Date of Publication
January 2, 2026

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

DECEMBER 2025

Table Of Contents

Summary..... 03

Insights..... 04

Threat Landscape..... 05

Celebrity Vulnerabilities 06

Vulnerabilities Summary..... 09

Attacks Summary..... 11

Adversaries Summary..... 15

Targeted Products..... 17

Targeted Countries..... 20

Targeted Industries..... 21

Top MITRE ATT&CK TTPs..... 22

Top Indicators of Compromise (IOCs)..... 23

Vulnerabilities Exploited..... 26

Attacks Executed..... 40

Adversaries in Action..... 61

MITRE ATT&CK TTPS..... 78

Top 5 Takeaways..... 84

Recommendations..... 85

Appendix..... 86

Indicators of Compromise (IoCs)..... 87

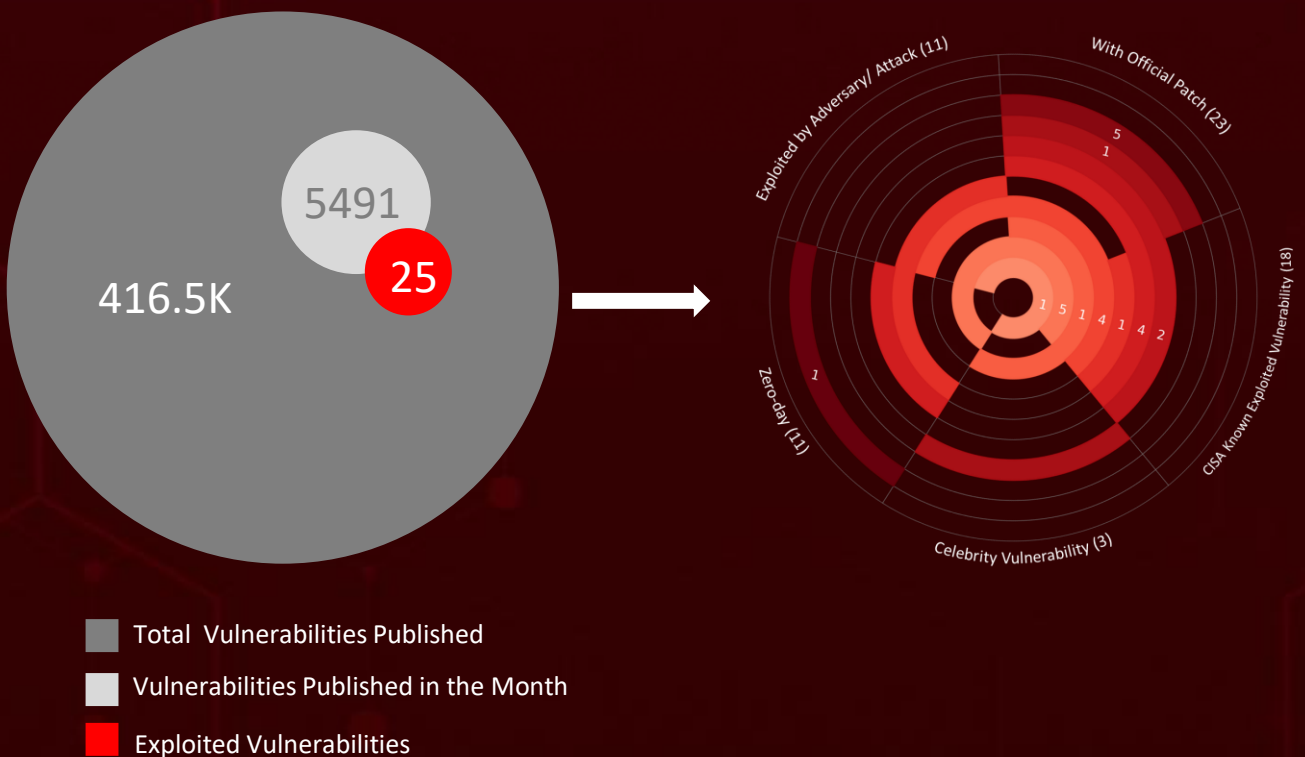
What Next?..... 109

Summary

December emerged as a particularly volatile period for cybersecurity, underscored by the disclosure of three high-profile "celebrity" vulnerabilities, **React2Shell**, **MongoBleed**, and **LangGrinch**, alongside eleven zero-day flaws. Chief among them was **CVE-2025-55182**, widely known as React2Shell, a critical unauthenticated remote code execution vulnerability rooted in unsafe deserialization within React Server Components' Flight protocol. The flaw was weaponized within days of disclosure, with multiple threat actors leveraging it to deploy cryptominers, web shells, and persistent backdoors. The month also saw Google issue an emergency Chrome update, patching three vulnerabilities, including the actively exploited zero-day **CVE-2025-14174** in the ANGLE graphics engine.

At the same time, attackers aggressively exploited weaknesses across widely deployed enterprise infrastructure. Two critical Fortinet flaws, **CVE-2025-59718** and **CVE-2025-59719**, enabled unauthenticated bypass of FortiCloud SSO authentication through crafted SAML responses, placing exposed environments at immediate risk. Cisco was also forced to confront a severe zero-day, **CVE-2025-20393**, affecting AsyncOS in Cisco Secure Email Gateway and Secure Email and Web Manager appliances. Exploitation has been ongoing since late November 2025 and has been attributed to the China-linked APT group **UAT-9686**, which deployed advanced persistence malware to maintain long-term access.

Beyond vulnerabilities, December highlighted a surge in mature and stealth-driven threat actor campaigns. Iran-aligned **MuddyWater** resurfaced with a refined cyberespionage operation targeting Israel and Egypt, using spear-phishing lures that directed victims to legitimate file-sharing services to deliver trojanized RMM installers and new tooling such as the Fooder loader and MuddyViper backdoor. In parallel, Russia-origin **Operation MoneyMount-ISO** continued to spread Phantom infostealer via multi-stage phishing chains abusing ISO files. **Silver Fox's** impersonation of India's Income Tax Department to deploy **ValleyRAT** further illustrated how trusted platforms and institutions are being weaponized at scale. Collectively, these developments reinforce a stark reality: the threat landscape is becoming faster, stealthier, demanding sustained vigilance and rapid defensive action from organizations worldwide.



Insights

In December 2025, a geopolitical cybersecurity landscape unfolds, revealing **India, Turkey,** and **Israel** as the top-targeted countries.

Highlighted in **December 2025** is a cyber battleground encompassing the **Technology, Finance, Government, Transportation,** and **Manufacturing** sectors, designating them as the top industries.

CVE-2025-55182 (React2Shell) turned a core React feature into a one-request server takeover, enabling near-instant compromise of internet-exposed applications at massive scale.

CVE-2025-14847 (MongoBleed) quietly leaks the most sensitive secrets from MongoDB memory, exposing credentials and keys at scale as hundreds of thousands of internet-facing databases remain vulnerable and actively exploited.

CVE-2025-68664 (LangGrinch) turns trusted AI outputs into an attack surface, allowing malicious inputs to trigger secret theft and potential code execution across millions of LangChain-powered applications.

Silver Fox turns fake tax notices into a silent entry point, using ValleyRAT to slip deep into Indian networks under the guise of official trust.

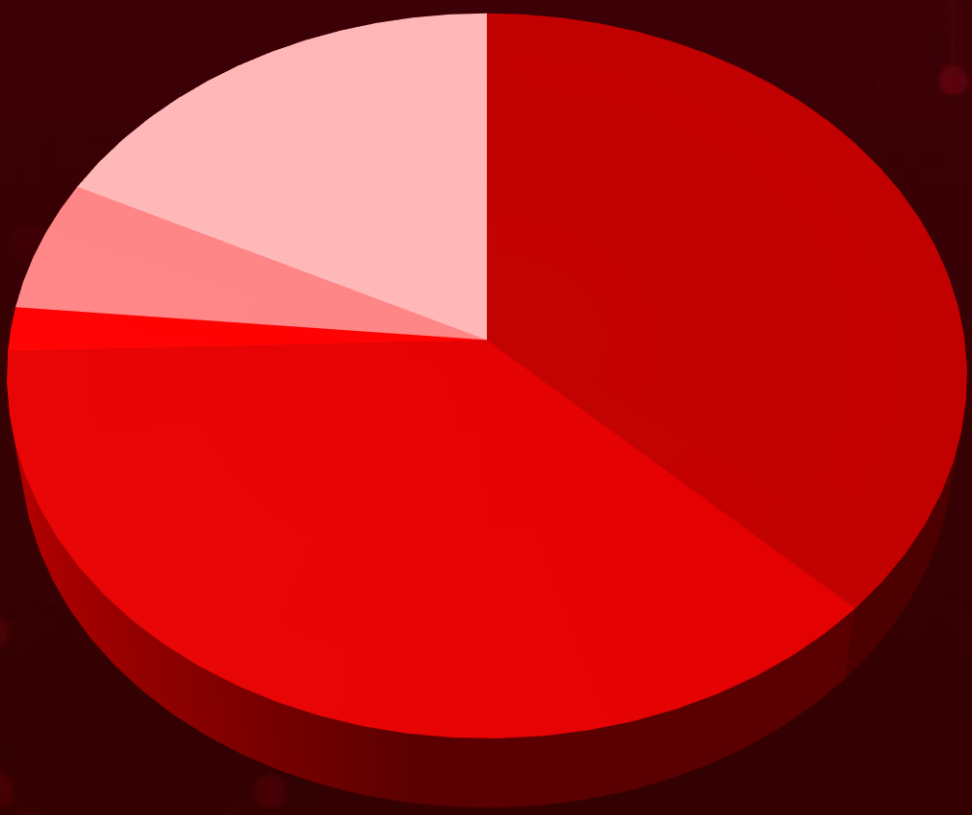
BRICKSTORM gives China-linked operators a quiet, persistent grip on U.S. VMware vCenter environments, turning critical infrastructure into long-term espionage footholds.

By exploiting Ivanti zero-days **CVE-2024-21893** and **CVE-2024-21887**, a China-linked threat group silently breached Japanese shipping networks, escalating from initial access to credential theft and the deployment of advanced **PlugX**-based backdoors.

Water Saci weaponizes everyday WhatsApp messages, using malicious files and layered loaders to quietly install a banking backdoor on unsuspecting victims' systems.

Operation Hanoi Thief masks itself as a routine hiring workflow, using fake resumes and GitHub profiles to silently slip the LOTUSHARVEST malware into Vietnamese IT environments.

Threat Landscape



Celebrity Vulnerabilities

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2025-55182</td><td>✗</td><td rowspan="2">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</td><td rowspan="2">Earth Lamia, Jackpot Panda and UNC5174, UNC6600, UNC6588, UNC6603, UNC6595, UNC5342</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="3">✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td rowspan="2">cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:* cpe:2.3:a:remix:react_router:*:*:*</td><td rowspan="2">XMRig, Sliver, PeerBlight and EtherRAT, Snowlight, Vshell, Noodle RAT, KSwapDoor, Auto-color, Minocat, Compood, and Hisonic</td></tr>
<tr><td rowspan="2">React2Shell (Meta React Server Components Remote Code Execution Vulnerability)</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter</td><td>https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-14847</td><td>✗</td><td rowspan="2">MongoDB 8.2.0 through 8.2.2
MongoDB 8.0.0 through 8.0.16
MongoDB 7.0.0 through 7.0.27
MongoDB 6.0.0 through 6.0.26
MongoDB 5.0.0 through 5.0.31
MongoDB 4.4.0 through 4.4.29
All MongoDB Server v4.2 versions
All MongoDB Server v4.0 versions
All MongoDB Server v3.6 versions</td><td rowspan="2">-</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td rowspan="3">cpe:2.3:a:mongodb:mongodb:*:*:*:*:*:*:*:*</td><td rowspan="3">-</td></tr>
<tr><td rowspan="3">MongoBleed (MongoDB Server Heap Memory Leak Vulnerability)</td><td>CWE ID</td></tr>
<tr><td>CWE-130</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials, T1082: System Information Discovery</td><td>https://www.mongodb.com/try/download/community, https://jira.mongodb.org/browse/SERVER-115508, https://www.mongodb.com/community/forums/t/important-mongodb-patch-available/332977</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-68664</td><td>✗</td><td rowspan="2">Langchain-core versions before: 0.3.81 and 1.2.5</td><td rowspan="2">-</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td rowspan="3">cpe:2.3:a:langchain-ai:langchain:*:*:*:*:*:*:*:*</td><td rowspan="3">-</td></tr>
<tr><td rowspan="2">LangGrinch (LangChain Serialization Injection Vulnerability)</td><td>CWE ID</td></tr>
<tr><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1059.006: Python, T1082: System Information Discovery, T1588.007: Artificial Intelligence</td><td>https://github.com/langchain-ai/langchain/releases</td></tr>
</table>

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-8489	WordPress King Addons for Elementor Plugin Privilege Escalation Vulnerability	WordPress King Addons for Elementor Plugin	✗	✗	✓
CVE-2025-55182	Meta React Server Components Remote Code Execution Vulnerability	Meta React Server Components	✗	✓	✓
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Policy Secure, and Neurons	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2025-62221	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	✓	✓	✓
CVE-2025-54100	PowerShell Remote Code Execution Vulnerability	Windows Server	✗	✗	✓
CVE-2025-64671	GitHub Copilot for Jetbrains Remote Code Execution Vulnerability	GitHub Copilot Plugin for JetBrains IDEs	✗	✗	✓
CVE-2025-14174	Google Chromium Out of Bounds Memory Access Vulnerability	Google Chrome, Apple Multiple Products	✓	✓	✓
CVE-2025-8110	Gogs Symlink Bypass Remote Code Execution Vulnerability	Gogs	✓	✗	✗
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-38812	VMware vCenter Server Heap-Overflow Vulnerability	VMware vCenter Server	✗	✓	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✗	✓	✓
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-22005	VMware vCenter Server File Upload Vulnerability	VMware vCenter Server	✗	✓	✓
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	WinRAR	✓	✓	✓
CVE-2025-6218	RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	WinRAR	✗	✓	✓
CVE-2025-43529	Apple Multiple Products Use-After-Free WebKit Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2025-59718	Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	Fortinet Multiple Products	✗	✓	✓
CVE-2025-59719	Fortinet FortiCloud SSO Login Authentication Bypass	Fortinet Fortiweb	✗	✗	✓
CVE-2025-40602	SonicWall SMA1000 Missing Authorization Vulnerability	SonicWall SMA1000	✗	✓	✓
CVE-2025-23006	SonicWall SMA1000 Appliances Deserialization Vulnerability	SonicWall SMA1000	✓	✓	✓
CVE-2025-20393	Cisco Multiple Products Improper Input Validation Vulnerability	Cisco Multiple Products	✓	✓	✗
CVE-2025-68613	n8n Remote Code Execution via Expression Injection Vulnerability	n8n	✗	✗	✓
CVE-2025-14847	MongoBleed (MongoDB Server Heap Memory Leak Vulnerability)	MongoDB Server	✗	✓	✓
CVE-2025-68664	LangGrinch (LangChain Serialization Injection Vulnerability)	LangChain	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LOTUSHARVEST	Information Stealer	-	-	-	Phishing
Fooder	Loader	-	-	-	Phishing
MuddyViper	Backdoor	-	-	-	Phishing
CE-Notes	Browser-data Stealer	-	-	-	Phishing
LP-Notes	Credential Stealer	-	-	-	Phishing
Blub	Browser-data Stealer	-	-	-	Phishing
go-socks5	Tool	-	-	-	Phishing
SORVEPOTEL	Hybrid Malware	-	-	-	Spear-phishing via WhatsApp
Arkanix	Stealer	-	-	-	Circulated through Discord and underground forums
ValleyRAT	RAT	-	-	-	Social Engineering, Phishing
XMRig	Miner	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Sliver	Dropper	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
PeerBlight	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
EtherRAT	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
UDPGangster	Backdoor	-	Microsoft Windows	-	Phishing
MetaRAT	RAT	CVE-2024-21893 CVE-2024-21887	Ivanti Connect Secure	✓	Exploiting Vulnerabilities
Talisman PlugX	RAT	CVE-2024-21893 CVE-2024-21887	Ivanti Connect Secure	✓	Exploiting Vulnerabilities
BRICKSTORM	Backdoor	CVE-2023-46805 CVE-2024-21887	Ivanti, VMware, F5 BIG-IP, VMware vCenter	✓	Exploiting vulnerabilities
Pteranodon	Loader	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting vulnerabilities
GamaWiper	Wiper	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting vulnerabilities
Snowlight	Loader	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Vshell	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Noodle RAT	RAT	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
KSwapDoor	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Auto-color	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Minocat	Tool	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Compood	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Hisonic	Backdoor	CVE-2025-55182	Meta React Server Components	✓	Exploiting Vulnerability
Phantom	Stealer	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SantaStealer	Infostealer	-	-	-	-
AquaShell	Backdoor	CVE-2025-20393	Cisco AsyncOS Software (physical and virtual appliances)	⊗	Exploiting Vulnerability
AquaTunnel	Tool	CVE-2025-20393	Cisco AsyncOS Software (physical and virtual appliances)	⊗	Exploiting Vulnerability
AquaPurge	Tool	CVE-2025-20393	Cisco AsyncOS Software (physical and virtual appliances)	⊗	Exploiting Vulnerability
Chisel	Tool	CVE-2025-20393	Cisco AsyncOS Software (physical and virtual appliances)	⊗	Exploiting Vulnerability
GhostPoster	Malicious browser extension–based	-	-	-	Social Engineering
GachiLoader	Loader	-	-	-	Phishing
Kidkadi	Dropper	-	-	-	Phishing
Rhadamanthys	Infostealer	-	-	-	Phishing
Foudre	Downloader	-	-	-	Phishing
Tonnerre	Stealer	-	-	-	Phishing
MacSync	Stealer	-	-	-	Social Engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
MgBot	Backdoor	-	-	-	-
Donut	Loader	-	-	-	Phishing

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
MuddyWater	Information theft and espionage	Iran	-	Fooder loader, MuddyViper, CE-Notes, LP-Notes, Blub, go-socks5, UDPGangster	Microsoft Windows
ShadyPanda	Information theft, Financial gain, and Espionage	China	-	-	Chrome, Edge
Earth Lamia	Information theft and espionage	China	CVE-2025-55182	-	Meta React Server Components
Jackpot Panda	Information theft and espionage	China	CVE-2025-55182	-	Meta React Server Components
UNC5174	Financial gain, Espionage	China	CVE-2025-55182	-	Meta React Server Components
WARP PANDA	Espionage, Information Theft	China	CVE-2024-21887 CVE-2023-46805 CVE-2024-38812 CVE-2023-46747 CVE-2023-34048 CVE-2021-22005	BRICKSTORM	Ivanti Connect Secure and Policy, VMware, F5 BIG-IP
Gamaredon	Information theft and espionage	Russia	CVE-2025-8088	Pteranodon, GamaWiper	RARLAB WinRAR
APT-C-08	Information theft and espionage	-	CVE-2025-6218	-	RARLAB WinRAR
UNC6600	Information Theft and Espionage	China	CVE-2025-55182	MINOCAT	Meta React Server Components

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNC6588	Information Theft and Espionage	-	CVE-2025-55182	COMPOOD	Meta React Server Components
UNC6603	Information Theft and Espionage	China	CVE-2025-55182	HISONIC	Meta React Server Components
UNC6595	Information Theft and Espionage	China	CVE-2025-55182	ANGRYREBEL.LINUX	Meta React Server Components
UNC5342	Information Theft and Espionage	Korea	CVE-2025-55182	-	Meta React Server Components
UAT-9686	Information Theft and Espionage	China	CVE-2025-20393	AquaShell, AquaTunnel, AquaPurge, and Chisel	Cisco Secure Email Gateway (SEG) & Cisco Secure Email and Web Manager (SEWM)
Prince of Persia	Information theft and espionage	Iran	-	Foudre, Tonnerre	-
Evasive Panda	Information Theft and Espionage	China	-	MgBot	-
Silver Fox	Information Theft and Espionage	China	-	Donut loader, Valley RAT	-

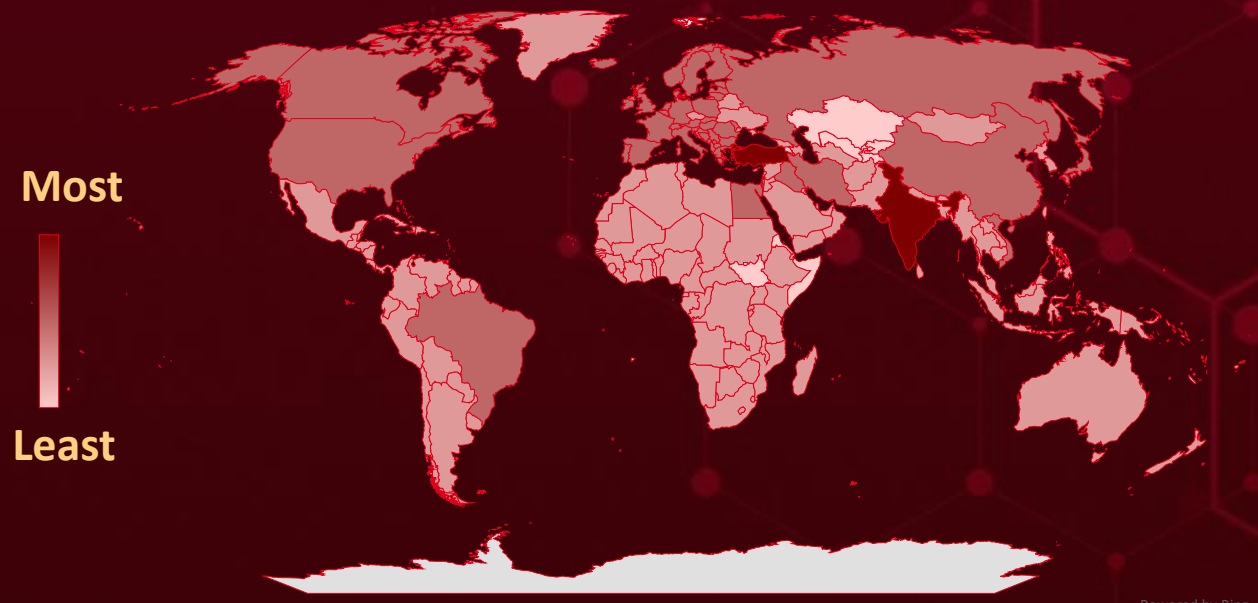
Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Plugin	WordPress King Addons for Elementor Plugin Versions 24.12.92 to 51.1.14
	Web application framework	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
ivanti	Virtual Private Network (VPN) and Secure Remote Access appliance, Network Access Control (NAC) appliance	Ivanti Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x, Ivanti Connect Secure and Policy Secure
Microsoft	Operating System	Windows Server 2022, 2025; Windows 11 Version 25H2; Windows 10 Version 1809, Windows Server 2025, 2012, 2008, 2016; Windows 10 Version 1607
	Developer productivity tool	GitHub Copilot Plugin for JetBrains IDEs
	Browser	iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Self-hosted Git repository management software	Gogs (Prior to 0.13.4, all versions through 0.13.3)
	Virtualization management platform, Hybrid cloud infrastructure platform	VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x, VMware vCenter Server: 6.7- 7.0.0
	Web-based management interface	F5 BIG-IP Configuration Utility
	File compression and archiving utility	WinRAR versions before 7.13, WinRAR Version Prior to 7.12
	Web browser	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac), iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80
	Network security operating system, Secure web gateway, Network switch management platform, Web Application Firewall (WAF)	Fortinet Fortios Before 7.0.18, Before 7.2.12, Before 7.4.9, Before 7.6.4; Fortinet Fortiproxy Before 7.0.22, Before 7.2.15, Before 7.4.11, Before 7.6.4; Fortinet FortiSwitchManager Before 7.0.6, Before 7.2.7, Fortinet FortiWeb Before 7.4.10, Before 7.6.5, Before 8.0.1
	Secure Remote Access	SonicWall SMA1000 12.4.3-03093 (platform- hotfix) and earlier versions, 12.5.0-02002 (platform-hotfix) and earlier versions

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
SONICWALL	Secure Remote Access	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and Earlier
CISCO	Email security gateway, Web Manager	Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM): All Cisco AsyncOS versions (physical and virtual appliances)
	Workflow automation and integration platform	n8n all versions starting with 0.211.0 and prior to 1.120.4
MongoDB	Database platform	MongoDB 8.2.0 through 8.2.2 MongoDB 8.0.0 through 8.0.16 MongoDB 7.0.0 through 7.0.27 MongoDB 6.0.0 through 6.0.26 MongoDB 5.0.0 through 5.0.31 MongoDB 4.4.0 through 4.4.29 All MongoDB Server v4.2 versions All MongoDB Server v4.0 versions All MongoDB Server v3.6 versions
	AI/ML development framework	Langchain-core versions before: 0.3.81 and 1.2.5, Langchain-core versions before: 0.3.80 and 1.1.8, and Langchain versions before: 0.3.37 and 1.2.3

Targeted Countries



Color	Countries
	India
	Turkey
	Israel
	North Macedonia
	Liechtenstein
	Serbia
	Bosnia and Herzegovina
	Moldova
	Brazil
	Republic of Ireland
	Bulgaria
	Austria
	Canada
	Luxembourg
	China
	Montenegro
	Croatia
	Poland
	Denmark
	Russia
	Egypt

Color	Countries
	Belgium
	Estonia
	Vietnam
	Finland
	Lithuania
	France
	Malta
	Germany
	Monaco
	Greece
	Netherlands
	Hungary
	Norway
	Iceland
	Portugal
	Albania
	Romania
	Iran
	San Marino
	Iraq
	Slovakia

Color	Countries
	Slovenia
	Spain
	Sweden
	Switzerland
	United Kingdom
	Italy
	United States
	Japan
	Kosovo
	Latvia
	Singapore
	Northern Ireland
	Uruguay
	Democratic Republic of Congo
	Central African Republic
	Aruba
	Tibet
	Djibouti
	Burundi
	Dominica
	Peru

Color	Countries
	Australia
	Turkmenistan
	El Salvador
	Namibia
	Equatorial Guinea
	Nigeria
	Akrotiri and Dhekelia
	Palestine
	Ethiopia
	Puerto Rico
	Faroe Islands
	Saint Kitts and Nevis
	Fiji
	Senegal
	Azerbaijan
	South Korea
	Bahamas
	Syria
	French Guiana
	Tonga
	Gabon

Color	Countries
	United Arab Emirates
	Georgia
	Yemen
	Bahrain
	Nepal
	Ghana
	Nicaragua
	Gibraltar
	Cambodia
	Bangladesh
	Oman
	Greenland
	Papua New Guinea
	Grenada
	Anguilla
	Guadeloupe
	Cape Verde
	Guam
	Saba
	Guatemala
	Saint Maarten

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1071** Application Layer Protocol	**T1027** Obfuscated Files or Information	**T1071.001** Web Protocols	**T1588** Obtain Capabilities
T1082 System Information Discovery	**T1036** Masquerading	**T1190** Exploit Public-Facing Application	**T1041** Exfiltration Over C2 Channel	**T1005** Data from Local System
T1204 User Execution	**T1140** Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1566** Phishing	**T1588.006** Vulnerabilities
T1574 Hijack Execution Flow	**T1070** Indicator Removal	**T1056** Input Capture	**T1573** Encrypted Channel	**T1547** Boot or Logon Autostart Execution
T1204.002 Malicious File	**T1083** File and Directory Discovery	**T1068** Exploitation for Privilege Escalation	**T1547.001** Registry Run Keys / Startup Folder	**T1497** Virtualization /Sandbox Evasion

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LOTUSHARVEST	SHA256	48e18db10bf9fa0033affaed849f053bd20c59b32b71855d1cc72f613d0cac4b
Fooder	SHA1	76632910CF67697BF5D7285FAE38BFCF438EC082,
CE-Notes	SHA1	8E21DE54638A79D8489C59D958B23FE22E90944A, CD47420F5CE408D95C98306D78B977CDA0400C8F, C1299E8C9A8567A9C292157F3ED65B818AA78900
LP-Notes	SHA1	29CDA06701F9A9C0A6791775C3EB70F5B52BBEFF, 8F3ED626E7B929450E36E97BA5539C8371DF0EF8
Blub	SHA1	1723D5EA7185D2E339FA9529D245DAA5D5C9A932, 69B097D8A3205605506E6C1CC3C13B71091CB519, B7A8F09CB5FF8A33653988FFBA585118ACF24C13, B8997526E4781A6A1479690E30072F38E091899D
go-socks5	SHA1	25361183DE63F296BA71B6FCF0725E022B3C989A, 0E9A4892CFA1C9065B36D8F2E164E28609A8CF5D, 2B09241CA025BDC4455E9F6BA6009E2F27C08EDF, 2E9BE23CDD8152DB6CD1A54E001C4EA82FF6F1C6, 45FA7DE711FEA1F8D1E348E87834246C455DD2ED, 4E0EF2386980639FC5355FD68DAFF54EB2AD622E, 4E9529BA4A6E42D6278D37E3FDEE9E1D991CEBE0, 50C6D4A2AD16A231CF11C43F3BBC868D90E20D25, 52009F36058337B6401DA0A0F4885A0C185F0520, 535882B6EDAB29247E035236A84CA510FB1E0854, 544CE18E4C1F1B288DEE6018DFCF4E4D4A315F7A, 54EBC125039CC83E4682CA44DD592534562B25C3, 5A08150C1DC17E9F691296F0A577C2EC9BA8028C, 5D1E61DA8083C41FF1FC23A1222A4A88B43A4E9B,
Arkanix	URLs	hxxps[:]//arkanix[.]pw/stealer[.]py, hxxps[:]//arkanix[.]pw/delivery, hxxps[:]//arkanix[.]pw/api/upload/direct
	Domain	arkanix[.]pw
	SHA256	6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5, 6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389

Attack Name	TYPE	VALUE
BRICKSTORM	SHA256	aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38, 013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf, 57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d, b3b6a992540da96375e4781afd3052118ad97cfe60ccf004d732f76678f6820a, 22c15a32b69116a46eb5d0f2b228cc37cd1b5915a91ec8f38df79d3eed1da26b, f7cda90174b806a34381d5043e89b23ba826abcc89f7abd520060a64475ed506, 39b3d8a8aedffc1b40820f205f6a4dc041cd37262880e5030b008175c45b0c46, 73fe8b8fb4bd7776362fd356fdc189c93cf5d9f6724f6237d829024c10263fe5, 40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759
UDPGangster	SHA256	028dcda69ba17f9c0d492fe2e0aa0b1bbb5154266c52840bd49f51ce11c934d4, 863f94873b7535f49a03784abf74a8a29b792b97dadc5361a379c7ae29d0ba4c, a35e0fccee6d9cf10a806c5134a85a1dadc0301312bbd9ae92af2fe1fbb77d24, a8aed7a290f38952be0e7360fd5f36276c279e430b51303780c5242d66cea932, b0dc4e34701f2032059c9eea77313628e7f79474a90dc40b4ed3ab39e0d06a37, 6d9ee1f6b8c344224116f47f81d4d2af58569925d22d731fb38b555771aa85f8, b95d35ef7dd6e98bcb30b896a5cee385c2e42cc94a1c9b124ef80fa65f20d3ba, 7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53
GachiLoader	SHA256	00bcfecad4b679f72c50cbdcd883caf55b6a1f641258a636317871c7b8940156, 00db4aa911e95ecfafa6f10ebfeb9f0a8051ee63de51ea1d9515ece5be2a294b, 01a3da42f74578c0b7c1146f30eceb2a2bc26c2d814a48fcf29ae527a1048aff, 028711c1b435c773ba600a863f4d4a2d1218860de799a1275d15d4ea93f0cbef, 02c0de5116d9b05d930e4858cd9768cc2ba70e91be62690439537fdf0f52de53,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	032a297bfbdc94226f0d88c77ab27148c54ebde6bfa2750fed09b1d8667ddcd6, 03d55245ef2766943813c0d1eaa3859d3918ee6fed2705bb5eeb38f4f87a5643, 079a180eeed0f4fc84c2412ba0398a79c5262efa1d9e8fd53290cd001b5abf9f, 094240cd298de1121da36adb96b3cdd632f866837f27e3951b6a0a544e5437f6, 0a6d41411ef3c65540a525dc5c3ab0964cd595aa73c3a477a8a96ec986277660, 0bd44592e75854a1c763384bf9dcea6dfe1174f6f45df342ebd9dfaa3a27dc85, 0c03845b9e2ff5ddac56f6e75b8e9dadf1a7bd1681d074e732478596b3173922, 0f81656ce724b65c230c4d63259c3a0edff20cc664de964f16451417eda60005, 14bfaf75b5c7ffac451f41352f8e94b6cc060efe7d645189795fa921f4e602bc, 16b2f7d9d4ace9e3004bd47f97c252a7fea21662656ec6b906d30a6b21900fc4, 18649874ab887ab613a3ccdd7cddc683e2b21f7cbe0762d2ce8201fc7e57540c, 1d28c23b271eb2156bf2780cb0dd042573f38f4758ef61877a7347bbbc756c8b, 1ebeca5dc62d759904c47597ebeb67865017a99892081c94d7647206b78a6cd2, 1f35a5ee4ead5c286f3e0d3ddecaf8789f12da7b8b7422b0511af619353284b7, 2038f38ccd42cd1df84abfb5915e3a6eb9c976b8d822768068343716f46a09f1, 210d821109ec1dff3b92ad3cfdde59912581327f4017b754864ba1e263c3c366, 2601d2c2b4515d3f1414d4543cfe2091490e2502457eab6c437a310f7e5e2a1a
MacSync	SHA256	06c74829d8eee3c47e17d01c41361d314f12277d899cc9dfa789fe767c03693e, be961ec5b9f4cc501ed5d5b8974b730dabcdf7e279ed4a8c037c67b5b935d51a, ecfaa20f25e11878686249c7094706bc3dcd2dc0ace0f2932a39d1bfdac85863, c4d3e5cdb264eded917cd61b8131c40715c0ee3f4d2c94c84d60fa295ca4ed97, 9990457feac0cd85f450e60c268ddf5789ed4ac81022b0d7c3021d7208ebccd3, 9d43e059111460c4f81351a062fb7eb7dbfd34988a06d756c7206f330c06cb42

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8489	✗	WordPress King Addons for Elementor Plugin Versions 24.12.92 to 51.1.14	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kingaddons:king_addons_for_elementor_plugin:*:*:*:*:*:*:*:*	-
WordPress King Addons for Elementor Plugin Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://wordpress.org/plugins/king-addons/

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

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

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

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

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

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

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

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

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

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

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

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-14174	✗	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac), iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium Out of Bounds Memory Access Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-122	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://www.google.com/intl/en/chrome/?standalone=1, https://support.apple.com/en-us/100100, https://support.apple.com/en-us/125892, https://support.apple.com/en-us/125886, https://support.apple.com/en-us/125885, https://support.apple.com/en-us/125884, https://support.apple.com/en-us/125892, https://support.apple.com/en-us/125889, https://support.apple.com/en-us/125890, https://support.apple.com/en-us/125891

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-43529	ZERO-DAY	iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use-After-Free WebKit Vulnerability		**CWE ID**	**ASSOCIATED TTPs**	**PATCH LINK**
		CWE-416	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/100100 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125886 , https://support.apple.com/en-us/125885 , https://support.apple.com/en-us/125884 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125889 , https://support.apple.com/en-us/125890 , https://support.apple.com/en-us/125891 , https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-59718	✗	Fortinet Fortios Before 7.0.18, Before 7.2.12, Before 7.4.9, Before 7.6.4; Fortinet Fortiproxy Before 7.0.22, Before 7.2.15, Before 7.4.11, Before 7.6.4; Fortinet Fortiswitchmanager Before 7.0.6, Before 7.2.7	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	-
Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-347	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol, T1556 Modify Authentication Process	https://www.fortiguard.com/psirt/FG-IR-25-647

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-59719	✗	Fortinet Fortiweb Before 7.4.10, Before 7.6.5, Before 8.0.1	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*:*	-
Fortinet FortiCloud SSO Login Authentication Bypass	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-347	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol, T1556 Modify Authentication Process	https://www.fortiguard.com/psirt/FG-IR-25-647

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-40602	✗	SMA1000 12.4.3-03093 (platform- hotfix) and earlier versions, 12.5.0-02002 (platform-hotfix) and earlier versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Missing Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862, CWE-250	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-23006	✗	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and Earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:sonicwall:sma1000:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Deserialization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059 Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20393		Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM): All Cisco AsyncOS versions (physical and virtual appliances)	UAT-9686
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:secure_email_and_web_manager_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_and_web_manager:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_gateway:-:*:*:*:*:*:*:*	AquaShell, AquaTunnel, AquaPurge, and Chisel
Cisco Multiple Products Improper Input Validation Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-68613</td><td>  </td><td rowspan="2">n8n all versions starting with 0.211.0 and prior to 1.120.4</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:n8n:n8n:*:*:*:*:*:node.js:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">n8n Remote Code Execution via Expression Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-913</td><td>T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1565.001: Stored Data Manipulation</td><td>https://github.com/n8n-io/n8n/releases</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSHARVEST	LOTUSHARVEST is a C++-based DLL implant designed to run quietly on a victim's machine via DLL sideloading, blending into legitimate processes to avoid attention. Once active, it focuses on harvesting data from browsers like Google Chrome and Microsoft Edge by opening and reading targeted files to extract stored information. After collecting these details, the implant enriches the stolen data by appending the victim's computer name and username, retrieved through system functions, creating a more complete profile for the attackers.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal data	-
Information Stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Fooder	Fooder is a newly uncovered loader crafted to execute the MuddyViper backdoor, entirely in memory. Several versions of Fooder cleverly disguise themselves as the classic Snake game, an approach that inspired the "MuddyViper" designation. Beneath this harmless façade, the loader uses a custom delay mechanism that mimics the logic of the Snake game, paired with repeated Sleep API calls. This combination intentionally slows down execution to evade automated analysis and obscure its true malicious purpose before deploying the backdoor.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Loads MuddyViper	-
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
MuddyWater			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MuddyViper	MuddyViper is a C/C++ backdoor designed to give attackers extensive control over a compromised system. Once deployed, it can gather detailed system information, execute files and arbitrary shell commands, and handle both file uploads and downloads. Beyond basic control features, MuddyViper also focuses on credential theft, specifically targeting Windows account passwords and browser-stored data, allowing attackers to deepen their access and move further within the victim's environment.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft, System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CE-Notes	CE-Notes is a browser-data stealing tool named after its staging file, ce-notes.txt, which it uses to temporarily store the information it collects. First identified in 2024, this stealer came to light when MuddyWater was seen deploying both EXE and DLL variants of it across compromised systems. Its primary role is to quietly extract sensitive browser data, adding another layer to the group's broader espionage toolkit.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	-
Browser-data Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LP-Notes	LP-Notes is a C/C++-based Windows credential stealer built with the same design philosophy as the CE-Notes browser-data stealer but focused entirely on harvesting login credentials. Its only purpose is to trick victims into entering their Windows username and password by presenting a convincing fake Windows Security dialog. Once displayed, the prompt encourages users to "re-authenticate," effectively handing their credentials to the attacker. LP-Notes delivered and launched via PowerShell using command lines nearly identical to those associated with CE-Notes.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal data	-
Credential Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Blub	Blub is a C/C++ browser-data stealer named after its executable, Blub.exe, and is built with a statically linked SQLite library to make data extraction seamless. Once running, it targets major web browsers, including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera, to pull stored login credentials directly from their local databases.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	-
Browser-data Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
go-socks5	MuddyWater's go-socks5 reverse tunnels are a set of Go-compiled proxy tools built on publicly available libraries like go-socks5, yamux, and resocks, and they have become a staple in the group's recent operations. These tools function as intermediaries, relaying traffic from a compromised machine, over a designated port, to a hardcoded C&C server, authenticating the connection with an embedded key over SSL/TLS.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Tool		Stealthy persistence	-
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Arkanix	Arkanix is a fast-moving, financially motivated infostealer designed for quick monetization rather than long-term campaigns. It targets a broad spectrum of Chromium-based browsers and cryptocurrency extensions, while also harvesting wallet data from standalone clients like Electrum and various Ethereum applications. Initially released as a Python-based stealer, distributed through Discord channels and online forums where it was disguised as harmless tools, it was packaged with Nuitka to compile the Python code into bytecode. Within a month, the operators replaced it with a more capable C++ version, promoted as a "Premium" build on their web panel. This upgraded edition expands its reach by adding modules to steal VPN credentials and Steam accounts, positioning Arkanix as a commodity stealer aimed at rapid, high-volume financial gain.	circulated through Discord and underground forums	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ValleyRAT	ValleyRAT is a remote access trojan (RAT) designed to infiltrate systems and give attackers unauthorized control. It adds new capabilities, including screenshot capture, process filtering, forced shutdown, and clearing Windows event logs to cover its tracks.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Service Disruption, Remote Access, Data Theft	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
Silver Fox			-

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

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

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

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

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

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

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

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

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

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Talisman PlugX</td><td rowspan="6">Talisman PlugX is a side-loading variant capable of executing multiple plugins for tasks such as keylogging, file manipulation, and command execution. It follows an execution flow, loading an encrypted payload, decrypting and decompressing embedded components, and injecting itself into legitimate processes to blend into normal system activity.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-21893
CVE-2024-21887</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="5">Credential theft, Long-term persistence</td><td>Ivanti Connect Secure</td></tr>
<tr><td>RAT</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US, https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</td></tr>
<tr><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">BRICKSTORM</td><td rowspan="6">BRICKSTORM is a Go-based ELF backdoor built for stealth, durability, and deep system control. It begins by performing integrity and environment checks, then anchors itself with a self-monitoring mechanism that automatically reinstalls or restarts if interrupted. The malware configures environment variables to match the compromised host, enabling stable operation.</td><td>Exploiting vulnerabilities</td><td>CVE-2023-46805
CVE-2024-21887</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="5">Stable long-term foothold</td><td>Ivanti, VMware, F5 BIG-IP, VMware vCenter</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>WARP PANDA</td></tr>
</table>

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

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

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

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Snowlight	A lightweight Linux loader used to stage and deploy additional payloads. Commonly observed executing follow-on implants such as VSHELL and establishing persistence via system services or cron jobs.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Loads other payloads	Meta React Server Components
Loader			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
UNC6586, CL-STA-1015			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Vshell	A lightweight Linux webshell and backdoor providing remote command execution. Often deployed alongside SNOWLIGHT for interactive access and lateral movement.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
CL-STA-1015			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Noodle RAT	Noodle RAT (aka ANGRYREBEL.LINUX) is a Linux RAT associated with DPRK-linked activity, providing remote command execution and persistence. Frequently observed masquerading as legitimate system components.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Command Execution	Meta React Server Components
RAT			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
UNC6595			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
KSwapDoor	A stealthy Linux backdoor disguised as a kernel-related service, using encrypted communications and peer-to-peer-style C2. Designed for long-term persistence and evasion.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Auto-color	A backdoor masquerading as a legitimate PAM or system library. Enables remote command execution and persistence while blending into normal system processes.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			https://nextjs.org/blog/CVE-2025-66478

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Minocat	A tunneling tool used to expose internal services and maintain remote access. Commonly deployed post-exploitation to bypass network segmentation and firewall controls.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Expose Internal Services	Meta React Server Components
Tool			
ASSOCIATED ACTOR			PATCH LINK
UNC6600			https://nextjs.org/blog/CVE-2025-66478

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Compood	A custom-built backdoor enabling remote command execution and persistence. Often deployed in targeted intrusions rather than mass exploitation campaigns.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC6588			https://nextjs.org/blog/CVE-2025-66478

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Hisonic	A lightweight Linux backdoor used for sustained access and execution of attacker-supplied commands. Typically observed in conjunction with other implants during advanced intrusion campaigns.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC6603			https://nextjs.org/blog/CVE-2025-66478

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Phantom	Phantom Stealer is promoted as an 'ethical hacking' tool for 'educational purposes' and is sold using a pricing model ranging from $70 to $700. Once installed and executed, it gathers extensive system information, including The Windows version, hardware details, browser cookies, passwords, card data, images, and documents are sent to attackers through channels like Telegram, Discord, or SMTP, containing the stolen data.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SantaStealer	SantaStealer is an emerging malware-as-a-service (MaaS) information stealer that is being actively promoted across Telegram channels and Russian-speaking underground hacker forums. Marketed as a rebranded evolution of the earlier BluelineStealer project, the malware features a modular, multi-threaded architecture that allows operators to flexibly expand its capabilities. Its primary focus is on harvesting sensitive documents, login credentials, cryptocurrency wallet data, and information from popular applications such as Telegram, Discord, and Steam.	-	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	Windows
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AquaShell	Custom Python-based backdoor developed by UAT-9686 that embeds itself into existing web server files on Cisco AsyncOS appliances. It passively listens for specially crafted unauthenticated HTTP POST requests, decodes incoming payloads using a proprietary algorithm combined with Base64, and executes arbitrary commands in the system shell with root privileges. The implant is designed to blend with legitimate application code, enabling persistent remote access that survives reboots and standard remediation efforts.	Exploiting Vulnerability	CVE-2025-20393
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Cisco AsyncOS Software (physical and virtual appliances)
ASSOCIATED ACTOR			**PATCH LINK**
UAT-9686			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AquaTunnel	GoLang-compiled reverse SSH tunnel implant derived from the open-source ReverseSSH project, previously associated with Chinese APT groups including APT41 and UNC5174. It establishes outbound SSH connections from compromised systems to attacker-controlled infrastructure, effectively bypassing perimeter firewalls and NAT configurations. The tool provides UAT-9686 with reliable encrypted remote access channels for long-term persistence on targeted Cisco email security appliances.	Exploiting Vulnerability	CVE-2025-20393
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Tool		Extended Persistence	Cisco AsyncOS Software (physical and virtual appliances)
ASSOCIATED ACTOR			**PATCH LINK**
UAT-9686			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AquaPurge	Specialized anti-forensics utility deployed by UAT-9686 to systematically erase evidence of intrusion activity from compromised systems. It leverages the egrep command with inverted matching to filter out log entries containing attacker-specified keywords, then overwrites the original log files with sanitized versions. This selective log manipulation complicates incident response investigations and allows threat actors to maintain stealth on compromised appliances.	Exploiting Vulnerability	CVE-2025-20393
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Tool		Erase Traces, Maintain Stealth	Cisco AsyncOS Software (physical and virtual appliances)
ASSOCIATED ACTOR			**PATCH LINK**
UAT-9686			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Chisel	Open-source tunneling tool legitimately used for penetration testing but weaponized by UAT-9686 for malicious lateral movement operations. It creates TCP/UDP tunnels encapsulated within HTTP connections over a single port, enabling attackers to proxy traffic through compromised edge devices into internal network segments. The tool's legitimate origins and encrypted communications make detection challenging without behavioral analysis of network traffic patterns.	Exploiting Vulnerability	CVE-2025-20393
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Tool		Lateral Movement	Cisco AsyncOS Software (physical and virtual appliances)
ASSOCIATED ACTOR			**PATCH LINK**
UAT-9686			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GhostPoster	GhostPoster is a stealthy malware that abuses trusted Firefox extensions to compromise users at scale by concealing malicious JavaScript within PNG logo files using steganography. Once deployed, the final payload quietly manipulates browser behavior for financial gain, hijacking affiliate links, injecting tracking code, stripping security headers, bypassing CAPTCHA protections, and embedding hidden iframes, effectively converting the victim's browser into a covert monetization engine without the user's awareness.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Malicious browser extension–based		System Compromise, Code Execution	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GachiLoader	GachiLoader is a newly identified and heavily obfuscated malware loader written in Node.js, designed to deploy multiple malicious payloads on compromised Windows systems. In the observed campaign, its primary function is to act as an initial delivery mechanism for the Rhadamanthys information stealer.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Loads Other payloads	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Kidkadi	Kidkadi is a notable malware loader that stands out for its use of a novel PE injection technique, abusing the Windows loading process to deceive the system into loading a malicious executable directly from memory in place of a legitimate DLL. This approach allows the malware to execute without writing a traditional payload to disk, significantly reducing its visibility and making detection and analysis more challenging.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Drops other payloads	Windows
Dropper			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Rhadamanthys	Rhadamanthys is an advanced infostealer distributed via multi-stage loaders. It collects credentials, system data, financial information, and browser data. It uses obfuscation and underground updates to bypass defenses.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Windows
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Foudre	Foudre is a downloader and victim profiler that targets high-value systems, delivering a secondary malware implant known as Tonnerre.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Additional payload deployment	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
Prince of Persia			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Tonnerre	Tonnerre extracts sensitive data from compromised machines, making it a potent tool for cybercriminals. Additionally, Tonnerre includes a mechanism to contact a Telegram group through the C2 server.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data theft	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
Prince of Persia			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MacSync	MaxSync is an advanced macOS information-stealing malware that exploits Apple's code-signing and notarization mechanisms to bypass Gatekeeper protections without requiring user interaction. By leveraging trusted digital signatures, decoy files, and cleaning up execution chains, MaxSync operates stealthily to steal sensitive data while evading detection.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data theft	macOS
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MgBot	MgBot is a long-standing, modular malware closely tied to the Daggerfly threat group, with observed use dating back to at least 2012. Written in C++, the malware is built around a flexible, plugin-based architecture that allows operators to load and swap capabilities as needed during an intrusion. This design has enabled MgBot to evolve steadily over time, with new modules and enhancements continuing to surface through 2024, underscoring its role as a mature and actively maintained tool.	-	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise, Data Theft	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Evasive Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Donut	Donut is an open-source in-memory injector and loader designed for executing VBScript, JScript, EXE, DLL files, and .NET assemblies. As a shellcode generation tool, creates x86 or x64 shellcode payloads from .NET assemblies, which can then be injected into arbitrary Windows processes. This allows attackers to run the injected code directly in memory, bypassing disk-based detection mechanisms. Due to its ability to execute a variety of file formats and deliver payloads stealthily.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Deploy Malware	-
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
Silver Fox			

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, G0069)	Iran	Technology, Engineering, Government, Manufacturing, Transportation, Utilities, University	Israel, Egypt, Turkey, Azerbaijan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Fooder loader, MuddyViper, CE-Notes, LP-Notes, Blub, go-socks5, UDPGangster	Microsoft Windows

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1591: Gather Victim Org Information; T1583: Acquire Infrastructure; T1608: Stage Capabilities; T1587: Develop Capabilities; T1587.001: Malware; 1588: Obtain Capabilities; T1588.002: Tool; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1106: Native API; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1543.003: Windows Service; T1053: Scheduled Task/Job; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1140: Deobfuscate/Decode Files or Information; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Checks; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1134.002: Create Process with Token; T1622: Debugger Evasion; T1070: Indicator Removal; T1622: Clear Persistence; T1070.004: File Deletion; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1112: Modify Registry; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1056: Input Capture; T1056.002: GUI Input Capture; T1082: System Information Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1074: Data Staged; T1074.001: Local Data Staging; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1219: Remote Access Tools; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1001: Data Obfuscation; T1090: Proxy; T1041: Exfiltration Over C2 Channel; T1030: Data Transfer Size Limits, T1566.001: Spearphishing Attachment; T1204.002: Malicious File; T1033: System Owner/User Discovery; T1095: Non-Application Layer Protocol; T1005: Data from Local System; T1083: File and Directory Discovery

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
ShadyPanda</td><td>China</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft, Financial gain, and Espionage</td><td colspan="2"></td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>-</td><td>-</td><td>Chrome, Edge</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1189: Drive-by Compromise; T1176: Software Extensions; T1176.001: Browser Extensions; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1027: Obfuscated Files or Information; T1480: Execution Guardrails; T1036: Masquerading; T1539: Steal Web Session Cookie; T1185: Browser Session Hijacking; T1005: Data from Local System; T1056: Input Capture; T1056.004: Credential API Hooking; T1041: Exfiltration Over C2 Channel; T1217: Browser Information Discovery; T1567: Exfiltration Over Web Service; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1557: Adversary-in-the-Middle</td></tr>
</table>

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

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

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

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

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 

UNC5174 (aka Uteus, CL-STA-1015)</td><td>China</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain, Espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td colspan="3">CVE-2025-55182</td><td>-</td><td>Meta React Server Components</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0010: Exfiltration; TA0042 : Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057 : Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron</td></tr>
</table>

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

TTPs

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

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

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036: Masquerading; T1036.001: Invalid Code Signature; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Browser Session Hijacking; T1005: Data from Local System; T1114: Email Collection; T1114.001: Local Email Collection; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1658: Exploitation for Client Execution; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol; T1574: Hijack Execution Flow; T1574.001: DLL; T1137: Office Application Startup; T1137.001: Office Template Macros

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
APT-C-08 (aka Bitter, T-APT-17, TA397, G1002, Manlinghua)</td><td>-</td><td rowspan="2">Financial, Manufacturing, Defense, Logistics, Government, Political, Military, Administrative entities</td><td rowspan="2">Europe, Canada, Russia, Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>CVE-2025-6218</td><td>-</td><td>RARLAB WinRAR</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036: Masquerading; T1036.001: Invalid Code Signature; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Browser Session Hijacking; T1005: Data from Local System; T1114: Email Collection; T1114.001: Local Email Collection; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1658: Exploitation for Client Execution; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol; T1574: Hijack Execution Flow; T1574.001: DLL; T1137: Office Application Startup; T1137.001: Office Template Macros</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6600	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	MINOCAT	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6588	-	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	COMPOOD	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC6603</td><td>China</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-55182</td><td>HISONIC</td><td>Meta React Server Components</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
UNC6595</td><td>China</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>CVE-2025-55182</td><td>ANGRYREBEL.LINUX</td><td>Meta React Server Components</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
UNC5342</td><td>Korea</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>CVE-2025-55182</td><td>-</td><td>Meta React Server Components</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-9686	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-20393	AquaShell, AquaTunnel, AquaPurge, and Chisel	Cisco Secure Email Gateway (SEG) & Cisco Secure Email and Web Manager (SEWM)

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0011: Command and Control; TA0003: Persistence; TA0005: Defense Evasion; T1203: Exploitation for Client Execution; T1140: Deobfuscate/Decode Files or Information; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1090: Proxy; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.006: Python; T1505.003: Web Shell Server; T1505: Software Component; T1070.002: Clear Linux or Mac System Logs; T1070: Indicator Removal; T1572: Protocol Tunneling; T1095: Non-Application Layer Protocol; T1027: Obfuscated Files or Information

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Prince of Persia (alias Infy, Operation Mermaid, APT-C-07)	Iran	Critical Infrastructure, Telecommunication, Government, Private Sector, Media	Iran, Iraq, Turkey, India, Canada, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Vatican City
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Foudre, Tonnerre	-

TTPs

TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1598: Phishing for Information; T1583: Acquire Infrastructure; T1583.001: Domains; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1543.003: Windows Service; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1574: Hijack Execution Flow; T1574.001: DLL; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1082: System Information Discovery; T1057: Process Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1056: Input Capture; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1102: Web Service; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1048: Exfiltration Over Alternative Protocol; T1485: Data Destruction

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Evasive Panda (aka Bronze Highland, Daggerfly, Storm Cloud, StormBamboo, TAG-102, TAG-112, Digging Taurus)</td><td>China</td><td rowspan="2">All</td><td rowspan="2">Turkey, China, India</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>MgBot</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059: Command and Scripting Interpreter; T1106: Native API; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1620: Reflective Code Loading; T1055: Process Injection; T1036: Masquerading; T1553: Subvert Trust Controls; T1555: Credentials from Password Stores; T1056: Input Capture; T1557: Adversary-in-the-Middle; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Silver Fox (alias Void Arachne)	China	Enterprise, Finance, Medical, Technology	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Donut loader, Valley RAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1106: Native API; T1129: Shared Modules; T1620: Reflective Code Loading; T1547: Boot or Logon Autostart Execution; T1112: Modify Registry; T1574: Hijack Execution Flow; T1574.001: DLL; T1218: System Binary Proxy Execution; T1027: Obfuscated Files or Information; T1497: Virtualization/Sandbox Evasion; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1057: Process Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1573: Encrypted Channel; T1008: Fallback Channels; T1041: Exfiltration Over C2 Channel; T1056: Input Capture; T1056.001: Keylogging; T1547.001: Registry Run Keys / Startup Folder; T1489: Service Stop		

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.003: Cron
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1559: Inter-Process Communication	T1559.001: Component Object Model
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1136: Create Account	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.007: Path Interception by PATH Environment Variable

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.001 : Additional Cloud Credentials
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.007: Path Interception by PATH Environment Variable
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.007: Double File Extension
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.012: Process Hollowing

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1070: Indicator Removal	T1070.002: Clear Linux or Mac System Logs
		T1070.004: File Deletion
		T1070.006: Timestomp
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	
	T1480: Execution Guardrails	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
		T1553.002: Code Signing
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts	T1564.006: Run Virtual Instance
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.007: Path Interception by PATH Environment Variable
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.003: NTDS
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.004: Credential API Hooking
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
	T1557: Adversary-in-the-Middle	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.003: Email Account
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.004: SSH
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.004: Credential API Hooking
	T1074: Data Staged	
	T1113: Screen Capture	
	T1114: Email Collection	T1114.001: Local Email Collection
		T1114.002: Remote Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1213: Data from Information Repositories	T1213.002: Sharepoint
	T1530: Data from Cloud Storage Object	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
		T1560.002: Archive via Library

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	
TA0011: Command and Control	T1001: Data Obfuscation	
	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
		T1568.003: DNS Calculation
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1565: Data Manipulation	T1565.001: Stored Data Manipulation
	T1657: Financial Theft	

Tactic	Technique	Sub-technique
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.004: Server
		T1583.006: Web Services
		T1583.007 : Serverless
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.003: Install Digital Certificate
TA0043: Reconnaissance	T1591: Gather Victim Org Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment

Top 5 Takeaways

#1 In **December 2025, eleven zero-day** vulnerabilities were discovered; additionally, **Three Celebrity Vulnerabilities** took center stage. This included flaws named **React2Shell, MongoBleed,** and **LangGrinch.**

#2 Activity during the period was dominated by **Silver Fox**, **Evasive Panda**, and **MuddyWater**, all well-resourced groups known for their 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.

#3 A diverse array of malware families was also detected actively targeting victims in real-world environments. These included **SORVEPOTEL, Arkanix, UDPGangster, Talisman PlugX, SantaStealer,** and **MacSync.**

#4 Cyber threat activity in December 2025 was predominantly concentrated in **India, Turkey,** and **Israel**, where malicious campaigns spanned ransomware, botnets, and malware deployments.

#5 Key sectors under attack included **Technology, Finance, Government, Transportation,** and **Manufacturing**, with attackers focusing on disrupting critical operations and stealing sensitive information.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **25 significant vulnerabilities** and block the indicators related to the **17 active threats actors, 43 active malware,** and **193 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 **25 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
LOTUSHARVEST	SHA256	48e18db10bf9fa0033affaed849f053bd20c59b32b71855d1cc72f613d0cac4b
Fooder	SHA1	76632910CF67697BF5D7285FAE38BFCF438EC082,
CE-Notes	SHA1	8E21DE54638A79D8489C59D958B23FE22E90944A, CD47420F5CE408D95C98306D78B977CDA0400C8F, C1299E8C9A8567A9C292157F3ED65B818AA78900
LP-Notes	SHA1	29CDA06701F9A9C0A6791775C3EB70F5B52BBEFF, 8F3ED626E7B929450E36E97BA5539C8371DF0EF8
Blub	SHA1	1723D5EA7185D2E339FA9529D245DAA5D5C9A932, 69B097D8A3205605506E6C1CC3C13B71091CB519, B7A8F09CB5FF8A33653988FFBA585118ACF24C13, B8997526E4781A6A1479690E30072F38E091899D
go-socks5	SHA1	25361183DE63F296BA71B6FCF0725E022B3C989A, 0E9A4892CFA1C9065B36D8F2E164E28609A8CF5D, 2B09241CA025BDC4455E9F6BA6009E2F27C08EDF, 2E9BE23CDD8152DB6CD1A54E001C4EA82FF6F1C6, 45FA7DE711FEA1F8D1E348E87834246C455DD2ED, 4E0EF2386980639FC5355FD68DAFF54EB2AD622E, 4E9529BA4A6E42D6278D37E3FDEE9E1D991CEBE0, 50C6D4A2AD16A231CF11C43F3BBC868D90E20D25, 52009F36058337B6401DA0A0F4885A0C185F0520, 535882B6EDAB29247E035236A84CA510FB1E0854, 544CE18E4C1F1B288DEE6018DFCF4E4D4A315F7A, 54EBC125039CC83E4682CA44DD592534562B25C3, 5A08150C1DC17E9F691296F0A577C2EC9BA8028C, 5D1E61DA8083C41FF1FC23A1222A4A88B43A4E9B, 6532E0437C8913FA418F1EE258561B15BBEE9052, 6CA41565844118385B345A39A9B79E0BBC0DD338, 6FC50A99AAE1D6C40111632D4F49BD19F9794CF6, 826CFF5D85713CE4B2F3C15AB53A84E6848D2E2C, 87ADD79C7C8335447113EE0D413F52AE2B17F066, 93055115559219BE8441880597C533381B99213B, 97C3376AB551E899F347CC9DDF49EA01DB2D7903, 99FAD0862E2E8D363F3E18952FD92E09493CC27D, A101CBCCD950AA36FC3B40C3C331FDE43ACDBBD2, A227C0A4425E24268B759A740231676A589CA4E6, A997A7AAE727D2C12CCE80FE3607317775A4DF3E, B0271CA76052EC340014D7BCCDBD69325A4E60F2,

Attack Name	TYPE	VALUE
go-socks5	SHA1	B0CD4F5DF192BFFE6500E44B80C28505DFD9CA66, B16E7D56A8DC0FF6B3AFD797E1EAB22B20DFFB39, D49979D0063B28BD73390481E6AE642C00CE0791, D518F5C648AB64B390A29AA2858219318CFC556A, DF223D653F761ED55F9C0774F1DBF545FD741F86, DF8FC5213AA11EE445EAD1AAE17A826E7D51A743, E02DD79A8CAED662969F6D5D0792F2CB283116E8, E8F4EA3857EF5FDFEC1A2063D707609251F207DB, F26CAE9E79871DF3A47FA61A755DC028C18451FC, FF09608790077E1BA52C03D9390E0805189ADAD7, A9747A3F58F8F408FECEFC48DB0A18A1CB6DACAE
SORVEPOTEL	SHA256	2d95769a016b397333ba90fdc2f668f883c64774a2c0aaaf6b2d942bebaee9e0
Arkanix	URLs	hxxps[:]//arkanix[.]pw/stealer[.]py, hxxps[:]//arkanix[.]pw/delivery, hxxps[:]//arkanix[.]pw/api/upload/direct
	Domain	arkanix[.]pw
	SHA256	6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5, 6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389
ValleyRAT	SHA256	a32fa6ba08db96ebd611f6ee06da44b419d569a6bac43ed00c68d6ca674004c3, 068e49e734c2c7be4fb3f01a40bb8beb2d5f4677872fabbced7741245a7ea97c, 1c3501b4689c6072553f84fd7ea04c655a204f9d960825c09745fcbe38a33cdf
XMRig	URL	hxxps[:]//raw[.]githubusercontent[.]com/C3Pool/xmrig_setup/master/setup_c3pool_miner[.]sh, hxxps[:]//raw[.]githubusercontent[.]com:443/c3pool/xmrig_setup/master/setup_c3pool_miner[.]bat
	SHA1	59de54c4cb7ccc1602c90d8afe2efc071751d9ae
Sliver	File Path	/usr/bin/sshd-agent, ~/.config/.system-monitor/.sys-mon, /tmp/.system-update/
	Domain	keep[.]camdvr[.]org, t[.]cnzzs[.]co
	IPv4	154[.]26[.]190[.]6
	URL	hxxp[:]//keep.camdvr[.]org[:]8000/BREAKABLE_PARABLE5, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE5, hxxp[:]//keep[.]camdvr[.]org[:]8000/d5[.]sh, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE10
	SHA1	0972859984decfaf9487f9a2c2c7f5d2b03560a0, 470ce679589e1c3518c3ed2b818516f27ccad089,

Attack Name	TYPE	VALUE
Sliver	SHA1	0972859984decfaf9487f9a2c2c7f5d2b03560a0, 2937c58115c131ae84a1b2a7226c666f6a27ef88
	SHA256	2cd41569e8698403340412936b653200005c59f2ff3d39d203f433adb2687e7f, cb5524b6605af240a7385f8f875c6af0b5009d5bcba4a3cc7c3e399057c7c644
PeerBlight	SHA256	a605a70d031577c83c093803d11ec7c1e29d2ad530f8e95d9a729c3818c7050d
	URL	hxxp://45.32.158[.]54/5e51aff54626ef7f/x86_64,
	IPv4	185.247.224[.]41, 49.51.230[.]175
	File Path	/lib/systemd/system/systemd-agent.service, /bin/systemd-daemon, /bin/systemd-daemon
EtherRAT	IPv4:PORT	193[.]24[.]123[.]68[:]3001
	URL	hxxp[:]//193[.]24[.]123[.]68[:]3001/gfdsgsdfhfsd_ghsfdgsfdgsdfg[.]sh
UDPGangster	SHA256	028dcda69ba17f9c0d492fe2e0aa0b1bbb5154266c52840bd49f51ce11c934d4, 863f94873b7535f49a03784abf74a8a29b792b97dadc5361a379c7ae29d0ba4c, a35e0fccee6d9cf10a806c5134a85a1dadc0301312bbd9ae92af2fe1fbb77d24, a8aed7a290f38952be0e7360fd5f36276c279e430b51303780c5242d66cea932, b0dc4e34701f2032059c9eea77313628e7f79474a90dc40b4ed3ab39e0d06a37, 6d9ee1f6b8c344224116f47f81d4d2af58569925d22d731fb38b555771aa85f8, b95d35ef7dd6e98bcb30b896a5cee385c2e42cc94a1c9b124ef80fa65f20d3ba, 7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53
MetaRAT	SHA256	aba6f7611291433983ba9c65654b04745a050530329d3ad329cc859c1ce12c44, d3ec33ae5c8ce2ac5eb0c96c6d6dc1d5ca610bacaa9de85d1e4bfe1d60923970, fd87149d6b8fdcad5d84ba4a3ca52e1cef8f0c54cafca6dbbb5d156f313d79dd, fd6b1ca0f26e54fa9c97ea15c834e58ffb71798df38071ad00b14f19d6a4126c, c91595edd1c9a0a2c1168e3bfa532e4a7dbb6b1380afd80ba445b728622798a4, c90460e820a8c5874d5412032b7db719cb8ea34ae8e48e4ab934a4096a09612b, a92ed5f831c99bb84208ef7d7c733e0183a79de40f9d3b3be54744951f0a1391,

Attack Name	TYPE	VALUE
MetaRAT	SHA256	0ec83d1deb6065cac8ba8f849cdf5672da7313ec2e860a7d71bb7e397e661394, 7b028a9bd2bc0c306ab6561cf702406f5925fc073f9d0d2d9408ceccd6907743
	Domains	doodle01[.]space, piao.mil.onmypc[.]net, newsinfom[.]org, mailserver[.]kozow[.]com
	IPv4	117[.]254[.]105[.]200, 45[.]114[.]192[.]137, 103[.]9[.]14[.]218, 23[.]254[.]225[.]184, 103[.]136[.]45[.]108, 103[.]172[.]10[.]165, 117[.]239[.]199[.]202
Talisman PlugX	IPv4	220[.]130[.]204[.]242
	Domains	turky[.]info, nord.ocry[.]com
	SHA256	78c3eb67fdc59fd09cba6388d6e31c428ed3c227f04b9cd739e8c36a8f1a182e, 367ad2eaa851ae17a4b75d92ec712d889fa85c0f2a51b9d5c5e08ae84fa7514d
BRICKSTORM	SHA256	aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38, 013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf, 57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d, b3b6a992540da96375e4781afd3052118ad97cfe60ccf004d732f76678f6820a, 22c15a32b69116a46eb5d0f2b228cc37cd1b5915a91ec8f38df79d3eed1da26b, f7cda90174b806a34381d5043e89b23ba826abcc89f7abd520060a64475ed506, 39b3d8a8aedffc1b40820f205f6a4dc041cd37262880e5030b008175c45b0c46, 73fe8b8fb4bd7776362fd356fdc189c93cf5d9f6724f6237d829024c10263fe5, 40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759

Attack Name	TYPE	VALUE
Pteranodon	SHA256	18b2956ceea0e45e2183dc1590fb306f9431943ed612e110af508d819d2ffd67, f08ea988890f33b18ae15d6d3466be0d60e974dece876450f16a0c82bf8469a7, 1f8a3ec047e0f44f1f21e1e3f8af5ea32749ecac3e2bef4fc2ba1a2006934581, c6e629c8375df83184401dd941ca2d490e78a1a338a9d0acdd43665b333cebfe, 7370668e7d715e19d36a7580ca04f349c7365d568ffbb5735eb6c79d80d63b63, 9b14d367c99b7d9187a58406ad3eb55e2dee12b4b2bc341f9058c622b7b87fa3
GamaWiper	SHA256	d4ce4776bdad9b741a1e8345b41737245b80f4cf8d361ebb1ae5415c7a4fe1eb, 9a39423ec90dc06a3058279cd744c08d83252d1c7096633b9853e435cc205755
Snowlight	SHA256	a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665, 18c68a982f91f665effe769f663c51cb0567ea2bfc7fab6a1a40d4fe50fc382b, 1a3e7b4ee2b2858dbac2d73dd1c52b1ea1d69c6ebb24cc434d1e15e43325b74e, 1cdd9b0434eb5b06173c7516f99a832dc4614ac10dda171c8eed3272a5e63d20, 1e31dc074a4ea7f400cb969ea80e8855b5e7486660aab415da17591bc284ac5b, 2b0dc27f035ba1417990a21dafb361e083e4ed94a75a1c49dc45690ecf463de4, 2ca913556efd6c45109fd8358edb18d22a10fb6a36c1ab7b2df7594cd5b0adbc, 4ff096fbea443778fec6f960bf2b9c84da121e6d63e189aebaaa6397d9aac948, 55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864, 62e9a01307bcf85cdaeecafd6efb5be72a622c43a10f06d6d6d3b566b072228d, 7d25a97be42b357adcc6d7f56ab01111378a3190134aa788b1f04336eb924b53, 7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a, 9c931f7f7d511108263b0a75f7b9fcbbf9fd67ebcc7cd2e5dcd1266b75053624, ac2182dfbf56d58b4d63cde3ad6e7a52fed54e52959e4c82d6fc999f20f8d693

Attack Name	TYPE	VALUE
Snowlight	SHA256	ac7027f30514d0c00d9e8b379b5ad8150c9827c827dc7ee54d906fc2585b6bf6, b38ec4c803a2d84277d9c598bfa5434fb8561ddad0ec38da6f9b8ece8104d787, bc31561c44a36e1305692d0af673bc5406f4a5bb2c3f2ffdb613c09b4e80fa9f, bf602b11d99e815e26c88a3a47eb63997d43db8b8c60db06d6fbddf386fd8c4a, d704541cde64a3eef5c4f80d0d7f96dc96bae8083804c930111024b274557b16, d9313f949af339ed9fafb12374600e66b870961eeb9b2b0d4a3172fd1aa34ed0, E2d7c8491436411474cef5d3b51116ddecfee68bab1e15081752a54772559879
	IPv4	115[.]42[.]60[.]223
Vshell	SHA256	4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b
Noodle RAT	SHA256	33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f
	URL	hxxp[:]//146[.]88[.]129[.]138:5511/443nb64
	IPv4	192[.]238[.]202[.]17
KSwapDoor	SHA256	1f3f0695c7ec63723b2b8e9d50b1838df304821fcb22c7902db1f8248a812035
	IPv4	140[.]99[.]223[.]178
Auto-color	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43, 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4, 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a633, a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d53d0a, bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f02d6b, e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc3048f7, 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042bb255, bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b051510d1ca
Minocat	SHA256	776850a1e6d6915e9bf35aa83554616129acd94e3a3f6673bd6ddaec530f4273
Compood	IPv4	45[.]76[.]155[.]14

Attack Name	TYPE	VALUE
Hisonic	SHA256	df3f20a961d29eed46636783b71589c183675510737c984a11f78932b177b540, 92064e210b23cf5b94585d3722bf53373d54fb4114dca25c34e010d0c010edf3
Phantom	SHA256	4b16604768565571f692d3fa84bda41ad8e244f95fbe6ab37b62291c5f9b3599
SantaStealer	SHA256	1a277cba1676478bf3d47bec97edaa14f83f50bdd11e2a15d9e0936ed243fd64, abbb76a7000de1df7f95eef806356030b6a8576526e0e938e36f71b238580704, 5db376a328476e670aeefb93af8969206ca6ba8cf0877fd99319fa5d5db175ca, a8daf444c78f17b4a8e42896d6cb085e4faad12d1c1ae7d0e79757e6772bddb9, 5c51de7c7a1ec4126344c66c70b71434f6c6710ce1e6d160a668154d461275ac, 48540f12275f1ed277e768058907eb70cc88e3f98d055d9d73bf30aa15310ef3, 99fd0c8746d5cce65650328219783c6c6e68e212bf1af6ea5975f4a99d885e59, ad8777161d4794281c2cc652ecb805d3e6a9887798877c6aa4babfd0ecb631d2, 73e02706ba90357aeeb4fdcbdb3f1c616801ca1affed0a059728119bd11121a4, e04936b97ed30e4045d67917b331eb56a4b2111534648adcabc4475f98456727, 66fef499efea41ac31ea93265c04f3b87041a6ae3cd14cd502b02da8cc77cca8, 4edc178549442dae3ad95f1379b7433945e5499859fdbfd571820d7e5cf5033c, 926a6a4ba8402c3dd9c33ceff50ac957910775b2969505d36ee1a6db7a9e0c87, 9b017fb1446cdc76f040406803e639b97658b9876019701258269 60e94e9a1a6, f81f710f5968fea399551a1fb7a13fad48b005f3c9ba2ea419d14b597401838c
	IPv4:Port	31[.]57[.]38[.]244:6767, 80[.]76[.]49[.]114:6767
AquaShell	File Path	/data/web/euq_webui/htdocs/index.py
AquaTunnel	SHA256	2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef
AquaPurge	SHA256	145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca

Attack Name	TYPE	VALUE
Chisel	SHA256	85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc
	IPv4	172[.]233[.]67[.]176, 172[.]237[.]29[.]147, 38[.]54[.]56[.]95
GachiLoader	SHA256	00bcfecad4b679f72c50cbdcd883caf55b6a1f641258a636317871c7b8940156, 00db4aa911e95ecfafa6f10ebfeb9f0a8051ee63de51ea1d9515ece5be2a294b, 01a3da42f74578c0b7c1146f30eceb2a2bc26c2d814a48fcf29ae527a1048aff, 028711c1b435c773ba600a863f4d4a2d1218860de799a1275d15d4ea93f0cbef, 02c0de5116d9b05d930e4858cd9768cc2ba70e91be62690439537fdf0f52de53, 032a297bfbdc94226f0d88c77ab27148c54ebde6bfa2750fed09b1d8667ddcd6, 03d55245ef2766943813c0d1eaa3859d3918ee6fed2705bb5eeb38f4f87a5643, 079a180eeed0f4fc84c2412ba0398a79c5262efa1d9e8fd53290cd001b5abf9f, 094240cd298de1121da36adb96b3cdd632f866837f27e3951b6a0a544e5437f6, 0a6d41411ef3c65540a525dc5c3ab0964cd595aa73c3a477a8a96ec986277660, 0bd44592e75854a1c763384bf9dcea6dfe1174f6f45df342ebd9dfaa3a27dc85, 0c03845b9e2ff5ddac56f6e75b8e9dadf1a7bd1681d074e732478596b3173922, 0f81656ce724b65c230c4d63259c3a0edff20cc664de964f16451417eda60005, 14bfaf75b5c7ffac451f41352f8e94b6cc060efe7d645189795fa921f4e602bc, 16b2f7d9d4ace9e3004bd47f97c252a7fea21662656ec6b906d30a6b21900fc4, 18649874ab887ab613a3ccdd7cddc683e2b21f7cbe0762d2ce8201fc7e57540c, 1d28c23b271eb2156bf2780cb0dd042573f38f4758ef61877a7347bbbc756c8b, 1ebeca5dc62d759904c47597ebeb67865017a99892081c94d7647206b78a6cd2, 1f35a5ee4ead5c286f3e0d3ddecaf8789f12da7b8b7422b0511af619353284b7, 2038f38ccd42cd1df84abfb5915e3a6eb9c976b8d822768068343716f46a09f1,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	210d821109ec1dff3b92ad3cfdde59912581327f4017b754864ba1e263c3c366, 2601d2c2b4515d3f1414d4543cfe2091490e2502457eab6c437a310f7e5e2a1a, 266216b097561e57448b940c3087b82c4cea7581b67e5dcc52c8c4dfcbbf8333, 278c5a0acd6603947e59e1961642279e29cc4b9be299c8edb7b719d6568eb8da, 29fac0ce48b9114990a4dd942d6de1da55bf9c49938929123fb1f221be385eff, 2a87f4d47ad95f4eb46c08a4d33fd4732c10a1408db1b758871dfe6b1059c6bb, 2e5389a32a6c21fec476fdc6e80fcb577de31c43adb7c090c3a11f3b048787ed, 2fee47e12ca72863ee132d63dcac3b39aeace1a4d71b0aa14a30b56ecabf29c9, 30bcfa6bbb5e9d9bc64c65a27e1565a9ad21af3d5e1f202933a340cc400abdb9, 3124fe59b26dc77c1e4b4d615112928ca1830c890c8c77e853ac6948069ba463, 3151700d8f13cf55ad46148cd46ccb0b3409c0adf253433f16ef6612e9280eb2, 31dac5bc21b0dabfac51cb99c821e62421c39949971a44898a1ec15efe33e8c4, 32855dba1ec6b3c9ba422cf9203d8130e59dcb5235764b8f56b6d02970a5e5b5, 33dce93dfdb43f47ef1d36e2dd16725ed365300c371dc45491b52afe13b6e412, 3630538febdedf693ca9d996c3f1998d50c97052ab99e653d95b381ddb3546ef, 38a7feb5ab611e6a487ce8b048732f7721484ceebb316fd34c9cc611dbc4e3cc, 38ac7917ce895448203e6d14f121850ecc4ff89f530e792c794d771f881c7b07, 3c16548ab32996a58298978b20db1d4133827298e166f93b7c943dc3ffc51782, 3d8c1469de3bb01ef72992e07d1feea9380183983327576978851b8c78ea7fc9, 3ed63941e7411e93f644a064094b5a6c7e2a9547840a5198dd7f6b4d45ef9eea, 401e7b72f4b7ed4119b625ab34c2c7d37c0dabc08bbdf943fd291445e2fe753c, 40f899294ea02f7a9823ada63c869ede18a8afc6238aedb62d2b30a2744cb846, 4210e9e1df0bc41e497285483782609c0b4777ef6682fb40b0d25c8149c9f3d2,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	428f86204b69f31dfc3f3479d18d23b15cad63d72998a8418e8da22941c74956, 43b1a11962f83db6bb59bb7467d5456e852d0421ca5eaeae3a249a34839e67b4, 43d9130c8f077a5885842bda24bee19e4dd231c49f88629442e5b9f02ff5f33a, 45fd42669157357f1e16c0b542eab5836061f5b2e2160a5104a4bde38cac85bf, 47ab9b9deaa14202b94320df16f52c8d98adee49c9bff8909ab5deefcbdfe401, 48a269d2c083868e2b5347012afb85bb3c233c9f042985bcab764f7788316660, 4b71d8cb7ce8de8d557283df3543aa2aed89dd5446c7acf855c0ea2e5e7e89dd, 4be48937c603c910c29de2af3b0d3e3bc05b809b19190e90ade2489a347d8b03, 4ed90af2fb3fe13eb8ab69fe2fcd82a0775426da33da4ba043d7e7e2fd4a18f7, 4f8c55cb3f99741f4fcccdbcff07c7d0b8ab7fa23dcbf8847d7a37a35f6d3f5e, 4f95af5b4a1569eb54f6995e547584f429a49895d0d81c71d74970275b170a08, 5173c6b57642dd89dba2f039a1ad630d6d73d3557248dd09ca2a51a329e6119e, 53ac3b1601f2fa43121cfd43ac9b49f6751a8b84b4ffcc5a1241f71eb1e8d7b8, 5538d6f24e1330c934cdfc95188aede5c9668154376e507c41fe1c752cdd7a5b, 561436df09f87be34317eeb25a2b7bf5c67201fa501262f72a9a63b9977ae217, 59c93f81063e8b77b20292d1d03598f74d997690aac41f5fb7a248ac8ad866c2, 5c88a6efd0a713460dcf8b828575285be3a43d6481e245662bafb3472d344dd1, 5d1bf72af319901f22d78625d60c877d7a8d6c54bbbcbcfc643376558e176211, 5dbdd6d45021383a3c76b2e0c7258a7b0fcfd70904602eb2fb1afe3b33efc80e, 60de97fff85ba6f0b114fe565f53ffc1ef43a19de95c31299884e034f05dc037, 616b74a6b17b70bae357c43cf03fe1946abc36eea1d0e7d911ca29bd067f63ae, 61e215ccf73cba014ecd72abd38ff78d5a23c2727577c5b3e2c8f52b90dc2a4a, 62bab101900a92db76e2c368c4a83f7340f42c460b16d11dea94c8db002d5bc9,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	62bcb939df4a8b7bdc896cd229cf34f55d93555c14e5816ac2aa6285d1cf4112, 6463e7f48f01f482fa846bc106de245c833ad7c3ea7fae4caa7ead54b2901cb9, 64d6d018e3b7a1d718b96d9950b3579af2a784ab004ad575e13cb41b2c27aa25, 66e684ab10b1daf2a46df1031c6ddc331ab80af4e21144a68997d4a1859e9fd7, 6985717a754fe121e99c337cc33b0e9a25852fa33c580dc9caaffefaf0908233, 69c0084b78bf963997033759fa45933b61de425aea7612a06289ec6c78492745, 6a8dd64af57926514131efdc388c9883db2c23aebfd8b97c44e808d637f0fc23, 6b80c4fa88fbb35af2b254c63586fd6e0455d0e917b842afc79b821ac87a2b9d, 6c428016506c2ae076d049deeba60514cb8c0afa6fd00fc349722cdbc6e1b305, 6d5af67f05c9db6763cd494f64c5f62faeb8f1b67ba26a7ab278e27d4c9b8f22, 6f1b97838bc5702954ef5f536de86a8477e0008f25bcfba72b7fda4c1f37b9d2, 6fcd071c6ab51e71407e8bf242fac8552a10aedff113c9efb92ccc53cc49fbed, 7029d2c60ee04772d9dc4d8d34f5effd3e3be17769584bbf912954e926280131, 71415238f740c7528f3314f94dc07ffd9b802a34c3997b09ad02da1bcd3c8137, 717f05b96a344b1fdd159b4c45e3089a26d1f64e63cd4ac2ed3bf2db33074c3a, 765041cdf97bf0b55734cd5619d7d4568a641ae3fc35540344a488184839674b, 78908b01a8d959b80f7fa1f42c734c4c64a8cec58394f94cf362b8efd38c7b9c, 78b6c96910d8f1e3889bad17f97cd26aed5f6c7a15432cc11c2224a8c9adf691, 7a155a20c1e5df83b566fdad3bf59ca49ac6559e0561233a95c7cd70a5caa6dc, 7db2025192f4f2497bdc356c1920dfc4740bb868de8a6b5786f01865dfa9e564, 825bd0b103d647c296bd2b9eee251b04b7f5dc72f27898fcf0fc25ca24587125, 8295cddaf1c23d554b90e4d1ee1ca064f68124df63003a046f58241c3513cd1e, 8383a421e9a4f55af53cf1911680042659b28722cff8a30cd202bc728a8fea23,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	8443994a687269f2d7d19678e571ce1a1658df7da69c25b4bd902f87f849c98d, 857f68127546f829861e796b11b80304e2c53e70e54191fec8087f64d7c8146d, 86082a735440124bae953c0a68e5eff6a7fe6792f90ea1e71cc0c83a724bc273, 87c1c62369657904418affebca3f706a4e968dd1a672729274ba287dfae43be4, 88938ad37225074c923ac4baa0b4a171076c273cb064a4905c66a25ca3acfee0, 8d473631c12231079a241d63ddc9e4b537d2531135e9aa4d795abf22f2aefd39, 8db4cf8f666b7c4ec5051139570b5d3b88569c9e62de31249a70b6cdc716aecd, 9211d6fb5db70a51ba5795e0a7126aa1efd0f4b78262031dfb72e98c319ce37e, 95760397b9cc05d0180258afee22cd8e6bc997e13754a11cb737733d0beeb444, 95f875c01b889f9ba811dae11822c6c83eb28d8260f16ca070c76e83f6f7e7cb, 96d2c11dd5bb43da5945259494d7e26a68b5c48eaa32d5eb2d1dc61aa0dfb7fe, 980d0d78b3e288f24bcb793d2e49a4e26138cfe4ef272171557658be751d277d, 99a3a973caf956102c563773a9a58ff79c539c7c77480873dd0e09fa259b3594, 99cc25edbc65ea201b957abbd6cfbd7b3b6f04759cbb47fc999d35508a654748, 9a0ccafc516df1e931ba2028ea59f39b31e1cc812c3a2ab1765b9e91fb8cc507, 9a28d80ce2c191d743554313edbb8eef09e6f72b34c4d701c0a84090d61264e9, 9b60930efa096a98d9fb6392c74f8d3e5f2df6ba8a5b31a304b7fac3d847e7f1, 9c562c28323e7681c1cb5a4b23e703c21cda8bc020946de691b6765fcb613a16, a9ec251b719b2ebb85e50f43eea4e2944e0a065daaf5c92420efc852b594d96f, ad27bfdd9d51f81e6e743ed351c47812874565e89f6ace03ac39d6c85fefa949, af0891bff41d67815ed7a979fc2127295ea662079afa16d09d1a377684d678ba, b1b72689afa038d413e36f5aca61b971b69e4e411976cbd01e3cbf5b2e83141e, b67ac42c0ef7402dd53dc950e8162e9a213aa65d5a7901a5cc4aee0b93058b93,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	b6a3ad06c57b45142dd7ac2c77ea70980296b5d168517f5d7ec4100ec10d305a, b8eaa5c0686fb49f6f3e4edd5716df48581001249d5e62563f2468db73526cce, bd378786d84743beb0adc8d3dd14ff3d7996caaf6a1eb8783c665091ee9ae225, bd7df13098f3984a18c4a21282ba04ed802bb73c1f91c7eb5a35b89544c545cb, bfd049ef7d1384a25c3edaf857b94539525b5f442dbe543fafa2356315780d8d, c164232a5a3a2b49705257e62c5f8e004df68e3cf32d7702e4af879abd55008b, c1a6587fb04a94943ab616cf0ce8b3d0c55e59ffbd4bc9b3a1add955391210ae, c1fb323ed08adca20912906e8756e6f8a805cd1d08cf20226f37cb51f33117eb, c4cd91a5ce722f3c510151513501e9aab54ad535b934132e6e6f6c9c76be2e9e, c50c73ef1be87b84055ee73bda503ad20884fcf67b207fa918190f40f4353729, c5e9eaaa5dc6ec4780c319c26a4f552f7030438dcfb008ccfd52358512dc3f81, c605642e0edac4b63e9819648f79d54d5f47cac240480fad808cbfb61f31c88a, c67bad311a48bb86a865b08ad2ef175a17e46063ef3c5de734fb3c4a5ea07578, ca0c525bf22b499b2f374d41f7e07a60ed9181645af485b0183c65eea68d364d, ca1465224a206c9323a4a3215afa402ce7f592ddf17db5d477d2a5905e982d56, cd6c1ebc720ba509967f9e508657ad02d8fafee1d958af0174bfd0d192291d0a, d2c3f54b03d50271dad1eba0abf1cad6529d67b74015e530f716bd18f943c6b5, d52894f027b8ce185efa3f584024b8a9a7f6694f6e294aba8ddac9789d00468f, d56afbac1b7eebdb1aa03744cb45a260975de75a08e7f4d9a89ccb57656d9b65, d5e05fa6ddbaf68f6b08e188d444b664a08a69a6102df37c4c3c3cbc7ebfd326, d5e530f607260ee2ce19ef3f6ac277b202cd15fc947b0c02ba9060421f799bc3, d64d4ede406cc439617a2f17e31a3d9c1adb81d35cbb97de1a7e0145b03a08cd, d666dcf48f569d6ba9defd87e149408373c0ac237a017624fd51aacfcfeb89d0,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	d66fb9cc2c40311df8af5aee664303f5226338cd0f2046cb2f8d8d42bda6f9b9, d737d53d2fb7a233b9732bfcd9c99ac8ef9846ad65af07cae490c8ffd9dc02ee, d858fd5207e758e84b7ea1a84f27b0e782d0cf3a39db9fd72c3869bd136f9440, d9133df2668bac02ab8150fe9bc7b44a69936322b624fdf80a4f0de635970e81, df481a8014760def4bdd933639d01e8381fed910f5cf6d0e974560afc446451b, dff27eb46d17a25416a9cbefb705d13ccaf8bbc03461f3112fd5132c6261a187, e111cbbc94fa932ad24e84cb308195ad7d05fa2d9bb2716a0f6f9c11a4c3f570, e17622f041536a253ab17dfc10011a65225356cb120970b4c4948df1c37ced23, e1d90617390211860b40839338c235df016cafeed7bdda9f39b17b86f48a9fe8, e37d2b812d6ce5653ee7c54157b6288469152dd64a4cb3cb25943bbc3b28e909, e6cdc47ab4a4496d42d84281d5d89c4fdad665cad0546e820aa29e9a18d454f2, e70516e7aa7c9dbfc459993516cde705685f1e44a75c29c55d9f71abe7733c78, eb3f6f8f99b86d4a68490e56a6f5a963523743685ecb6c8bd1d87389dbe0fde0, ed74747bb58f78df2c11f247cc173051cc0e058fad7def595d14b8ce03889a53, f09e67864cc19f5b831fde944c7ee917cbd3af9ff89ed4893d2fa441d12bf5d9, f25531eef40e268b251ce117375bbcaa1a586506d3fa56fa722b200713ee4c1b, f37df47e517702f3becf6e3c85733dfea0031572bf199c1f56faad951b354573, f566a942a7c59f53efd9418f0c97850a749a806ee84e88056138c699d3b4d08a, f624c81e47e350123490897fa04fe43886ae9cec9b128e8b9ef54fe9405b4612, f64a20a44a60dd899bf0cccb5de57897dd80819cd36c55878a56ed0d1c995352, f8a881216fce67e89b8a56774504b5ea86ebb763d87ff7426a9344d13790e7ea, f94c8771545fd31371dcdfbe80260378709e686b44c2b440957cb923aa952b37, f9bc90f545b3eb8d5bd963d00debc6f3ff22403f94f91d063f18a7fb85be59eb,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	fa1bd55fc9aecc625992448306e0dd456e4011bc07a926046ed6d3280aededae, fbfa7f980b0d29f8c12933ef68daff306e2cbec3247db8242a5d97e6a96927d7, ff02edab9a670769ce074b2f6d6728909950785d2c8507e01d3333de98156c58, ff89d6917b775ef0bd38e4ee3a401bb310c4276eba79ff872b827920f72185b3, ffd7d43487fa1e15d8ea2a1e8737533cfcf7763cad6cb7504f270500a37f4261
	IPv4	94[.]154[.]35[.]99, 176[.]46[.]152[.]18, 213[.]209[.]150[.]104, 62[.]60[.]226[.]233, 66[.]63[.]187[.]72, 178[.]16[.]52[.]231
	Domains	davpniktonevidit[.]cfd, nupogodi[.]cfd, nexus-cloud-360[.]com, globalmarket247online[.]com, vault-360-nexus[.]com, iietrich[.]cfd, mceenzie[.]sbs, digitalservice365cloud[.]com
Kidkadi	SHA256	01bdbb37d4b5d22ab98f1977f89c0eb69b35cdbf1d690c434a9d21dc1d0c56b0, 02bdf8a8206b520db3d55fb7426ecef1ad10518f22eba26c848e548b75bc9999, 04bb04bbea55fa1dabda974b2c2f4aceb44ddccb7b9c1715e0aa67318369a768, 0577a28c0bcc1b033f44f458ab2d068fc301ef30d4175a3d2012d3601e9e13e1, 0859936dff1e2af60940c5f0764e187c642ffea5344118eb702a7ac59f5a9281, 08b5875f9867aa6c71cb8d96fb79de9f8975e0f7d1298388c95845aaa49e55de, 0ef9623e3ba8bc2c5be6de9cccd4a9e17bf74d1f8f83455da40c35f72fb34922, 110a17f1d65790337329d22d94ac10a9b6581202d5eab02897cb41ac543f1007, 13f1ee54ec2f7ca835313b828c64d1b0ffd6288c59e3361013a17c765da7335c, 178a24418d3057eb38b80e63786f9908a856618f1d19a9b667a55dff2717c9db,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	20179c8ceeede0056b0d3f545d0641160490642c90b23dce5603b8b47acb62d0, 2101d91dc775638f1f392d0867aca9a15d9139f0c986ed7004df134c9c52fcfe, 254abb6da9296f8c6f8e567186e3d59ddba2392fa4baf791492f7e76b4ff5af7, 28a9a74d8eeae80de63a1938cadfa55a5a0f334e593e975cb32af8ec3cae79e6, 2aea932e216145e38e5751f4daa9788974dd8e4ad4e90d7b42613d3df6341aee, 2e519a26e3cb67b9e1186065c4245f89b8cdfb5b3346fc86b028213e0f08c286, 2ed1c34780a3e9d2972f14d2828abf77a329075bd4c055458ef2f064237544b9, 354a66191805500b4a45d7455fd02527ffe0b76ae9285eabf8f182ea7d893c19, 38063272da02cf4fd383c634df988c07dcb2ce59cc3cdb036c4ff155fefc62e2, 38da058e5fafbdd9c371f4d64e7cc0e317ad1e59291470ddf01c7681c0c03c43, 3903bab79a2fa38e05df6f311d2dc9640c5916f8050bffab0d47ab8e58837210, 396caae9215849b674eecb0f8d5b91985f81986069c09e50454cb8f607ad4231, 39c72a4467ead5190ab2aff718c1d8fe66dd03760b3c2bb085466d56a6d10f3e, 39cdf78fdfeeb8ce82f5a8b0abbbfb1a74fd0bf9568e11a9b5f5d47060c33dc7, 3dbea0934dd2de6441ba27b762dc6424ce518f4882555fb96cd5225f9167339a, 405072e611a49489d1074dafcd84791f60ab9daebf55be36b924718e9d847c48, 416b81138d3c20578228c9610dca686eb7193e8d93cc4a2a18e6815efeacb810, 425d78b7a5cbd87b36e4ca991171e90851d0dac29fe5934fe9b289ea88793298, 46926ff7f778ea242603d233eabc0916a8a6945769fa0ea20c60cbac1f164150, 4a509f3605cb039c6f426e110b23ce82f1ef67db06c32e4bc5ebfb3ae3ca1e31, 4bdf84addb7e9bce6bb98086e6554f68fd529c49ae20b770d8db9ffc9debd3df, 4bf54789913bfbca6bb87263137ff6a662e32eb9e9ff124441af6304cc2b401e, 568e8082704d7fd2473862e93120412de1d043da5d106a12f9d1d5f1492eb173,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	56e4bb0f077b2081f0fcdaeaa90d8c6da48beedfb0a381ae054030e5a2988f05, 574934eeab1d23c163c4e59cad869de2f5c3d46dbdd563b17fb4320b53e95770, 5982d92d6a3bd210fd13a9986bda7f9fc6cb0321e523506acf9dc2e9ee6501de, 59a17d129944bf8bc426d23746b285522d94b293eb2c2808d56a307022e5b92d, 5a290d01a08f774f13f0991b7cf5c8c48b8cd2c0eb896ad069f02a474d8747f2, 5bd83b8ecfb1efd13191a76cb0998cf6d645491b76b6fe4f1a516bfd756bed3b, 5e4ae0bdc6081a22357e73aff3023a63623f3475610b23c35ff073b0b6890175, 6253d1285a7579f482ba1983a2c4db2c01f9f11194dac76aca4424e3d6977a02, 62db621c97bdaadffc1e900aac8d3af6e4e759b27018da635418c3921e1c8068, 679ff95c8c383d55b60d80d1803f347e206bd358e3980ee8de1de105680ffb37, 6bcb16d0ceae1b27bc7860477aa60a8c2a2588fb7625aa3a2dd78ee543658437, 6dc57007880918de4ef89d98b70dfa0cb1ac4c7a9d1eeffc57408d3f18524980, 6e087f40e4aac5fa780bfd1046c1d65e2b59c6abf391f9507718e61be61ddf42, 6edb286fa173145e8bb9597d8f02ec3d86f9f680468ba48618bcc5d2240ad121, 73cf316dc4359d80022e0ff7be22b9c86530e982a1d939e78a20090b9373b8a4, 77c728333ebff9d313d87b763b9d8e4a9d580b76f734ea6e43d7cc7bc81da260, 7a70e48a2721d5f5946ec2904dee105ba6c8561b205e5e8fce2aa5f6f3ef0549, 7c53826ea6a9f4ba8d44ca455f1723af9d72b99e97d5053babcfd528fb344e24, 80e8a40be533b4470275d567f7f9d21f6ba4e41e9b3272de77ff67ab9f8442b4, 828c2b61686f9dd8ee888a89ad92793b586a273b57bfd0ad57be6ae2f72616b1, 861c9536994ea3bb6c7aa5463001b79ab61fd945cf44956074d9034e384b3834, 8b30ecb0376e7853c4b323e6b504c967d76f22aa880c587878aa4d5de9bd9808, 8ee29bb1ea8f289d2233fd8053001a29b4fb7d5275120bbcb3e92f5cd5a77b47,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	8fb633896f714598c3b935cc45658f3fa14c99a006708c0a78e2f7d29b4c2b1f, 90f4f2c7d5fd9ea10e05cd9bb28a7700fe3fd5cc97d5d59b7e0f043e74f4adbd, 9dc8628aa94effdb2e982d10a6daa4b7897b75db9d452d806f839c9099c01fd4, 9f074ac880d8ae454c84dc03fcbaf0a9c4a15b32a28a590708a38ec6542fc620, 9f38d473a87c4c72760dd3e578c21f23b271c3c6a28d92e9ffa842073c4abc3b, a0857210ed5a0e38a73a908158905f4271bf82d3f18e0f73494c1846043102f6, a21d016f92be196e4d101a9f20d928ededa930dca835e5bdaffa0ea96372530e, a3bdc6f2f7930af9d4f3378c88fa9c84ee36c8a79b6689c0907fb4e065d7b572, a66220bea0f76e47ca218b99a2b91c7347cb3a291f2df03329009fde23c1a02a, a745b6efbb006d7c9c33503c12f247a95d3d72b98e22f6aa883d7ef45359afdc, aa71db5eb8ec06fbf676dacbb53bc3fdab62169b7287fe5d489713661ddf6360, af14df77f75b1440cd98dc39e4fd24e4d4da62904a699ca2e977c91db30ecc0d, afdcb3443f1b46fe4bd0818654dcbf48a542afdebef4c0725618cd66b2dbddf9, b10e7bbe60e82ec581a3dea4d829838d9c9603f4581125d0200b620d366c75cb, b281b6ffb8cf114b5836ead7cbc424179ac4070e2b15721a5a84af6be0b376d1, b8d46875182730276cf2a67de909ab4b8f3f298554f39928b418984d8cb515b0, bb359ebb2ddc1489a3489c0c37b974d05f9a37e23d4e74517d882fb5c7e493b0, bb88a06cff4e8d73eef046c6a8352dfff7f52903761ced27acd68c065391a464, bd2fb7d2bb7c15d634a986068d5cf811faa83aed72cb7e81df5e5082b22356d2, be68dd32a6b3375935fac1cebf132a2fc7fbfd4074cb8c53022d8eb4e7e17db1, bf5ce4b2911f2d6592abafaf5096936e61d23f98fd9a6b6bbcd763269fba729b, c0b239f989ecd535b9e80570487a39ad67c1e77ba3133caba150da7bf553b724, c10d286de8111a7133831d57394164586584157da2b50d7f3bb85582d69c2b17,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	c26b86a7e9ff0fb61a2ac0e9eaf78ed34e97a0326df66c7d2311ee7a6033e590, c2b66d97a64d87ce48eb5fb972d23a6b834a677ae154f9f8d4300e9699922ca5, c7646b0f6de08759e19928e25f2ca65cd023a9b820101ae52eb2dc7c7f6f1a69, cbeb46542f05028aee563efb5afa3616612637b31928f98b3d880de2ca524fb0, ce5b2579a7893c29ad24ad7126cb83ab629e1d879f69348ad2eb5f9b884d4c44, d1b7ae2d2e12faa4244bd4e5625ffbb2e525586f888bf5b292386221672b5b6d, d5038061e4d308341f6dfd7e807c84266442dbd0afe3b567082ebf6fdbd4c5d4, d51e67e9d81041500994880ecbad47f43a66fc4779a5f79c2c1f47517b8b14ec, d79722670889cf3ce869ed23be59c12029e0df3e536162045b6a87f0b522672d, d80cd0fe212dcfd4a0e683d36c48ba73a7e500a31dbf3f629a13c89565db7580, d8d138f4ebb7a5f12691e2c4edddcf906b66bd5640f8e09e1196a629a624a2ca, d9e2773a56847f4d28e82b2e7215bc4db05807a08d49588f6d6b40be9a430d1b, dbb8a2943af9559d4b3ec8e4c0879cfee3edd882e78b1cd1fb4546acdd7365ee, dce1732d7e260843a9930dea78ff1dc6c469bd306817c827318b56d754f77a98, dd851d7d8b79900e151f91f82d9f1826db493b67f012829783001ab5ffe392e2, ddf5f0ac5484e8e3090b9ce51f53f57cba9550be0e5fcdc2b60787ffc31c15c5, de13a7f1f2cc3cfeeaed063b558134631add81f74e58595bfdf921ff78470a9c, de40f512a3ead48f8c334bcd92198304df41d166ee0c0a90dc4a281464ee7980, ded2e57b60ba81fe9fc9a52ee0591db262527a0b6d166c6ca7165bfb99c4e835, e076d0d1bac228175f0ea23046f0bb7241b0a0457d245ae365ec3de8554a3499, e2627e6c31bb30f791ae80fbbf7d6b57a9ce6ae9e568cff6942ccf6f72195a5e, e4d7ace20cd9704805d144c26bd8c54f6a1b3175b549b6c8279e2d0ee81da9d2, e58ed739c3e6f0f1b0aee262ce0cd99cff6fa04ec7bd665c7c9de7fdfd289c1e,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	e7372984816703e5664bb1a0632bd7689d573e2868ceccd138c0a5a2977b2a23, e79d67e6c265ff53fb428123711db25b5fc3612ae650b55a2c6484bce3385bec, e806c33313e0490293edeb998abcd9413744e307af5619662ae6a62f6224aee7, ec55eadc6aab2a8c519c016e4b238b39463345c87160b7e2005e6e38ef05ff21, eca5155749b0f83671e8c17094a4380c19a3b5096781bd7b88cd9f93a70fc574, ed0cbb7b137a10493319473610209016f2c1a8b9560876bc32999b472a32e18f, ee363c5bdc5e786b0b47840d8fe69a5bd71f3684a9eec5d9e49b9ab68c64c793, ee752ce83f645fe4d3db0b1d8c41428d7b9adf37e72a9c21c153450862d30906, eed231bda3ad5a946a254d06865610e50b05eabaece8f09f84323d9fb23e2742, ef4d2a7ca4306626ff90e53ebad63e243a50dff63f34eb0eeaeb4acb2f39c42b, f0269f2b26534acc3ef8bee5b243c54b14812769249a974b2e2b7eba9734a967, f1de30fa0eeedc1f1a7d97736cf751c88fb01456a182f97ede7294bc89bf69af, f4f18af4acee36826b8e2162749250ffb96fc7f8f154d181dd1b8179cf4da68d, f73e65f624f15d967951a6795c712daf31363ab1602485c164549b04989caaaf, f9648d34727738abe86310378929ab7a8d5c8f2698c913bc84dee9be49e3b96a, f98ce437118aeca437a43612858068f4ea6099bb93c63f1b4ffc4d4335e8eaed, fbae3424943aec7aea7ce380c7a83c89ca9c6ff243bfac5186edba6e560f5b66, fd06caf741fd4e5fc9f00c575cc22c00f1a7fd55e826a16dbabc8b3436ed64c4
Rhadamanthys	URLs	hxxp[:]//176[.]46[.]152[.]18[:]8181/gDatFeDway/r26ggaap[.]dssde, hxxp[:]//178[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/mh3af5md[.]wg4ja, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/ujp8k5q9[.]kbtsk,

Attack Name	TYPE	VALUE
Rhadamanthys	URLs	hxxp[:]//185[.]141[.]216[.]120[:]1888/gateway/st2jdbg8[.]gsg45, hxxp[:]//78[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/el3tkioe[.]xcg4w, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/mbw0n34s[.]gibis, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/wwpac3ey[.]q23nf, hxxp[:]//cxbnqdytjgrxutmzawczv[.]cg/gateway/0f4m3h8r[.]trz19, hxxp[:]//jfbcrmphnnikoktsmcpzirlplkwp[.]zl/gateway/8pv47lge[.]93qfg
Foudre	SHA256	43ccc2620229d88d5a6ca2b064da0554ec3c3cc29a097e7a2d97283257cfae69, 0bfc11c6ba57fdaa8b865555d80d8f7d7b1d0f41a23a277885198b3113c945d9, cf64bf78ce570f8085110defc8ec32ff4f01c7359723510b9d1923fd93d12240, fbb2ac0d07b84068aa35376cc994039f9fc1d2341643bc2bf268d65ab11ecbe3, 2c46406fb9111e0e4d982de54f335ae2900cdc39490d58f765cd5014153b3e12, 52abb57bf6f9db815b3ddf6241e21d4096f36eb998bb51e728bbe68c0f8e8e15, fa95a09e538b8c186a3239e3ff80ec9054b50aab80c624e75563ace4e60e31da, f54cfe296186644d0fed271c469af1ef9b6156affe9e030e7b83b8de097eb1e7, 6f976a685ae838a7062fb4f152c6c77c42168b78b9aadd4278ec1c19f9bc1055, 12847dc6dfd86603e8f0085ae561b4b2e3089e5414e49628f7c411483c7b5ce8, d3d8b79f86f152338aabeadfaf35ba2e43f82aa4bfa29ff70b59702b455fa6a6, 15dd41ec1bdaabb741e8cc6481e0a98831798ac4e93c2513cdbd00c51241ffb7, 52e3a856548825ec0a3d6630e881ff4f79d2a11bc3420a73d42e161fabed53d9
Tonnerre	SHA256	cb6ed0dd5dbc2e34ae36dd22b9522f7eec94bbfda2dcda7425736656279f8cdf, 30c20ada243b7e476e006dec94876bdeece4f8aca12a4cb6cf962c80f1a6ee3c, d9dfc8a8e3e259a517a91e2e91e3a1d6ef1d5b0886e6729bf897d6ef1b2de722, c8583fddf668808e31f993ff6bcfc6f8ba8b4c2c0c4ea51d4ccc6f5d311b6c90

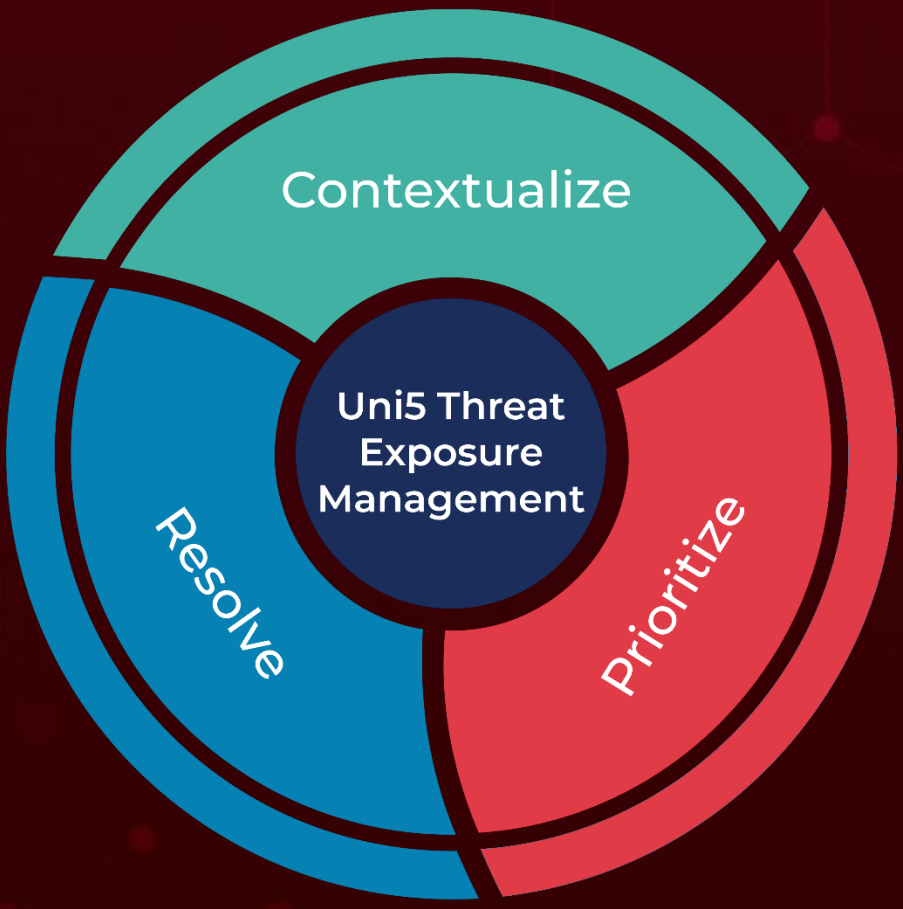
Attack Name	TYPE	VALUE
MacSync	SHA256	06c74829d8eee3c47e17d01c41361d314f12277d899cc9dfa789fe767c03693e, be961ec5b9f4cc501ed5d5b8974b730dabcdf7e279ed4a8c037c67b5b935d51a, ecfaa20f25e11878686249c7094706bc3dcd2dc0ace0f2932a39d1bfdac85863, c4d3e5cdb264eded917cd61b8131c40715c0ee3f4d2c94c84d60fa295ca4ed97, 9990457feac0cd85f450e60c268ddf5789ed4ac81022b0d7c3021d7208ebccd3, 9d43e059111460c4f81351a062fb7eb7dbfd34988a06d756c7206f330c06cb42
MgBot	MD5	9e72410d61eaa4f24e0719b34d7cad19
	SHA256	7376FCB7D2BFDCD858CF0920F6B7611E263D779CDC419A246B2D3004CBA2C39F
	IPv4	60[.]28[.]124[.]21, 123[.]139[.]57[.]103, 140[.]205[.]220[.]98, 112[.]80[.]248[.]27, 116[.]213[.]178[.]11, 60[.]29[.]226[.]181, 58[.]68[.]255[.]45, 61[.]135[.]185[.]29, 103[.]27[.]110[.]232, 117[.]121[.]133[.]33, 139[.]84[.]170[.]230
Donut	SHA256	7cfd50d3099b681c6739bd392700e5bf18a314ab7d554a2f39faf53d445dbce0, cd1373851bc2dc1ac18743aa988fbefe9d32d0c21a0dbf65e3361cf455b3cc4f, c971b537adc9851fcdd3ba4ce13693a2615021c478d384d0089603a6a13d69e0, da23077aa0cd928f82b178ba9ad9e43d684ce40000998051799c28b0439a6c4d, b37b346737c69ec3b32d468f3fb085a30d26b368b33b9442ca0687cb30c966f3

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 2, 2026 . 8:00 AM

More at www.hivepro.com