Date of Publication
May 5, 2026

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

APRIL 2026

Table Of Contents

Summary..... 03

Insights..... 04

Threat Distribution..... 05

Celebrity Vulnerabilities..... 06

Vulnerabilities Summary..... 08

Attacks Summary..... 14

Adversaries Summary..... 18

Targeted Countries..... 25

Targeted Industries..... 26

Top Indicators of Compromise (IOCs)..... 28

Vulnerabilities Exploited..... 31

Attacks Executed..... 52

Adversaries in Action..... 87

MITRE ATT&CK TTPS..... 102

Top 5 Takeaways..... 113

Recommendations..... 114

Appendix..... 115

Indicators of Compromise (IoCs)..... 116

What Next?..... 125

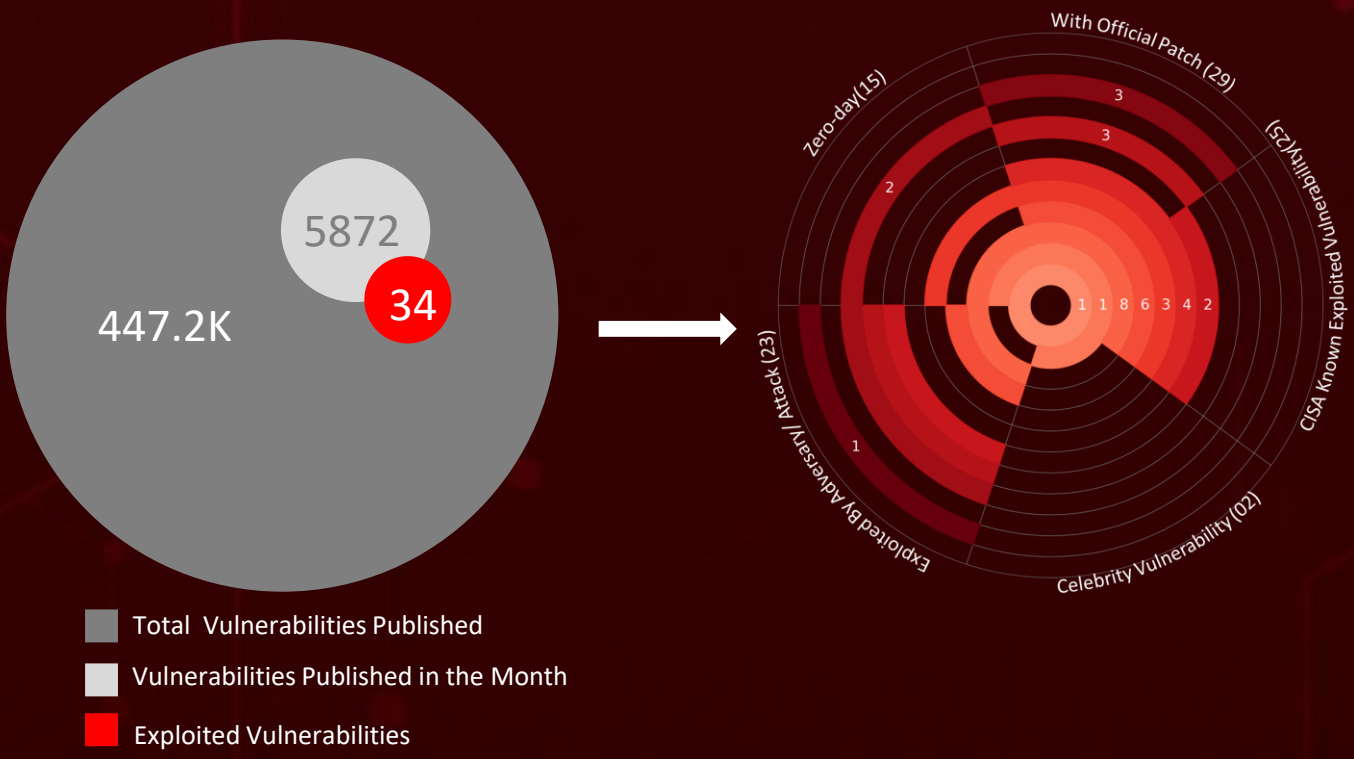
Summary

April reshaped the cybersecurity landscape with active exploitation of **15** zero-days. Google pushed out emergency patches for **CVE-2026-5281**, a Chrome zero-day already under active exploitation, stemming from a use-after-free flaw in the WebGPU-based Dawn component. The vulnerability allows attackers to manipulate memory and execute arbitrary code, making immediate patching non-negotiable.

Meanwhile, **Handala Hack Team** Iran-affiliated threat group launched a destructive campaign against GCC critical infrastructure, allegedly wiping 6 PB of data and exfiltrating 149 TB of classified documents via compromised VPN credentials, infostealer-harvested accounts, and targeted phishing.

Scattered LAPSUS$ Hunters (SLH) are scaling cloud-focused data theft and extortion by exploiting trusted SaaS integrations, moving laterally across platforms, and pressuring victims through data leaks, DDoS attacks, and targeted harassment, often blurring attribution as impersonators mimic well-known cybercrime brands.

Finally, the rebranded **VECT 2.0** ransomware group is rapidly expanding its RaaS ecosystem with a purpose-built C++ framework designed for efficiency and impact. Alongside this, **Operation TrustTrap** is leveraging a vast phishing infrastructure of over 16,800 domains, cleverly mimicking government services across multiple countries by manipulating subdomains and trusted naming patterns to evade detection. With these increasing risks, strengthening defensive measures is more critical than ever in today's digital landscape.



Insights

In April 2026, a geopolitical cybersecurity landscape unfolds, revealing **United States, Spain, Italy, Germany, and United Kingdom** as the top-targeted countries.

Highlighted in **April 2026** is a cyber battleground encompassing the **Government, Energy, Financial, Transportation,** and **Healthcare** sectors, designating them as the top industries.

The Gentlemen RaaS surges ahead, blending multi-OS encryption with stealthy tunneling and domain-wide deployment to execute fast, synchronized double-extortion at scale.

Storm-2755 AiTM phishing via fake M365 logins steals session tokens, bypasses MFA, and reroutes salaries through Workday.

Operation TrueChaos: The TrueConf CVE-2026-3502 Zero-Day That Turned Against Its Users.

MCPwn (CVE-2026-33032) Auth bypass in Nginx UI ≤2.3.5 lets unauthenticated attackers invoke MCP tools via JSON-RPC to alter configs.

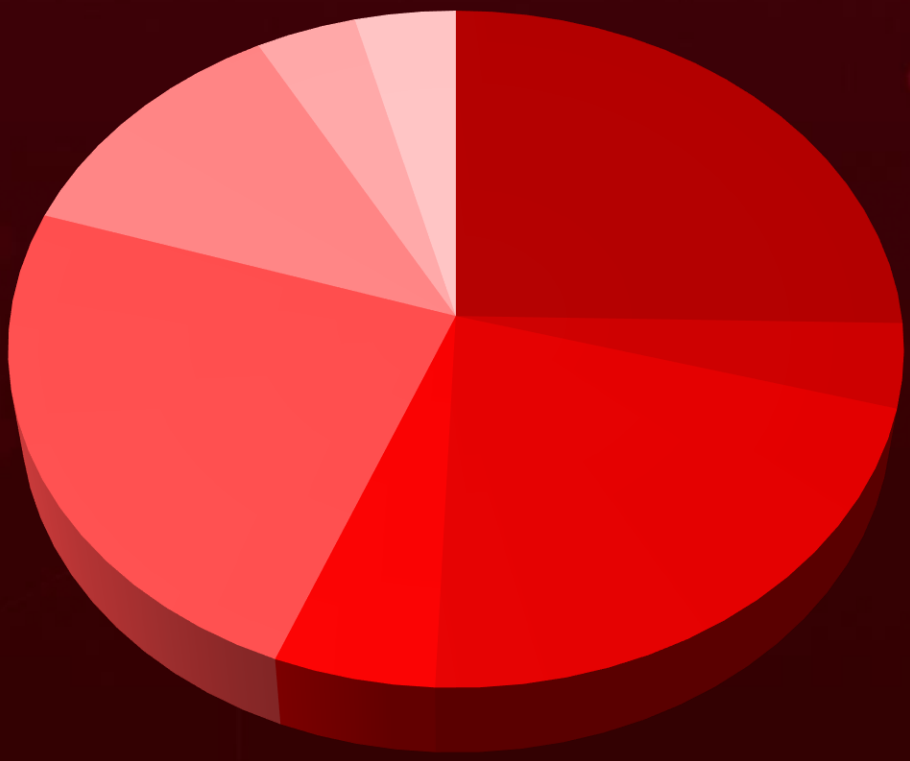
Operation TrustTrap scales deception globally, leveraging 16,800+ spoofed domains to impersonate government services and harvest trust at scale.

Payouts King Ransomware Ex-BlackBasta crew uses spam-bombing and Teams vishing with Quick Assist to deploy ransomware and kill EDR via direct syscalls.

CyberAv3ngers Unleashed: The PLC Attacks Hitting Critical Infrastructure.

TeamPCP turns trusted dev tools into attack vectors, exploiting CI/CD pipelines to weaponize a single weak link into a cascading, multi-ecosystem supply chain breach.

Threat Distribution



- Malware Attacks
- Man-in-the-Middle Attacks
- Injection Attacks
- Denial-of-Service Attacks
- Social Engineering
- Eavesdropping Attacks
- Password Attacks
- Supply Chain Attacks

Celebrity Vulnerabilities

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	TeamPCP
	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:*:*:*	-
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

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-34621</td><td>Prototype Pollution</td><td rowspan="2">Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 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:acrobat_dc:*:*:*:*:continuous:*:*:*
cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:*:continuous:*:*:*
cpe:2.3:a:adobe:acrobat:*:*:*:*:*:classic:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Adobe Acrobat and Reader Improperly Controlled Modification of Object Prototype Attributes Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-1321</td><td>T1203: Exploitation for Client Execution, T1059.007 Command and Scripting Interpreter: JavaScript</td><td>https://helpx.adobe.com/security/products/acrobat/apsb26-43.html</td></tr>
</table>

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-3055	Citrix NetScaler Out-of- Bounds Read Vulnerability	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262	✗	✓	✓
CVE-2026-5281	Google Dawn Use-After- Free Vulnerability	Google Chrome (Before 146.0.7680.178)	✓	✓	✓
CVE-2026-33634	Aquasecurity Trivy Embedded Malicious Code Vulnerability	Aquasecurity setup-trivy Version before 0.2.6, aquasecurity trivy-action Before 0.35.0, Aquasecurity Trivy version before 0.69.3	✗	✓	✓
CVE-2025-29927	Vercel Next.js Middleware Authorization Bypass Vulnerability	Next.js version 1.11.4 and prior to versions 12.3.5, 13.5.9, 14.2.25, and 15.2.3	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2021-22681	Rockwell Multiple Products Insufficient Protected Credentials Vulnerability	Rockwell Automation Multiple Products: Studio 5000 Logix Designer, Logix Controllers (multiple)	✗	✓	✓
CVE-2026-21513	Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability	Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019	✓	✓	✓
CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems)	✓	✓	✓
CVE-2018-10561	Dasan GPON Routers Authentication Bypass Vulnerability	Dasan GPON home routers	✗	✓	✗
CVE-2018-10562	Dasan GPON Routers Command Injection Vulnerability	Dasan GPON home routers	✗	✓	✗

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-12847	NETGEAR DGN1000 authentication bypass vulnerability	NETGEAR DGN1000 before 1.1.00.48	✗	✗	✓
CVE-2026-34621	Adobe Acrobat and Reader Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability	Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 and earlier)	✓	✓	✓
CVE-2026-39987	Marimo Terminal WebSocket Pre-Auth Remote Code Execution Vulnerability	Marimo versions before 0.23.0	✗	✓	✓
CVE-2025-27152	Axios SSRF and Credential Leakage Vulnerability	Axios version before 1.8.2	✗	✗	✓
CVE-2026-32201	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft Office SharePoint Server	✓	✓	✓
CVE-2026-33825	Microsoft Defender Elevation of Privilege Vulnerability	Microsoft Defender	✗	✓	✓
CVE-2026-33032	Nginx Authentication Bypass Vulnerability	Nginx UI (all versions through v2.3.5)	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-34197	Apache ActiveMQ Improper Input Validation Vulnerability	Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	✗	✓	✓
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E- Business Suite Versions 12.2.3- 12.2.14	✓	✓	✓
CVE-2021-35587	Oracle Fusion Middleware Unspecified Vulnerability	Oracle Access Manager product of Oracle Fusion Middleware affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0.	✗	✓	✓
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR-4104 and DVR-4216 up to 20240412	✗	✗	✗
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532	✓	✗	✗

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	✓	✓	✓
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	✗	✓	✓
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	✗	✓	✓
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier	✓	✗	✗
CVE-2025-55182	React2Shell (Meta React Server Components Remote Code Execution Vulnerability)	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	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-35616	Fortinet FortiClient EMS Improper Access Control Vulnerability	Fortinet FortiClient EMS version 7.4.5 through 7.4.6	✓	✓	✓
CVE-2026-21643	Fortinet FortiClient EMS Sql Injection Vulnerability	Fortinet FortiClient EMS 7.4.4	✗	✓	✓
CVE-2026-3502	TrueConf Client Download of Code Without Integrity Check Vulnerability	TrueConf Client for Windows (versions 8.1.0 through 8.5.2)	✓	✓	✓
CVE-2023-50224	TP-Link TL-WR841N Authenticati on Bypass by Spoofing Vulnerability	TP-Link WR841N	✗	✓	✓
CVE-2025-20333	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)	✓	✓	✓
CVE-2025-20362	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall (FTD)	✓	✓	✓
CVE-2026-42208	BerriAI LiteLLM SQL Injection Vulnerability	BerriAI LiteLLM	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
WAVESHAPER.V2	Backdoor	-	Axios npm package	-	Supply Chain
SILKBELL	Dropper	-	Axios npm package	-	Supply Chain
Vect ransomware	Ransomware	-	Windows, Linux, VMware ESXi	-	-
Havoc	Framework	CVE-2026-3502	TrueConf Client	✓	Exploiting vulnerabilities
PrismexDrop	Dropper	CVE-2026-21513 CVE-2026-21509	Microsoft Office, Microsoft Windows (MSHTML Framework)	✓	Exploiting vulnerabilities
PrismexLoader	Loader	CVE-2026-21513 CVE-2026-21509	Microsoft Office, Microsoft Windows (MSHTML Framework)	✓	Exploiting vulnerabilities
PrismexStager	Stager	CVE-2026-21513 CVE-2026-21509	Microsoft Office, Microsoft Windows (MSHTML Framework)	✓	Exploiting vulnerabilities
LucidRook	Stager	-	Microsoft Windows	-	Spear-phishing
PrismexSheet	Dropper	-	Microsoft Office, Microsoft Windows (MSHTML Framework)	-	Exploiting vulnerabilities
LucidPawn	Dropper	-	Microsoft Windows	-	Spear-phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SNOWBELT	Backdoor	-	Windows, Linux	-	Social Engineering
SNOWGLAZE	Tunneler	-	Windows, Linux	-	Social Engineering
SNOWBASIN	Backdoor	-	Windows, Linux	-	Social Engineering
EntryShell	Backdoor	-	Windows	-	Social Engineering
AdaptixC2 Beacon agent	Beacon agent	-	Windows	-	Social Engineering
TOSHIS loader	Loader	-	Windows	-	Social Engineering
The Gentlemen	Ransomware	CVE-2024-55591, CVE-2023-27532, CVE-2024-37085, CVE-2025-7771	Windows, Linux, NAS, BSD, and VMware ESXi		Exploiting Vulnerabilities
SystemBC	Backdoor	CVE-2024-55591, CVE-2023-27532, CVE-2024-37085, CVE-2025-7771	Windows, Linux, NAS, BSD, and VMware ESXi		Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LucidKnight	Reconnaissance tool	-	Microsoft Windows	-	Spear-phishing
Masjesu	Botnet	-	-	-	Exploiting Vulnerabilities
Handala	Wiper	-	Windows	-	Phishing
Payouts King	Ransomware	-	Windows	-	Vishing
PHANTOMPULSE	RAT	-	Windows, macOS	-	Obsidian plugin abuse
PHANTOMPULL	Loader	-	Windows, macOS	-	Obsidian plugin abuse
LummaC2	Stealer	CVE-2025-31324	SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware	✓	Exploiting Vulnerabilities
StealC	Stealer	CVE-2025-31324		✓	Exploiting Vulnerabilities
Vidar	Stealer	CVE-2025-31324		✓	Exploiting Vulnerabilities
RedLine	Stealer	CVE-2025-31324		✓	Exploiting Vulnerabilities
Meduza	Stealer	CVE-2025-31324		✓	Exploiting Vulnerabilities
Rhadamanthys	Stealer	CVE-2025-31324		✓	Exploiting Vulnerabilities
Nexcorium	Botnet	CVE-2024-3721, CVE-2017-17215	TBK DVR- 4104 / DVR- 4216, Huawei HG532	✗	Exploiting Vulnerabilities
Lotus Wiper	Wiper	-	-	-	-
LOTUSLITE backdoor (v1.1)	Backdoor	-	Windows	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
FIRESTARTER	Backdoor	CVE-2025-20333 CVE-2025-20362	Cisco Secure Firewall ASA and FTD Software		Exploiting Vulnerabilities
LINE VIPER	Loader	CVE-2025-20333 CVE-2025-20362	Cisco Secure Firewall ASA and FTD Software		Exploiting Vulnerabilities
RayInitiator	Bootkit	CVE-2025-20333 CVE-2025-20362	Cisco Secure Firewall ASA and FTD Software		Exploiting Vulnerabilities

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
TeamPCP	Espionage, Sabotage, Disruption, Financial Gains	-	CVE-2026-33634 CVE-2025-29927 CVE-2025-55182	Vect ransomware	-
UNC1069	Financial crime	North Korea	-	WAVESHAPER.V2 (aka ZshBucket RAT), SILKBELL	Axios npm package (versions 1.14.1 and 0.30.4), Node.js environments, CI/CD pipelines
UAT-10362	Information Theft, Espionage	-	-	LucidRook, LucidPawn, LucidKnight	Windows
Handala Hack	Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated	Iran	-	Handala	Windows
Storm-2755	Financial gain	Iran	CVE-2025-27152	-	Windows
Scattered Spider	Financial gain	Suspected UK and US	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
ShinyHunters	Financial gain	-	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware
LAPSUS$	Financial gain	Brazil	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware
Mustang Panda	Information theft and espionage	China	-	LOTUSLITE backdoor (v1.1)	-
UNC6692	Information theft and espionage	-	-	SNOWBELT, SNOWGLAZE, SNOWBASIN	-
Tropic Trooper	Information theft and espionage	China	-	EntryShell backdoor, AdaptixC2 Beacon agent, TOSHIS loader	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT28	Information theft and espionage	Russia	CVE-2023-50224 CVE-2026-21513 CVE-2026-21509	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet	TP-Link WR841N, Windows
CyberAv3ngers	Sabotage and destruction	Iran	CVE-2021-22681	-	Rockwell Automation CompactLogix PLCs, Micro850 PLCs, Rockwell Automation Studio 5000 Logix Designer, RSLogix 5000
UAT-4356	Espionage	China	CVE-2025-20333 CVE-2025-20362	FIRESTARTER, LINE VIPER, RayInitiator	Cisco Secure Firewall ASA and FTD Software
APT36	Information theft and espionage	Pakistan	-	-	-

Targeted Products

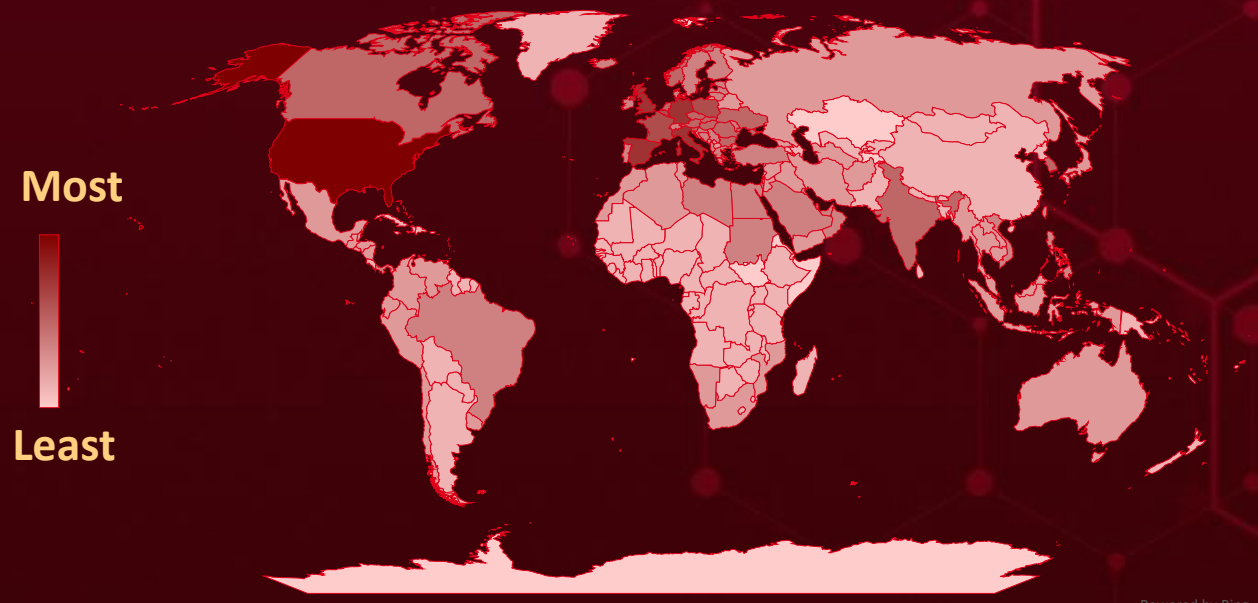
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
citrix	Network Device	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262
	Web Browser	Google Chrome (Before 146.0.7680.178)
aqua run free	Container Security	Aquasecurity setup-trivy Version before 0.2.6, aquasecurity trivy-action Before 0.35.0, Aquasecurity Trivy version before 0.69.3
NEXT.JS	Web Framework	Next.js version 1.11.4 and prior to versions 12.3.5, 13.5.9, 14.2.25, and 15.2.3
FORTINET	Security	Fortinet FortiClient EMS version 7.4.5 through 7.4.6
	Operating System	FortiOS Versions 7.0.0 through 7.0.16
	Application	FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19
	Network Device	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

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
TrueConf	Operating System	TrueConf Client for Windows (versions 8.1.0 through 8.5.2)
tp-link	Network Device	TP-Link WR841N
Microsoft	Operating System	Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019
	Productivity Software	Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems)
		Microsoft Office SharePoint Server
	Security Software	Microsoft Defender
DASAN DNS Dasan Network Solutions	Network Device	Dasan GPON home routers
NETGEAR	Network Device	NETGEAR DGN1000 before 1.1.00.48
Adobe	Productivity Software	Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 and earlier)
marimo	Developer Tool	Marimo versions before 0.23.0

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
AXIOS	JavaScript Library	Axios version before 1.8.2
NGINX	Web Framework	Nginx UI (all versions through v2.3.5)
ORACLE	Enterprise Software	Oracle E- Business Suite Versions 12.2.3-12.2.14
		Oracle Access Manager product of Oracle Fusion Middleware affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0.
APACHE HTTP SERVER PROJECT	Web Framework / Server	Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)
SAP	Enterprise Software	SAP NetWeaver
TBK	Network Device	TBK DVR-4104 and DVR-4216 up to 20240412
HUAWEI	Network Device	Huawei HG532

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
VEEAM	Backup Software	Veeam Backup & Replication Cloud Connect
vmware by Broadcom	Virtualization	VMware ESXi
TECHPOWERUP	System Driver / Utility	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier
CISCO	Network device	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7
BerriAI	Proxy server	BerriAI LiteLLM (>= 1.81.16, < 1.83.7)

Targeted Countries



Color	Countries
	United States
	Spain
	Italy
	Germany
	United Kingdom
	France
	Poland
	Belgium
	Ukraine
	Slovakia
	Norway
	Canada
	South Korea
	Czech Republic
	Netherlands
	Hungary
	Romania
	India
	Slovenia
	Israel

Color	Countries
	Austria
	Bulgaria
	Sweden
	Saudi Arabia
	Qatar
	Denmark
	Cyprus
	Egypt
	Croatia
	Kuwait
	Andorra
	Latvia
	Singapore
	Libya
	Bahrain
	Lithuania
	Taiwan
	Albania
	Portugal
	Vietnam

Color	Countries
	Republic of Ireland
	United Arab Emirates
	San Marino
	Estonia
	Serbia
	Montenegro
	Greece
	Finland
	Iceland
	Bosnia and Herzegovina
	Sudan
	Oman
	Switzerland
	Panama
	Turkey
	Philippines
	Brazil
	Monaco
	Moldova
	Angola

Color	Countries
	Malta
	Liechtenstein
	Thailand
	South Africa
	Uruguay
	Namibia
	Australia
	Hong Kong
	Guatemala
	Nicaragua
	Chile
	North Macedonia
	Yemen
	Brunei
	Syria
	Algeria
	Mexico
	Palestine
	Honduras
	Ecuador

Color	Countries
	Mozambique
	Peru
	Afghanistan
	Indonesia
	Colombia
	Iran
	Georgia
	Iraq
	Malaysia
	Cambodia
	Belarus
	El Salvador
	Tunisia
	Japan
	Turkmenistan
	Russia
	Holy See
	Jordan
	Morocco
	Kosovo
	Venezuela

Targeted Industries

Most

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1071** Application Layer Protocol	**T1190** Exploit Public-Facing Application	**T1566** Phishing	**T1036** Masqueradin g
T1078 Valid Accounts	**T1204** User Execution	**T1005** Data from Local System	**T1027** Obfuscated Files or Information	**T1071.001** Web Protocols
T1082 System Information Discovery	**T1547** Boot or Logon Autostart Execution	**T1036.005** Match Legitimate Name or Location	**T1083** File and Directory Discovery	**T1041** Exfiltration Over C2 Channel
T1053 Scheduled Task/Job	**T1562.001** Disable or Modify Tools	**T1204.002** Malicious File	**T1059.001** PowerShell	**T1552** Unsecured Credentials
T1105 Ingress Tool Transfer	**T1588** Obtain Capabilities	**T1021** Remote Services	**T1070** Indicator Removal	**T1562** Impair Defenses

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Vect ransomware	IPv4	158[.]94[.]210[.]11
	SHA256	8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d
Havoc	MD5	248a4d7d4c48478dcbeade8f7dba80b3
	IPv4	43[.]134[.]90[.]60, 43[.]134[.]52[.]221, 47[.]237[.]15[.]197
PrismexDrop	SHA256	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae
PrismexLoader	SHA256	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9
PrismexStager	SHA256	57357655a62e3a8b1f4b78e1d3ed7e0f6d59a9bac213087294f91bb7847b2a8f
Handala Wiper	MD5	5986ab04dd6b3d259935249741d3eff2
	SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
Payouts King	SHA256	335ad12a950f885073acdfebb250c93fb28ca3f374bbba5189986d9234dcbff4, d68ce82e82801cd487f9cd2d24f7b30e353cafd0704dcdf0bb8f12822d4227c2
PHANTOMPULSE	SHA256	33dacf9f854f636216e5062ca252df8e5bed652efd78b86512f5b868b11ee70f
	Domain	panel[.]fefea22134[.]net
PHANTOMPULL	SHA256	70bbb38b70fd836d66e8166ec27be9aa8535b3876596fc80c45e3de4ce327980
Nexcorium	SHA256	37132e804ccb3fc4ba1f72205da70c3d7a6e66b43178707a9d8ee1156d815c21, e4789416c35b345e75c023a8c07c207c79937c6a5444e1c29d85d18d2f660d8c, 0b510f93f47590791626d2fa74ddd62ba6eb8a5a5bb7b8476c0ceffc7be94ebe, 9b805585c457811d2c5c5664ede9ee869b53e3c9999100505d7ee8de7f855fdf,

Attack Name	TYPE	VALUE
Nexcorium	SHA256	95d1eb12d58206319c514c7240d058c512bb22b31f6ea22ed8be3ae44305c9f7, 7c01d5b53861cd34e10a79fdea16dcf08bce9c78ed72abd6d6f3e9ce75a24734, 838e35b62a6b38675e467301166cdcc54f98d528fe43d56936caeffec88ac696, 2ccf23b8165e8c05899aa7ba4755b896ebf1d20d3b701cffdc768482486b0a74, 29404df12a7723ce46c8b199c88a808aa315dd8ff8fd1e06a34ccd3d16f4553b, b1274de00a7f3d7ab9792ec3456e9d5bf057738666f34183f1d72060e2d4f678, 721c7cb2109ec97c14413cb8b58ddce0ecf0c1f13f22ee4f72eed79b57592cf5, 89dae116c77b0035277d39dfe01043624427c119ddee8883a3ba54a42a6ae400
The Gentlemen	SHA256	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67, 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d, 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235, 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd, 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8, 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923, 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c, 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db, 91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1, 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3, 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454, a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad, ,

Attack Name	TYPE	VALUE
The Gentlemen	SHA256	c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8, c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73, ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2, efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f, f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12, fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958, 5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca, 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19, 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c
SystemBC	SHA256	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5
LINE VIPER	SHA256	bd82a15394f80c6eb82e439dcec93eb8535e9bbc9b26e991fef8bd92c5ba345f, e6684678ace298f81aedd140415c74553612bf86b904c11ca059424ef8322e7c, 8dab6e20cfa9ec1445eb32d3ec836e3c17b97cee622caa1b7e6b110b44df769a, 531b619e8b27cfad4628c9539f2707903d129411bd908a0d6f862e382d7ac5a4, 5bf3100c49718b7567acfc5d84606dc010b91e10cedd25aef13e27f0ffc0f997, 27ed8628441ddc88bba8aba5783665b096975d948db92cb8ffc7790ddfa68414, 3a9486da872af184ba250059311f1ee70f46f84b6d92dcdfa4f0396eb83ffb6a, 0bdb8efb72c6566be86963ffb2ec5a135362e18e5e8c6afd3e42b3a761b85428, 0297f9852a70b04cdf2aaf5d66611451d1bde918e8e59ebe8e573e5a0b449af0, 1a4a37df0a6b5ad02b7e91ccbc7c706079761a4e85bebaa09533c3017c9aff71

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-3055		NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler Out-of-Bounds Read Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-125	T1190: Exploit Public-Facing Application; T1212: Exploitation for Credential Access	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-33634</td><td>✗</td><td rowspan="2">Aquasecurity setup-trivy Version before 0.2.6, aquasecurity trivy-action Before 0.35.0, Aquasecurity Trivy version before 0.69.3</td><td rowspan="2">TeamPCP</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:aquasec:setup-trivy:*:*:*:*:*:*:*:* cpe:2.3:a:aquasec:trivy:0.69.4:*:*:*:*:go:*:* cpe:2.3:a:aquasec:trivy_action:*:*:*:*:*:*:*:* cpe:2.3:a:litellm:litellm:*:*:*:*:*:*:*:* cpe:2.3:a:telnyx:telnyx:*:*:*:*:python:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Aquasecurity Trivy Embedded Malicious Code Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-506</td><td>T1059: Command and Scripting Interpreter</td><td>https://github.com/aquasecurity/trivy/releases</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-29927</td><td>✕</td><td rowspan="2">Next.js version 1.11.4 and prior to versions 12.3.5, 13.5.9, 14.2.25, and 15.2.3</td><td rowspan="2">TeamPCP</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:vercel:next.js:*:*:*:*:*:node.js:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Vercel Next.js Middleware Authorization Bypass Vulnerability</td><td>✕</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-863
CWE-285</td><td>T1059: Command and Scripting Interpreter</td><td>https://github.com/vercel/next.js/releases</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-35616</td><td>  </td><td rowspan="2">Fortinet FortiClient EMS version 7.4.5 through 7.4.6</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:fortinet:forticlientems:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Fortinet FortiClient EMS Improper Access Control Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-284</td><td>T1562.001: Disable or Modify Tools, T1059: Command and scripting interpreter</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-099</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21643	✗	Fortinet FortiClient EMS 7.4.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*:*:*	-
Fortinet FortiClient EMS Sql Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and scripting interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-25-1142

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-3502	✗	TrueConf Client for Windows (versions 8.1.0 through 8.5.2)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trueconf:trueconf_client:*:*:*:*:*:windows:*:*	Havoc
TrueConf Client Download of Code Without Integrity Check Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1195.002: Supply Chain Compromise, T1072: Software Deployment Tools	https://trueconf.com/downloads/windows.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-50224		TP-Link WR841N	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*	-
TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2021-22681		Rockwell Automation Multiple Products: Studio 5000 Logix Designer, Logix Controllers (multiple)	CyberAv3ngers
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rockwellautomation:factorytalk_services_platform:*:*:*:*:*:*:*:*	-
Rockwell Multiple Products Insufficient Protected Credentials Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-522	T0862: Supply Chain Compromise, T0859: Valid Accounts, T1552.004: Unsecured Credentials: Private Keys	https://www.rockwellautomation.com/es-es/trust-center/security-advisories/advisory.PN1550.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21513	✗ ZERO-DAY	Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019	Pawn Storm
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet
Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-693	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21509	✗ ZERO-DAY	Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems)	Pawn Storm
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:enterprise:*:*:*	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet
Microsoft Office Security Feature Bypass Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-807	T1566: Phishing, T1204: User Execution, T1204.002: Malicious File, T1055: Process Injection	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2018-10561	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
Dasan GPON Routers Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication, T1059: Command and Scripting Interpreter	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2018-10562	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
Dasan GPON Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-12847		NETGEAR DGN1000 before 1.1.00.48	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:netgear:dgn1000:-:*:*:*:*:*:*:*	Masjesu botnet (aka XorBot)
NETGEAR DGN1000 authentication bypass vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306, CWE-78	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://www.netgear.com/support/product/dgn1000

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-39987	✗	Marimo versions before 0.23.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:marimo-team:marimo:*:*:*:*:*:python:*:*	-
Marimo Terminal WebSocket Pre-Auth Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006 Command and Scripting Interpreter: Python	https://github.com/marimo-team/marimo/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-27152	✗	Axios version before 1.8.2	Storm-2755
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:axios:axios:*:*:*:*:*:node.js:*:*	-
Axios SSRF and Credential Leakage Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://github.com/axios/axios/releases/tag/v1.8.2

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-32201</td><td>✗</td><td rowspan="2">Microsoft Office SharePoint Server</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:microsoft:sharepoint_server:*:*:*:*:subscription:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft SharePoint Server Spoofing 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>T1190 Exploit Public-Facing Application, T1036 Masquerading, T1656 Impersonation</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-5281	 ZERO-DAY	Microsoft Edge (Chromium-based), Google Chrome	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Chromium Use after free in Dawn Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189 Drive-by Compromise, T1203 Exploitation for Client Execution, T1068 Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281, https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-33825	✗	Microsoft Defender	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_defender:*:*:*:*:*:*:*:*	-
Microsoft Defender Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1220	T1068 Exploitation for Privilege Escalation, T1562.001 Impair Defenses: Disable or Modify Tools, T1006 Direct Volume Access	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-33032	MCPwn	Nginx UI (all versions through v2.3.5)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:nginxui:nginx_ui:*:*:*:*:*:*:*:*	-
Nginx Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190 Exploit Public-Facing Application, T1505 Server Software Component, T1565.002 Data Manipulation: Transmitted Data Manipulation	https://github.com/0xJacky/nginx-ui/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-34197	✗	Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_broker:*:*:*:*:*:*:*:*	-
Apache ActiveMQ Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20, CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://activemq.apache.org/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-31324	✗	SAP NetWeaver	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*:*	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
SAP NetWeaver Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-434	T1059: Command and Scripting Interpreter	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-61882	✗	Oracle E- Business Suite Versions 12.2.3- 12.2.14	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
Oracle E-Business Suite Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1071: Application Layer Protocol	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2021-35587	✗	Oracle Access Manager product of Oracle Fusion Middleware affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0.	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:access_manager:*:*:*:*:*:*:*:*	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
Oracle Fusion Middleware Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1071: Application Layer Protocol	https://www.oracle.com/security-alerts/cpujan2022.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-3721	✗	TBK DVR-4104 and DVR-4216 up to 20240412	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tbkvision:tbk-dvr4216:*:*:*:*:*:*:*:* cpe:2.3:h:tbkvision:tbk-dvr4104:*:*:*:*:*:*:*:*	Nexcorium
TBK DVR OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2017-17215	✗	Huawei HG532	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:huawei:hg532:-:*:*:*:*:*:*:*	Nexcorium
Huawei HG532 Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-20	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-55591	✗	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
Fortinet FortiOS Authorization Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1133: External Remote Services	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-27532	✗	Veeam Backup & Replication Cloud Connect	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1212: Exploitation for Credential Access	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-37085	✗	VMware ESXi	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287 CWE-305	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/esxi-update-and-patch-release-notes/vsphere-esxi-803-release-notes.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-7771	✗	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:techpowerup:throttlestop:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
TechPowerUp ThrottleStop Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-782	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-34197		Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_broker:*:*:*:*:*:*:*:*	-
Apache ActiveMQ Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20, CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://activemq.apache.org/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20333	 ZERO-DAY	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT-4356
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*	FIRESTARTER, LINE VIPER, RayInitiator
Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-120	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1542.004 Pre-OS Boot: ROMMONkit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20362	✗	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT-4356
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	FIRESTARTER, LINE VIPER, RayInitiator
Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-862	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-42208	✗	BerriAI LiteLLM (>= 1.81.16, < 1.83.7)	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:berriai:litellm:*:*:*:*:*:*:*:*	-
BerriAI LiteLLM SQL Injection Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-89	T1190: Exploit Public-Facing Application; T1005: Data from Local System; T1552: Unsecured Credentials	https://github.com/BerriAI/litellm/releases/tag/v1.83.7-stable

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
WAVESHAPER.V2	WAVESHAPER.V2 (aka ZshBucket RAT) is a cross-platform backdoor primarily developed in C++ to target macOS systems, where it is used to gather system information, enumerate directories, and execute additional payloads. It relies on command-line arguments to obtain its command-and-control (C2) server details, enabling flexible deployment across compromised environments. Across all versions, the malware maintains consistent communication patterns, beaconing to its C2 server over port 8000 at regular 60-second intervals using Base64-encoded JSON data, along with a hard-coded User-Agent string to standardize its network traffic and evade detection.	Supply Chain	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Data theft, Execute commands, File System Enumeration	Axios npm package
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SILKBELL	SILKBELL is a stealthy loader that adapts its behavior based on the victim's operating system, dynamically delivering platform-specific payloads at runtime. To obscure its intent, it employs a custom obfuscation scheme combining XOR and Base64 encoding to hide critical elements such as the command-and-control (C2) URL and OS-specific execution commands.	Supply Chain	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Dropper		Drops additional payloads	Axios npm package
ASSOCIATED ACTOR			**PATCH LINK**
-			–

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Vect ransomware	Vect is a Ransomware-as-a-Service (RaaS) operation that surfaced in late December 2025 to early January 2026, rapidly positioning itself as a polished and professional threat actor. Unlike many ransomware groups that rely on repurposed or leaked builders, Vect stands out for deploying custom-developed malware written in C++, giving it greater control over functionality and evasion techniques. This tailored approach enables the group to support multi-platform targeting, reflecting a more advanced and adaptable ransomware framework designed for modern enterprise environments.	-	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Ransomware		Encrypt Data, Data Theft	Windows, Linux, VMware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Havoc	Havoc is an open-source command-and-control framework designed for post-exploitation, penetration testing, and adversary simulation. Despite its legitimate purpose, it is frequently repurposed by threat actors to manage and sustain real-world intrusions.	Exploiting vulnerabilities	CVE-2026-3502
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Framework		Persistent remote access, Surveillance, Privilege escalation	TrueConf Client
ASSOCIATED ACTOR			**PATCH LINK**
-			https://trueconf.com/downloads/windows.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PrismexDrop	PrismexDrop is a native dropper that initializes the environment for later-stage payloads and establishes persistence through COM hijacking.	Exploiting vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Dropper		Bypasses standard security mechanisms, maintains stealthy persistence	Microsoft Office, Microsoft Windows (MSHTML Framework)
ASSOCIATED ACTOR			**PATCH LINK**
-			_

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">PrismexLoader</td><td rowspan="6">PrismexLoader is a proxy DLL that retrieves embedded payloads from steganographic PNG images using a proprietary “Bit Plane Round Robin” extraction algorithm.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-21513
CVE-2026-21509</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="4">Malware staging, Stealth execution</td><td>Microsoft Office, Microsoft Windows (MSHTML Framework)</td></tr>
<tr><td>TYPE</td><td>PATCH LINKS</td></tr>
<tr><td>Loader</td><td rowspan="2">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509,
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>Pawn Storm</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">PrismexStager</td><td rowspan="6">PrismexStager is a Covenant Grunt stager that leverages Filen.io cloud storage as a covert command-and-control channel.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-21513
CVE-2026-21509</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Remote control, Data exfiltration</td><td>Microsoft Office, Microsoft Windows (MSHTML Framework)</td></tr>
<tr><td>Stager</td><td>PATCH LINKS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513</td></tr>
<tr><td>Pawn Storm</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LucidRook	LucidRook is an advanced stager that integrates a Lua interpreter and Rust-compiled libraries within a DLL to retrieve and execute staged Lua bytecode payloads.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload execution, Modular staging	Microsoft Windows
Stager			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-10362			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrismexStager	PrismexStager is a Covenant Grunt stager that leverages Filen.io cloud storage as a covert command-and-control channel.	Exploiting vulnerabilities	CVE-2026-21513 CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote control, Data exfiltration	Microsoft Office, Microsoft Windows (MSHTML Framework)
Stager			**PATCH LINKS**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
Pawn Storm			

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">LucidPawn</td><td rowspan="6">LucidPawn is a dropper that employs region-specific anti-analysis checks, manages decoy documents by identifying targeted file extensions, and embeds two AES-encrypted binaries.</td><td>Spear-phishing</td><td>-</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Anti-analysis evasion, Payload concealment</td><td>Microsoft Windows</td></tr>
<tr><td>Dropper</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>UAT-10362</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LucidKnight	LucidKnight is a companion reconnaissance tool that profiles targets by exfiltrating system information via Gmail. Implemented as a 64-bit Windows DLL, it incorporates Rust-compiled components to support staged escalation toward full payload deployment.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Reconnaissance tool		System profiling, Data exfiltration	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Masjesu</td><td rowspan="6">Masjesu is a commercially operated IoT botnet that initiates infection by binding to a hardcoded TCP port (55988), enabling direct attacker access. It maintains persistence by creating a cron job that repeatedly executes a renamed, masqueraded process at 15-minute intervals.</td><td>Exploiting Vulnerabilities</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Botnet</td><td rowspan="3">Remote access, Persistent control</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://www.netgear.com/support/product/dgn1000</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Handala	Handala Wiper is a custom destructive malware deployed via Group Policy logon scripts as handala.bat, enabling it to execute remotely from the Domain Controller without being written to disk on target systems. It is designed to overwrite files across the system and corrupt the Master Boot Record (MBR), leading to severe, low-level data destruction and system inoperability. The wiper also leverages the Telegram Bot API for command-and-control communication, helping operators manage attacks while maintaining a level of stealth.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Wiper		Data destruction	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Payouts King</td><td rowspan="6">Payouts King is a new ransomware operation first observed in April 2025, assessed with high confidence to be run by former BlackBasta affiliates. It uses AES-256 (CTR) with RSA-4096 and intermittent encryption for large files, combined with heavy obfuscation and direct syscalls to bypass EDR. Double-extortion operation combining data theft with selective file encryption.</td><td>Vishing</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Ransomware</td><td rowspan="3">File encryption, data exfiltration</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>PHANTOMPULSE</td><td rowspan="6">PHANTOMPULSE Is a novel, AI-assisted Windows .NET RAT featuring blockchain-based C2 resolution, tracked under campaign REF6598. It targets finance and cryptocurrency professionals, providing full host control including keylogging, screenshots, file upload/download, and shellcode/DLL injection. It queries transaction data from wallets on Ethereum, Base, and Optimism to dynamically resolve its active C2 server.</td><td>Obsidian plugin abuse</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>RAT</td><td rowspan="3">Remote access, credential theft</td><td>Windows, macOS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>PHANTOMPULL</td><td rowspan="6">PHANTOMPULL is a custom first-stage loader deployed on Windows that decrypts and reflectively loads the PHANTOMPULSE RAT payload entirely in memory. It uses AES-256-CBC encryption and includes anti-analysis techniques to avoid detection. Delivered through abuse of Obsidian's community plugin ecosystem (Shell Commands and Hider plugins) when a victim opens a shared cloud vault.</td><td>Obsidian plugin abuse</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Loader</td><td rowspan="3">In-memory payload loading</td><td>Windows, macOS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LummaC2	LummaC2 is a rapidly evolving information-stealer sold as Malware-as-a- Service.It targets browser data, cryptocurrency wallets, and authentication tokens.It communicates with a C2 panel for exfiltration and victim tracking.	Exploiting Vulnerabilities	CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>StealC</td><td rowspan="6">Stealc is an information-stealing malware offered as a Malware-as-a-Service by a threat actor known as Plymouth on Russian-speaking underground forums since early 2023. Developed in C and built on Windows API functions, it primarily targets sensitive data from web browsers, browser extensions, desktop cryptocurrency wallets, as well as messaging and email clients. To aid in data extraction, it leverages multiple legitimate third-party DLLs commonly associated with browser operations, enabling it to access stored credentials and other valuable information.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Stealer</td><td rowspan="3">Data Theft</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Vidar	Vidar is a widely recognized information-stealing malware family engineered to quietly extract sensitive data from compromised systems. It primarily targets credentials stored in web browsers, cryptocurrency wallet details, session cookies, authentication tokens, autofill entries, and saved payment information, along with files that may contain valuable data. Operating largely in memory, Vidar minimizes its on-disk footprint and maintains communication with remote command-and-control servers, allowing it to discreetly collect and exfiltrate information without triggering obvious signs of compromise.	Exploiting Vulnerabilities	CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RedLine	RedLine Stealer is a versatile malware that can be purchased either as a standalone product or on a subscription basis. It is designed to collect a wide range of information from browsers, including saved credentials, autocomplete data, and credit card details. RedLine Stealer have expanded their capabilities to include the theft of cryptocurrency.	Exploiting Vulnerabilities	CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Meduza</td><td rowspan="6">The Meduza Stealer malware has an objective of comprehensive data theft. It pilfers users' browsing activities, extracting a wide array of browser-related data. From critical login credentials to browsing history and curated bookmarks, no digital artifact is safe. Even crypto wallet extensions, password managers, and 2FA extensions are vulnerable, making Meduza Stealer a significant threat to users' financial and personal data.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Stealer</td><td rowspan="3">Data Theft</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
</table>

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.	Exploiting Vulnerabilities	CVE-2025-31324, CVE-2025- 61882, CVE-2021- 35587
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html, https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/support/?kmContentId=3106344, https://www.oracle.com/security-alerts/cpujan2022.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Nexcorium	Nexcorium follows a design closely aligned with Mirai-based malware, incorporating elements such as XOR-encoded configuration tables, a watchdog component, and a built-in DDoS attack module. Upon execution, it begins by decoding its embedded configuration using XOR, revealing critical details including the command-and-control server domain and port, persistence-related shell commands, a hard-coded brute-force credential list, attack instructions fetched from the C2 server, and integrated exploit code used to expand its reach.	Exploiting Vulnerabilities	CVE-2024-3721 CVE-2017-17215
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Botnet		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			EOL

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lotus Wiper	“Lotus Wiper” is a destructive malware designed to render infected systems irrecoverable by disabling recovery mechanisms, overwriting data on physical drives, and systematically deleting files across all accessible volumes. Through this multi-stage wiping process, it ensures that both system functionality and stored data are permanently destroyed, leaving little to no chance for restoration.	-	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Wiper		Wipes Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSLITE backdoor (v1.1)	The LOTUSLITE backdoor (v1.1) reflects a clear evolution from its earlier iteration, with notable changes in code structure and command-and-control communication. One of the most visible shifts appears in the DLL export table, while version 1.0 exposed 16 functions with DataImporterMain acting as the primary entry point, v1.1 expands this to 22 exports and replaces it with DnxMain at the same ordinal. Overall, the update marks a transition from a monolithic architecture to a more modular design, where responsibilities are distributed across multiple dedicated functions, improving flexibility and potentially making analysis and detection more challenging.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWBELT	SNOWBELT is a malicious Chromium browser extension, distributed via social engineering rather than the official Chrome Web Store, that serves as the initial foothold in the attack chain. Disguised as legitimate extensions like “MS Heartbeat” or “System Heartbeat,” it acts as a JavaScript-based backdoor, maintaining persistence through the browser’s extension framework and techniques like Service Worker Alarms and keep-alive tab injection. Its primary role is to capture attacker commands and forward them to the SNOWBASIN component for execution, effectively enabling continuous monitoring and control.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
-		Intercept commands, Maintain persistence	Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWGLAZE	SNOWGLAZE is a Python-based tunneling component deployed after initial access to handle external communications. Designed to run on both Windows and Linux systems, it establishes a secure, authenticated WebSocket tunnel between the compromised network and the attacker's command-and-control infrastructure, often hosted on services like Heroku. Through this channel, it enables SOCKS proxy functionality, allowing arbitrary TCP traffic to be routed through the infected host for further operations.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Tunneler		Masks malicious traffic	Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWBASIN	SNOWBASIN is a Python-based bindshell that provides hands-on control over the compromised system once access is established. Operating as a persistent backdoor, it typically runs a local HTTP server on port 8000, allowing attackers to execute commands via cmd.exe or PowerShell, capture screenshots, and stage data for exfiltration, effectively enabling direct interaction with the infected host.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Execute Commands	Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EntryShell	EntryShell is a custom backdoor attributed to the Tropic Trooper threat group, historically deployed in espionage operations targeting Chinese-speaking individuals. An EntryShell sample was hosted on the staging server. The sample reused the hardcoded AES-128 ECB key documented in an earlier Tropic Trooper campaign. Its presence on actor infrastructure, combined with the reuse of known watermarks, loaders, and post-exploitation TTPs such as VS Code tunnel abuse, served as a key attribution indicator.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>AdaptixC2 Beacon agent</td><td rowspan="6">AdaptixC2 is an open-source command-and-control (C2) framework that provides operators with a Beacon agent and configurable Beacon Listeners for managing compromised hosts, similar in concept to commercial offensive security tools like Cobalt Strike. Its agents encrypt C2 traffic using a 16-byte RC4 session key generated at initialization, and standard deployments rely on HTTP or TCP listeners for tasking and exfiltration.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Beacon agent</td><td rowspan="4">Encrypt Traffic</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TOSHIS loader	TOSHIS is a custom shellcode loader attributed to the Tropic Trooper threat group, originally observed in the TAOTH campaign. The loader is delivered through trojanized legitimate binaries, most recently a backdoored SumatraPDF reader, where the threat actor hijacks the executable's control flow by redirecting the _security_init_cookie function to execute malicious code, a departure from earlier variants that modified the entry point to jump to the payload.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Loads Payload	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
The Gentlemen	The Gentlemen ransomware-as-a-service (RaaS) operation is quickly gaining traction, drawing in multiple affiliates and claiming over 320 victims, with a significant surge of attacks observed in early 2026. Its toolkit includes a diverse set of lockers written in Go for Windows, Linux, NAS, and BSD systems, along with a C-based variant targeting ESXi, enabling broad coverage across enterprise environments. In a recent incident response case, an affiliate attempted to deploy SystemBC, a proxy malware commonly used in human-operated ransomware campaigns for stealthy tunneling and payload delivery. The group also operates an onion-based leak site to publish stolen data from non-paying victims, while ransom negotiations are handled separately via affiliate-specific Tox IDs, leveraging the decentralized, end-to-end encrypted messaging protocol for secure communication.	Exploiting Vulnerabilities	CVE-2024-55591 CVE-2023-27532 CVE-2024-37085 CVE-2025-7771
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Ransomware		Data encryption, Data Exfiltration	Windows, Linux, NAS, BSD, and VMware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535, https://www.veeam.com/kb4424, https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SystemBC	SystemBC is a proxy malware deployed on compromised hosts to establish covert network access for attackers. It creates SOCKS5 tunnels within the victim's environment and communicates with its command-and-control server using a custom RC4-encrypted protocol. In addition to tunneling, it can download and execute further payloads, either by writing them to disk or injecting them directly into memory for stealthier execution.	Exploiting Vulnerabilities	CVE-2024-55591 CVE-2023-27532 CVE-2024-37085 CVE-2025-7771
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows, Linux, NAS, BSD, and VMware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535, https://www.veeam.com/kb4424, https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>FIRESTARTER</td><td rowspan="6">FIRESTARTER is a stealthy backdoor attributed to UAT-4356 that enables remote access and arbitrary code execution within the LINA process, a core component of Cisco ASA and FTD appliances running FXOS. It operates by hijacking a legitimate handler function at a fixed memory offset, replacing it with a malicious routine that inspects incoming WebVPN XML requests. When a specially crafted request containing a predefined prefix is detected, FIRESTARTER extracts and executes the embedded shellcode directly in memory; otherwise, the traffic is passed to the original handler, helping the backdoor remain covert during normal operations.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-20333
CVE-2025-20362</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td rowspan="2">Backdoor</td><td rowspan="3">System Compromise, Persistence</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>LINE VIPER</td><td rowspan="6">LINE VIPER is a user-mode shellcode loader designed to execute and manage malicious tasks within compromised systems. It is typically delivered in memory by the RayInitiator component through a crafted WebVPN authentication request that includes a partial PKCS7 certificate followed by embedded shellcode. The malware supports dual communication methods, via HTTPS WebVPN sessions or ICMP with responses over raw TCP, and relies on victim-specific tokens, a technique also observed in related tools like LINE DANCER and LINE RUNNER. Once active, LINE VIPER enables a wide range of capabilities, including executing CLI commands, capturing network traffic, bypassing authentication controls, suppressing syslog logs, harvesting user command inputs, and even triggering delayed system reboots.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-20333
CVE-2025-20362</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Loader</td><td rowspan="3">Execute Commands, System reboot</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03</td></tr>
</table>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RayInitiator	RayInitiator is a persistent, multi-stage bootkit used to deploy the LINE VIPER implant on Cisco ASA 5500-X devices that lack secure boot protections. Implemented as a modified GRUB (GRand Unified Bootloader) component, it is flashed directly onto compromised devices, allowing it to survive both reboots and firmware upgrades. Its primary role is to establish a durable foothold and install a lightweight handler within the LINA process, enabling the execution of LINE VIPER and ensuring continued control over the system.	Exploiting Vulnerabilities	CVE-2025-20333 CVE-2025-20362
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Bootkit			-
ASSOCIATED ACTOR			**PATCH LINK**
-		Deploy the LINE VIPER implant	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">TeamPCP (aka PCPcat, ShellForce, DeadCatx3, CipherForce, Persy_PCP, UNC6780)</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide (Primary focus on Iran)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Sabotage, Disruption, Financial Gains</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>CVE-2026-33634, CVE-2025-29927, CVE-2025-55182</td><td>Vect ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1059.006: Python; T1204.002: Malicious File; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1053: Scheduled Task/Job; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1611: Escape to Host; T1027: Obfuscated Files or Information; T1027.001: Binary Padding; T1027.003: Steganography; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1528: Steal Application Access Token; T1528: Steal Application Access Token T1552: Unsecured Credentials; T1552.005: Cloud Instance Metadata API; T1552.004: Private Keys; T1003: OS Credential Dumping; T1082: System Information Discovery; T1083: File and Directory Discovery; T1021: Remote Services; T1021.004: SSH; T1610: Deploy Container; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1102: Web Service; T1102.001: Dead Drop Resolver; T1572: Protocol Tunnelling; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1485: Data Destruction; T1496: Resource Hijacking; 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"> 
UNC1069 (aka BlueNorOff, APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71, Alluring Pisces, Selective Pisces, G0082, CryptoCore, CageyChameleon)</td><td>North Korea</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>WAVESHAPER.V2 (aka ZshBucket RAT), SILKBELL</td><td>Axios npm package (versions 1.14.1 and 0.30.4), Node.js environments, CI/CD pipelines</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; TA0011: Command and Control; TA006: Credential Access; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.001: PowerShell; T1059.002: AppleScript; T1059.006: Python; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1070: Indicator Removal; T1070.004: File Deletion; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1027: Obfuscated Files or Information; T1620: Reflective Code Loading; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1552: Unsecured Credentials; T1552.001: Credentials In Files</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 APT28(aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)	Russia	Government, Critical Infrastructure, Information Technology, Telecommunications, Energy, Third-party Email and Cloud Service Providers, Government, Military, Critical Infrastructure, Defense, Emergency Services, Hydrometeorology, Rail Logistics, Maritime and Transport, Humanitarian Aid Organizations	North Africa, Central America, Southeast Asia, Europe, Ukraine, United States, Turkey, Central and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2023-50224 CVE-2026-21513 CVE-2026-21509	PrismexDrop, PrismexLoader, PrismexStager, PrismexSheet	TP-Link WR841N, Windows

TTPs
TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.002: DNS Server, T1583.003: Virtual Private Server, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1586: Compromise Accounts, TA0006: Credential Access, T1528: Steal Application Access Token, T1556: Modify Authentication Process, TA0009: Collection, T1557: Adversary-in-the-Middle, TA0003: Persistence, T1584: Compromise Infrastructure T1584.008: Network Devices, TA0043: Reconnaissance, T1595: Active Scanning, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.004: DNS, TA0005: Defense Evasion, T1036: Masquerading

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
CyberAv3ngers (aka Hydro Kitten, Shahid Kaveh Group, UNC5691, Storm-0784)</td><td>Iran</td><td rowspan="3">Government, Water and Wastewater Systems (WWS), Energy</td><td rowspan="3">United States</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Sabotage and destruction</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2021-22681</td><td>-</td><td>Rockwell Automation CompactLogix PLCs, Micro850 PLCs, Rockwell Automation Studio 5000 Logix Designer, RSLogix 5000</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.007: JavaScript, TA0003: Persistence, T1133: External Remote Services, TA0011: Command and Control, T1102: Web Service, T1571: Non-Standard Port, TA0009: Collection, T1005: Data from Local System, TA0040: Impact, T1565: Data Manipulation, T1565.001: Stored Data Manipulation, T1489: Service Stop</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UAT-10362</td><td>-</td><td rowspan="2">Non-Governmental Organizations (NGOs), Education (Universities)</td><td rowspan="2">Taiwan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>LucidRook, LucidPawn, LucidKnight</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1566: Phishing T1566.002: Spearphishing Link, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1204: User Execution, T1204.002: Malicious File, TA0003: Persistence, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1574.001: DLL, T1027: Obfuscated Files or Information, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1497: Virtualization/Sandbox Evasion, T1140: Deobfuscate/Decode Files or Information, TA0007: Discovery, T1082: System Information Discovery, T1057: Process Discovery, T1614: System Location Discovery, T1614.001: System Language Discovery, TA0009: Collection, T1560: Archive Collected Data, T1560.001: Archive via Utility, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.002: File Transfer Protocols, T1105: Ingress Tool Transfer, T1102: Web Service, TA0010: Exfiltration, T1048: Exfiltration Over Alternative Protocol, T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Handala Hack (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Void Manticore)</td><td>Iran</td><td rowspan="3">Government, Real Estate, Legal, Transportation, and Critical Infrastructure</td><td rowspan="3">Gulf Cooperation Council (GCC)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Handala</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1078: Valid Accounts, T1110: Brute Force, T1566: Phishing, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1133: External Remote Services, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1484: Domain or Tenant Policy Modification, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1003.002: Security Account Manager, T1087: Account Discovery T1087.002:Domain Account, T1021: Remote Services T1021.001: Remote Desktop Protocol, T1572: Protocol Tunneling, T1105: Ingress Tool Transfer Exfiltration, T1041: Exfiltration Over C2 Channel Impact, T1485: Data Destruction, T1561: Disk Wipe, T1561.002: Disk Structure Wipe,, T1486: Data Encrypted for Impact, T1005: Data from Local System, T1560: Archive Collected Data, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1585: Establish Accounts</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Storm-2755</td><td>Iran</td><td rowspan="3">-</td><td rowspan="3">Canada</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-2025-27152</td><td>-</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0040: Impact, T1608: Stage Capabilities, T1608.005: Link Target, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.003: Spearphishing via Service, T1189: Drive-by Compromise, T1557: Adversary-in-the-Middle, T1539: Steal Web Session Cookie, T1078: Valid Accounts, T1078.004: Cloud Accounts, T1098: Account Manipulation, T1087: Account Discovery, T1114: Email Collection, T1114.002: Remote Email Collection, T1564: Hide Artifacts, T1564.008: Email Hiding Rules, T1534: Internal Spearphishing, T1657: Financial Theft</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Scattered Spider (aka UNC3944, 0ktapus, Muddled Libra, Scatter Swine, Storm-0875, Octo Tempest, LUCR-3, Star Fraud)	Suspected UK and US	Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal	United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware

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; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShinyHunters	-	Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal	United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware

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; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
LAPSUS$ (aka DEV-0537, Strawberry Tempest, Slippy Spider)</td><td>Brazil</td><td rowspan="3">Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal</td><td rowspan="3">United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium</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-2025-31324, CVE-2025-61882, CVE-2021-35587</td><td>LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys</td><td>SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Mustang Panda (aka Bronze President, Earth Preta, Stately Taurus, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG, Twill Typhoon, Hive0154)	China	Banking and Financial Services, Government, Diplomatic, and Policy Organizations	India, South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	LOTUSLITE backdoor (v1.1)	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spear-Phishing Attachment; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1218: System Binary Proxy Execution; T1218.001: Compiled HTML File; T1204: User Execution; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1574: Hijack Execution Flow; T1574.001: DLL; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1106: Native API; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
UNC6692</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>SNOWBELT, SNOWGLAZE, SNOWBASIN</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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; TA0042: Resource Development; TA0040: Impact; T1566: Phishing; T1566.002: Spearphishing Link; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.006: Python; T1059.007: JavaScript; T1059.010: AutoHotKey & AutoIT; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1559: Inter-Process Communication; T1569: System Services; T1569.002: Service Execution; T1176: Browser Extensions; T1176.001: Browser Extensions; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1547.009: Shortcut Modification; T1068: Exploitation for Privilege Escalation; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1027.015: Compression; T1070: Indicator Removal; T1070.004: File Deletion; T1112: Modify Registry; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1140: Deobfuscate/Decode Files or Information; T1202: Indirect Command Execution; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1003.002: Security Account Manager; T1003.003: NTDS; T1110: Brute Force; T1110.001: Password Guessing; T1110.003: Password Spraying; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1016: System Network Configuration Discovery; T1018: Remote System Discovery; T1046: Network Service Discovery; T1087: Account Discovery; T1087.001: Local Account; T1007: System Service Discovery; T1012: Query Registry; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1005: Data from Local System; T1074: Data Staged; T1113: Screen Capture; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1020: Automated Exfiltration; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1090: Proxy; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1608: Stage Capabilities; T1608.002: Upload Tool; T1608.005: Link Target; T1489: Service Stop</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Tropic Trooper (aka APT23, Earth Centaur, KeyBoy, Bronze Hobart, Pirate Panda, Iron)	China	Government institutions, Military/Navy agencies, Hospitals, Banks, Transportation, High-tech, Healthcare	Taiwan, South Korea, Japan, Philippines, Hong Kong
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	EntryShell backdoor, AdaptixC2 Beacon agent, TOSHIS loader	-

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.002: Upload Tool; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1106: Native API; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1547: Boot or Logon Autostart Execution; T1547.004: Winlogon Helper DLL; T1036: Masquerading; T1036.001: Invalid Code Signature; T1036.004: Masquerade Task or Service; T1620: Reflective Code Loading; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1127: Trusted Developer Utilities Proxy Execution; T1016: System Network Configuration Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1219: Remote Access Tools; T1219.001: IDE Tunneling; T1105: Ingress Tool Transfer; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography; T1567: Exfiltration Over Web Service; T1567.001: Exfiltration to Code Repository; T1041: Exfiltration Over C2 Channel

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
UAT-4356 (aka Storm-1849)</td><td>China</td><td rowspan="3">Government, Critical Infrastructure, and Telecommunications (any organization with internet-facing Cisco ASA, FTD, or Firepower VPN web services)</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>CVE-2025-20333 CVE-2025-20362</td><td>FIRESTARTER, LINE VIPER, RayInitiator</td><td>Cisco Secure Firewall ASA and FTD Software</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0005: Defense Evasion; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0011: Command and Control; TA0002: Execution; TA0009: Collection; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1070: Indicator Removal; T1222: File and Directory Permissions Modification; T1564: Hide Artifacts; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestomp; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1055: Process Injection; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1543: Create or Modify System Process; T1078: Valid Accounts; T1546: Event Triggered Execution; T1546.004: Unix Shell Configuration Modification; T1547: Boot or Logon Autostart Execution; T1082: System Information Discovery; T1057: Process Discovery; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1219: Remote Access Software; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1070.004: File Deletion; T1059: Command and Scripting Interpreter; T1005: Data from Local System</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 APT36 (aka Transparent Tribe, ProjectM, TEMP.Lapis, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm- 0156, Opaque Draco)	Pakistan	Government, Defense, Diplomatic, Transportation, Department of Motor Vehicles (DMV), Toll Payment, Healthcare	United States, India, Vietnam, United Kingdom
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	-	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.006: Web Services; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.005: Link Target; T1566.002: Spearphishing Link; T1566.003: Spearphishing via Service; T1189: Drive-by Compromise; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1027: Obfuscated Files or Information; T1656: Impersonation; T1056: Input Capture; T1056.003: Web Portal Capture; T1185: Browser Session Hijacking; T1071: Application Layer Protocol; T1071.001: Web Protocols

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
		T1195.002: Compromise Software Supply Chain
	T1199: Trusted Relationship	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
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

Tactic	Technique	Sub-technique
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1559: Inter-Process Communication	
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.005: Device Registration
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
		T1136.003: Cloud Account
	T1176: Browser Extensions	
	T1505: Server Software Component	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
		T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.004: Winlogon Helper DLL
		T1547.009: Shortcut Modification
	T1556: Modify Authentication Process	
	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	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.005: Device Registration
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1484: Domain or Tenant Policy Modification	

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
		T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.004: Winlogon Helper DLL
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.001: Invalid Code Signature
		T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.006: Timestomp

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1127: Trusted Developer Utilities Proxy Execution	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1202: Indirect Command Execution	
	T1218: System Binary Proxy Execution	T1218.001: Compiled HTML File
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1484: Domain or Tenant Policy Modification	
	T1497: Virtualization/Sandbox Evasion	
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
		T1553.006: Code Signing Policy Modification
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
		T1562.009: Safe Mode Boot

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.008: Email Hiding Rules
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1578: Modify Cloud Compute Infrastructure	T1578.005 : Modify Cloud Compute Configurations
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
		T1003.003: NTDS
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1110: Brute Force	T1110.001: Password Guessing
		T1110.003: Password Spraying
	T1111: Multi-Factor Authentication Interception	
	T1212: Exploitation for Credential Access	
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.007: Container API
	T1555: Credentials from Password Stores	T1555.006: Cloud Secrets Management Stores
	T1556: Modify Authentication Process	
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1007: System Service Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
	T1135: Network Share Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1526: Cloud Service Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
		T1021.006: Windows Remote Management
	T1072: Software Deployment Tools	
	T1080: Taint Shared Content	
	T1210: Exploitation of Remote Services	
	T1534: Internal Spearphishing	
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1563: Remote Service Session Hijacking	
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.002: Remote Data Staging

Tactic	Technique	Sub-technique
TA0009: Collection	T1113: Screen Capture	
	T1114: Email Collection	T1114.002: Remote Email Collection
	T1119: Automated Collection	
	T1125: Video Capture	
	T1185: Browser Session Hijacking	
	T1213: Data from Information Repositories	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository
		T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication

Tactic	Technique	Sub-technique
TA0011: Command and Control	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
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1498: Network Denial of Service	T1498.001: Direct Network Flood
	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
	T1531: Account Access Removal	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe
		T1561.002: Disk Structure Wipe
	T1565: Data Manipulation	T1565.001: Stored Data Manipulation
		T1565.002: Transmitted Data Manipulation

Tactic	Technique	Sub-technique
TA0040: Impact	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.002: DNS Server
		T1583.001: Domains
		T1583.006: Web Services
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1585: Establish Accounts	
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.001: Malware
		T1588.002: Tool
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.002: Upload Tool
		T1608.005: Link Target
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1590: Gather Victim Network Information	T1590.002: DNS
	T1595: Active Scanning	
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1598.004: Spearphishing Voice

Top 5 Takeaways

#1 In April 2026, **16 zero-day vulnerabilities** surfaced. These zero-days were found across products from **Microsoft Office, Oracle E-Business Suite, Google Chrome, FortiOS, Meta, and Cisco.**

#2 Newly identified malware active in April included a broad mix of **Backdoors, RAT, and Loaders**. Key discoveries were **Vect ransomware, Havoc, SNOWBELT, The Gentlemen, SILKBELL**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

#3 Cyberattacks concentrated heavily on **United States, Spain, Italy, Germany, and United Kingdom**, which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4 **Government, Energy, Financial, Transportation, and Healthcare** sectors absorbed the bulk of targeted activity, with ransomware operations, data theft, and espionage campaigns driving operational disruption. Attackers continued refining techniques and expanding pressure across these industries.

#5 Activity during the period was dominated by **TeamPCP, Handala Hack Team, Scattered LAPSUS$ Hunters(SLH) , and APT28**, all well-resourced groups known for sustained, high-impact operations. Their campaigns shaped a threat landscape defined by disciplined tradecraft, rapid exploitation cycles, and a clear focus on high-value targets across public and private sectors.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **34 significant vulnerabilities** and block the indicators related to the **15 active threat actors, 36 active malware,** and **225 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 **34 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
WAVESHAPER.V2	SHA256	92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a, 617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101, ed8560c1ac7ceb6983ba995124d5917dc1a00288912387a6389296637d5f815c, fcb81618bb15edfdedfb638b4c08a2af9cac9ecfa551af135a8402bf980375cf
SILKBELL	SHA256	e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09
Havoc	MD5	248a4d7d4c48478dcbeade8f7dba80b3
	IPv4	43[.]134[.]90[.]60, 43[.]134[.]52[.]221, 47[.]237[.]15[.]197
PrismexDrop	SHA256	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae
PrismexLoader	SHA256	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9
PrismexStager	SHA256	57357655a62e3a8b1f4b78e1d3ed7e0f6d59a9bac213087294f91bb7847b2a8f
LucidRook	SHA256	11ae897d79548b6b44da75f7ab335a0585f47886ce22b371f6d340968dbed9ae

Attack Name	TYPE	VALUE
LucidRook	SHA256	edb25fed9df8e9a517188f609b9d1a030682c701c01c0d1b5ce79cba9f7ac809, 0305e89110744077d8db8618827351a03bce5b11ef5815a72c64eea009304a34
LucidPawn	SHA256	6aba7b5a9b4f7ad4203f26f3fb539911369aeef502d43af23aa3646d91280ad9, bdc5417ffba758b6d0a359b252ba047b59aacf1d217a8b664554256b5adb071d, d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964
LucidKnight	SHA256	d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964, aa7a3e8b59b5495f6eebc19f0654b93bb01fd2fa2932458179a8ae85fb4b8ec1
Masjesu	SHA256	f39b67fff1f106fb1b4fa9beb386427c8e7eb010f306ad0445da70bffc855f2e, dfd830368724f6abcc542bc8b85e3d5fa2aedf8282d3805d0d6d53f45c7e0937, de5fb68023465cb5d8ace412e11032d98a41bd6af2a83245c046020530130496, d8018e31b77b135ed300a988757f409347d013b76f9c9a4972e48cb715f45967, cb4a3665ebd12bdb094b9fc188793c67ec3008363a49b1dde00d488b54df984b, b53d4781bbadb17014da280e274e11f2de9063a35f2eabd32d4596707b147306, 4190491b9006404cab256d66125bd77b1c3a0e63451fbb3d829617d7e87acc9b, 85758df12964024af3ae829e3630f9ad5de7c55dae00181198033da8816e3293

Attack Name	TYPE	VALUE
Masjesu	SHA256	8340ff8920412a70f0c29cdf72f6f218e61142b3f210e70e24811c413971a8ed, 620f6949b82f9ef987b7511fbbb09c2da57d8be47b019fa6a9686ce08b4c3e70, 87f11a3ee2486bc4845a28465c2e70d2d9f98725edf4a73c3359c23a43ed74b7, 9c683b0be86d4cd274a7a16073bdf092218f259b055a72f848d589574e9b8084, 8ce9145fee0d3d2444554d901b334c36e71bb1346280ada7ff366cf9d25c5938
Handala Wiper	MD5	5986ab04dd6b3d259935249741d3eff2
	SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
Payouts King	SHA256	335ad12a950f885073acdfebb250c93fb28ca3f374bbba5189986d9234dcbff4, d68ce82e82801cd487f9cd2d24f7b30e353cafd0704dcdf0bb8f12822d4227c2
PHANTOMPULSE	SHA256	33dacf9f854f636216e5062ca252df8e5bed652efd78b86512f5b868b11ee70f
	Domain	panel[.]fefea22134[.]net
PHANTOMPULL	SHA256	70bbb38b70fd836d66e8166ec27be9aa8535b3876596fc80c45e3de4ce327980
LummaC2	SHA256	82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b
StealC	SHA256	dc5fc48cbd764acf7dd28c385279cf8b4296fb2d1e7b9aca3bc2352893194c94

Attack Name	TYPE	VALUE
StealC	SHA256	4630f2e42c67690b34c187feee43eabe447c935dea079b5bf1c480de070d097c, 5dda23dea89feea09086361d99a9dc1c04f1a2e552a2f5f52cb83d2d8e4e11f8, 9bc696c7c68c2c31cd431ed0af9264fe056942923399b1adb4c55241639bc835, a5f2f3c199df73e31969d96acc46694759792ba294c6311d37bb7b72f5e54fde
Vidar	SHA256	1e92acabf037a60e7fbb97c0ba73e997bb4b602ad51333871423b778cae4f0b1, 0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612
RedLine	SHA256	7ac90091d7037384ca3dc9a7a0459e3875e976496b3afd9a6a81ad6ace0ba002, a1d9659e8f9df7dbcfebec0faafadeec8b43e0e5d0818aab0d63d0815490bce5, 90522e6a880f6a97719035e3945da1c0c0384f154cf631732ea16a3a9f827b7c, 69587ec2c3e810dc6fca35c13341907fe7a96a24a4222589b72ef97b80e820f4, c1354dcaa9389550c2013e23418bb5c71474b6c368f8e68e51e31faa64ba4ea1
Meduza	SHA256	9e2b8c3888b8a93e8ebab39e7a6b636f921888edb7d15a6ab56b2e119693aaa8
Rhadamanthys	SHA256	5db892a52fbebbf0298d3b5b2cf0c3ed7f9612a9d337c56bb168be336d28cadb, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	b1c5d2eadbb2936f8b9644a5a4e24b5c54b163f0f2d6817c60edb3e5a73c6dc6, 0e94e5712d93d43423f3fec2f3a7f2b859d749411034c839c13e428f651f11a6, 3b9d0e62c06caeaf4244ff2fb275a1919fd9e14243fb436dce313c8d9b89faa4
Nexcorium	SHA256	37132e804ccb3fc4ba1f72205da70c3d7a6e66b43178707a9d8ee1156d815c21, e4789416c35b345e75c023a8c07c207c79937c6a5444e1c29d85d18d2f660d8c, 0b510f93f47590791626d2fa74ddd62ba6eb8a5a5bb7b8476c0ceffc7be94ebe, 9b805585c457811d2c5c5664ede9ee869b53e3c9999100505d7ee8de7f855fdf, 95d1eb12d58206319c514c7240d058c512bb22b31f6ea22ed8be3ae44305c9f7, 7c01d5b53861cd34e10a79fdea16dcf08bce9c78ed72abd6d6f3e9ce75a24734, 838e35b62a6b38675e467301166cdcc54f98d528fe43d56936caeffec88ac696, 2ccf23b8165e8c05899aa7ba4755b896ebf1d20d3b701cffdc768482486b0a74, 29404df12a7723ce46c8b199c88a808aa315dd8ff8fd1e06a34ccd3d16f4553b, b1274de00a7f3d7ab9792ec3456e9d5bf057738666f34183f1d72060e2d4f678, 721c7cb2109ec97c14413cb8b58ddce0ecf0c1f13f22ee4f72eed79b57592cf5, 89dae116c77b0035277d39dfe01043624427c119ddee8883a3ba54a42a6ae400
Lotus Wiper	MD5	0b83ce69d16f5ecd00f4642deb3c5895, c6d0f67db6a7dbf1f9394d98c1e13670, b41d0cd22d5b3e3bdb795f81421a11cb
	SHA256	405177294F6F9268432A43998049AD0D4A61C6909216533B8713C911BC430755

Attack Name	TYPE	VALUE
Lotus Wiper	SHA256	9D05854C95C6AFA68911BD28AF12282185E0FE34F2E58FDDBC503AB22D1508D7, 1D6F374087087738B7699EBF91F1CFDB3B2A65C2E9BE72E106EE7C9814BE3274
LOTUSLITE	SHA256	856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216
SNOWBELT	SHA256	7f1d71e1e079f3244a69205588d504ed830d4c473747bb1b5c520634cc5a2477, ca390b86793922555c84abc3b34406da2899382c617f9dcf83a74ac09dd18190, 6e6dab993f99505646051d2772701e3c4740096ff9be63c92713bcb7fcddf9f7, de200b79ad2bd9db37baeba5e4d183498d450494c71c8929433681e848c3807f
	URL	cloudfront-021[.]s3[.]us-west-2[.]amazonaws[.]com
SNOWGLAZE	SHA256	2fa987b9ed6ec6d09c7451abd994249dfaba1c5a7da1c22b8407c461e62f7e49
	URL	wss[:]//sad4w7h913-b4a57f9c36eb[.]herokuapp[.]com/ws
SNOWBASIN	SHA256	c8940de8cb917abe158a826a1d08f1083af517351d01642e6c7f324d0bba1eb8
EntryShell	IPv4	158[.]247[.]193[.]100
AdaptixC2 Beacon agent	SHA256	aeec65bac035789073b567753284b64ce0b95bbae62cf79e1479714238af0eb7, 7a95ce0b5f201d9880a6844a1db69aac7d1a0bf1c88f85989264caf6c82c6001
TOSHIS loader	SHA256	47c7ce0e3816647b23bb180725c7233e505f61c35e7776d47fd448009e887857
The Gentlemen	SHA256	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a

Attack Name	TYPE	VALUE
The Gentlemen	SHA256	22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67, 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d, 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235, 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd, 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8, 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923, 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c, 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db, 91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1, 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3, 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454, a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad, c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8, c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73, ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2

Attack Name	TYPE	VALUE
The Gentlemen	SHA256	efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f, f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12, fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958, 5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca, 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19, 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c
SystemBC	SHA256	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5
LINE VIPER	SHA256	bd82a15394f80c6eb82e439dcec93eb8535e9bbc9b26e991fef8bd92c5ba345f, e6684678ace298f81aedd140415c74553612bf86b904c11ca059424ef8322e7c, 8dab6e20cfa9ec1445eb32d3ec836e3c17b97cee622caa1b7e6b110b44df769a, 531b619e8b27cfad4628c9539f2707903d129411bd908a0d6f862e382d7ac5a4, 5bf3100c49718b7567acfc5d84606dc010b91e10cedd25aef13e27f0ffc0f997, 27ed8628441ddc88bba8aba5783665b096975d948db92cb8ffc7790ddfa68414, 3a9486da872af184ba250059311f1ee70f46f84b6d92dcdfa4f0396eb83ffb6a, 0bdb8efb72c6566be86963ffb2ec5a135362e18e5e8c6afd3e42b3a761b85428, 0297f9852a70b04cdf2aaf5d66611451d1bde918e8e59ebe8e573e5a0b449af0, 1a4a37df0a6b5ad02b7e91ccbc7c706079761a4e85bebaa09533c3017c9aff71
VECT Ransomware (VECT 2.0)	SHA256	a7eadcf81dd6fda0dd6affefaffcb33b1d8f64ddec6e5a1772d028ef2a7da0f2

Attack Name	TYPE	VALUE
VECT Ransomware (VECT 2.0)	SHA256	58e17dd61d4d55fa77c7f2dd28dd51875b0ce900c1e43b368b349e65f27d6fdd, e1fc59c7ece6e9a7fb262fc8529e3c4905503a1ca44630f9724b2ccc518d0c06, 8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d, 9c745f95a09b37bc0486bf0f92aad4a3d5548a939c086b93d6235d34648e683f, e512d22d2bd989f35ebaccb63615434870dc0642b0f60e6d4bda0bb89adee27a, 8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d
	IPv4	158[.]94[.]210[.]11

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 Demo of **HivePro**.

REPORT GENERATED ON

May 5, 2026 • 11:40 PM

More at www.hivepro.com