanese Shipping Networks

Microsoft December 2025 Patch Tuesday Roundup

Google Chrome Zero-Day Exploited in ANGLE Graphics Engine

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

BRICKSTORM Breaks In: China's Quiet Grip on US Virtual Stack

Zero-Day in WinRAR Actively Weaponized by Multiple Threat Groups

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
XMRig	URL	hxxps[:]//raw[.]githubusercontent[.]com/C3Pool/xmrig_setup/master/setup_c3pool_miner[.]sh, hxxps[:]//raw[.]githubusercontent[.]com:443/c3pool/xmrig_setup/master/setup_c3pool_miner[.]bat
	SHA1	59de54c4cb7ccc1602c90d8afe2efc071751d9ae
Sliver	File Path	/usr/bin/sshd-agent, ~/.config/.system-monitor/.sys-mon, /tmp/.system-update/
	Domain	keep[.]camdvr[.]org, t[.]cnzzs[.]co
	IPv4	154[.]26[.]190[.]6
	URL	hxxp[:]//keep.camdvr[.]org[:]8000/BREAKABLE_PARABLE5, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE5, hxxp[:]//keep[.]camdvr[.]org[:]8000/d5[.]sh, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE10
	SHA1	0972859984decfaf9487f9a2c2c7f5d2b03560a0, 470ce679589e1c3518c3ed2b818516f27ccad089, 0972859984decfaf9487f9a2c2c7f5d2b03560a0, 2937c58115c131ae84a1b2a7226c666f6a27ef88
	SHA256	2cd41569e8698403340412936b653200005c59f2ff3d39d203f433adb2687e7f, cb5524b6605af240a7385f8f875c6af0b5009d5bcba4a3cc7c3e399057c7c644

Attack Name	TYPE	VALUE
PeerBlight	SHA256	a605a70d031577c83c093803d11ec7c1e29d2ad530f8e95d9a729c3818c7050d
	URL	hxxp://45.32.158[.]54/5e51aff54626ef7f/x86_64,
	IPv4	185.247.224[.]41, 49.51.230[.]175
	File Path	/lib/systemd/system/systemd-agent.service, /bin/systemd-daemon, /bin/systemd-daemon
EtherRAT	IPv4:PORT	193[.]24[.]123[.]68[:]3001
	URL	hxxp[:]//193[.]24[.]123[.]68[:]3001/gfdsgsdfhfsd_ghsfdgsfdgsdfg[.]sh
UDPGangster	SHA256	028dcda69ba17f9c0d492fe2e0aa0b1bbb5154266c52840bd49f51ce11c934d4, 863f94873b7535f49a03784abf74a8a29b792b97dadc5361a379c7ae29d0ba4c, a35e0fccee6d9cf10a806c5134a85a1dadc0301312bbd9ae92af2fe1fbb77d24, a8aed7a290f38952be0e7360fd5f36276c279e430b51303780c5242d66cea932, b0dc4e34701f2032059c9eea77313628e7f79474a90dc40b4ed3ab39e0d06a37, 6d9ee1f6b8c344224116f47f81d4d2af58569925d22d731fb38b555771aa85f8, b95d35ef7dd6e98bcb30b896a5cee385c2e42cc94a1c9b124ef80fa65f20d3ba, 7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53
MetaRAT	SHA256	aba6f7611291433983ba9c65654b04745a050530329d3ad329cc859c1ce12c44, d3ec33ae5c8ce2ac5eb0c96c6d6dc1d5ca610bacaa9de85d1e4bfe1d60923970, fd87149d6b8fdcad5d84ba4a3ca52e1cef8f0c54cafca6dbbb5d156f313d79dd, fd6b1ca0f26e54fa9c97ea15c834e58ffb71798df38071ad00b14f19d6a4126c, c91595edd1c9a0a2c1168e3bfa532e4a7dbb6b1380afd80ba445b728622798a4, c90460e820a8c5874d5412032b7db719cb8ea34ae8e48e4ab934a4096a09612b, a92ed5f831c99bb84208ef7d7c733e0183a79de40f9d3b3be54744951f0a1391, 0ec83d1deb6065cac8ba8f849cdf5672da7313ec2e860a7d71bb7e397e661394, 7b028a9bd2bc0c306ab6561cf702406f5925fc073f9d0d2d9408ceccd6907743

Attack Name	TYPE	VALUE
MetaRAT	Domains	doodle01[.]space, piao.mil.onmypc[.]net, newsinfom[.]org, mailserver[.]kozow[.]com
	IPv4	117[.]254[.]105[.]200, 45[.]114[.]192[.]137, 103[.]9[.]14[.]218, 23[.]254[.]225[.]184, 103[.]136[.]45[.]108, 103[.]172[.]10[.]165, 117[.]239[.]199[.]202
Talisman PlugX	IPv4	220[.]130[.]204[.]242
	Domains	turky[.]info, nord.ocry[.]com
	SHA256	78c3eb67fdc59fd09cba6388d6e31c428ed3c227f04b9cd739e8c36a8f1a182e, 367ad2eaa851ae17a4b75d92ec712d889fa85c0f2a51b9d5c5e08ae84fa7514d
BRICKSTORM	SHA256	aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38, 013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf, 57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d, b3b6a992540da96375e4781afd3052118ad97cfe60ccf004d732f76678f6820a, 22c15a32b69116a46eb5d0f2b228cc37cd1b5915a91ec8f38df79d3eed1da26b, f7cda90174b806a34381d5043e89b23ba826abcc89f7abd520060a64475ed506, 39b3d8a8aedffc1b40820f205f6a4dc041cd37262880e5030b008175c45b0c46, 73fe8b8fb4bd7776362fd356fdc189c93cf5d9f6724f6237d829024c10263fe5, 40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759
Pteranodon	SHA256	18b2956ceea0e45e2183dc1590fb306f9431943ed612e110af508d819d2ffd67, f08ea988890f33b18ae15d6d3466be0d60e974dece876450f16a0c82bf8469a7, 1f8a3ec047e0f44f1f21e1e3f8af5ea32749ecac3e2bef4fc2ba1a2006934581, c6e629c8375df83184401dd941ca2d490e78a1a338a9d0acdd43665b333cebfe,

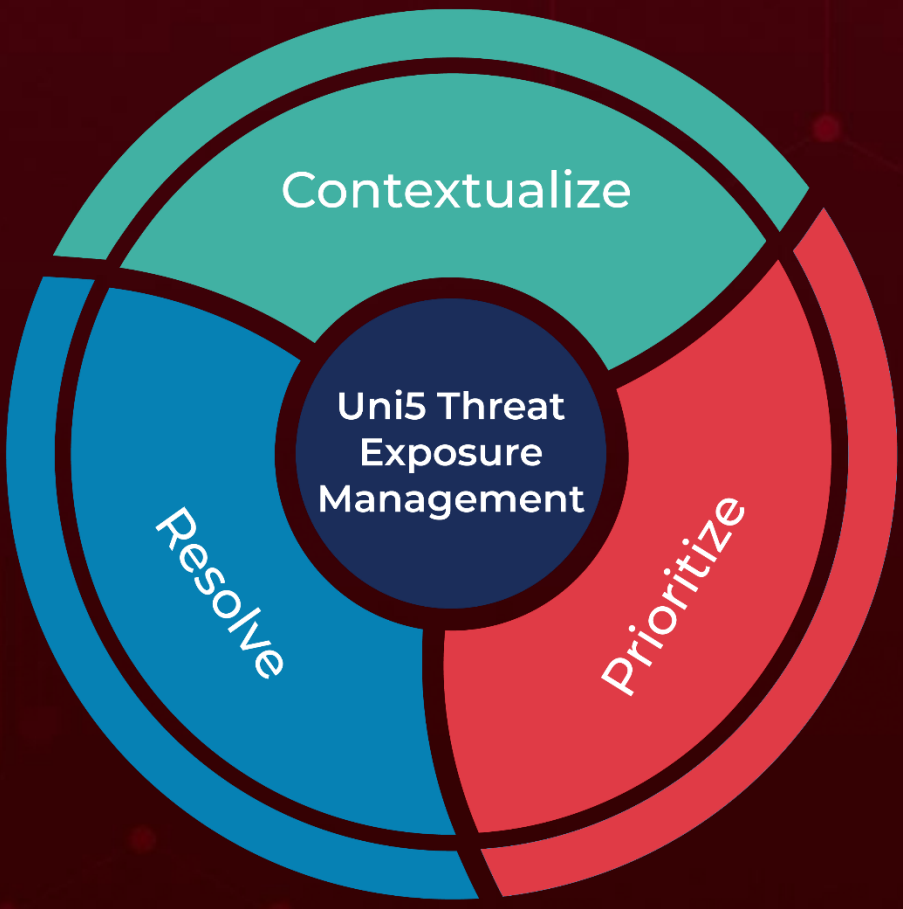
Attack Name	TYPE	VALUE
Pteranodon	SHA256	7370668e7d715e19d36a7580ca04f349c7365d568ffbb5735eb6c79d80d63b63, 9b14d367c99b7d9187a58406ad3eb55e2dee12b4b2bc341f9058c622b7b87fa3
GamaWiper	SHA256	d4ce4776bdad9b741a1e8345b41737245b80f4cf8d361ebb1ae5415c7a4fe1eb, 9a39423ec90dc06a3058279cd744c08d83252d1c7096633b9853e435cc205755

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

December 16, 2025 . 8:00 AM

More at www.hivepro.com