Date of Publication
February 2, 2026

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JANUARY 2026

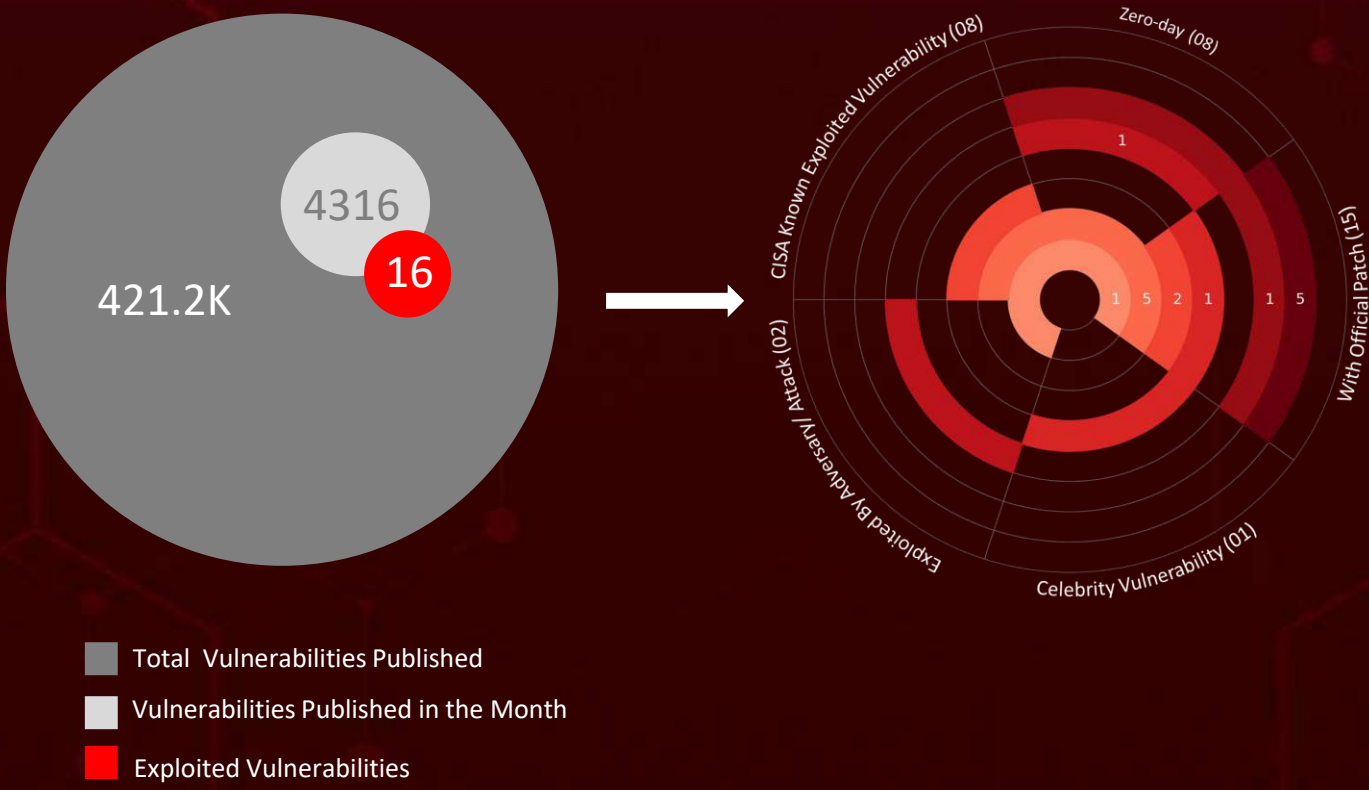
Table Of Contents

Summary

In **January**, the cybersecurity arena drew significant attention due to the active exploitation of **eight zero-day** vulnerabilities. The standout "celebrity" vulnerability, **Ni8mare** (CVE-2026-21858), exposes n8n workflow automation instances to unauthenticated remote code execution, potentially cascading into full infrastructure compromise. Cisco's **CVE-2026-20045**, affecting Unified Communications products, is already being actively exploited against internet-facing deployments, while the critical HPE OneView vulnerability (**CVE-2025-37164**) enables code injection attacks on enterprise infrastructure management systems.

GlassWorm is a self-propagating supply chain malware targeting Visual Studio Code extensions using "invisible" Unicode characters and leveraging Solana blockchain for unkillable C2 infrastructure. The **Astaroth** banking trojan has evolved with WhatsApp-based worm propagation capabilities, harvesting contact lists to distribute malicious archives in self-reinforcing infection loops. **VoidLink**, a sophisticated cloud-native Linux malware framework written in Zig, emerged with 37 plugins designed for long-term stealth access across AWS, GCP, Azure, and Kubernetes environments.

Concurrently, **five** threat actors have engaged in various campaigns. Iran-linked **MuddyWater** is evolving by deploying RustyWater, a new Rust-based RAT targeting diplomatic, maritime, financial, and telecom entities across the Middle East with enhanced stealth capabilities. **Mustang Panda** maintains persistent operations against government entities using the CoolClient backdoor with advanced clipboard monitoring and proxy credential extraction capabilities. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

In January 2026, a geopolitical cybersecurity landscape unfolds, revealing **Turkey, Cyprus, Qatar, Bahrain,** and **Slovenia** as the top-targeted countries.

Highlighted in **January 2026** is a cyber battleground encompassing the **Government, Technology, Telecommunications, Financial Services,** and **Human Resources** sectors, designating them as the top industries.

OneView, Total Control: Inside HPE's CVE-2025-37164 Critical RCE Exposure

Ivanti patches two actively exploited critical **zero-days** in EPMM enabling unauthenticated RCE.

Mustang Panda has stealthily evolved its CoolClient backdoor into a quieter, more persistent espionage tool built for long-term surveillance.

PHALT#BLYX: How **Hospitality** Networks Are Being Breached by Design

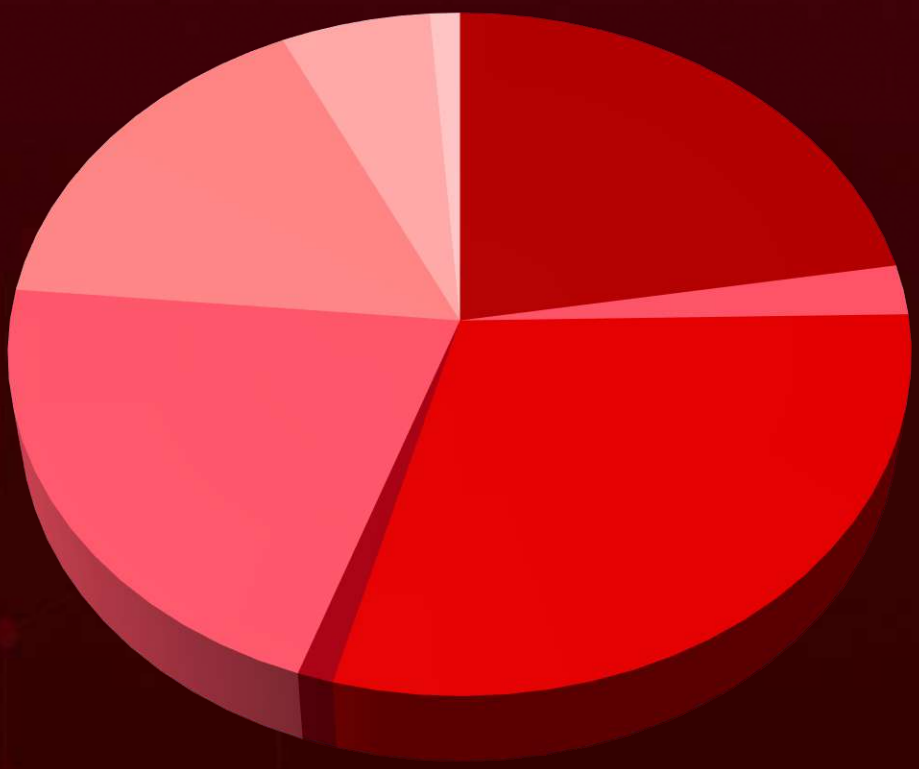
MuddyWater is evolving by using Rust-based malware and advanced phishing techniques to enhance stealth and persistence.

CVE-2026-20045 Cisco RCE Flaw: Active exploitation is already targeting internet-facing deployments in the wild.

Ni8mare (CVE-2026-21858) turns exposed n8n instances into high-impact entry points that can cascade into full infrastructure compromise.

CVE-2026-24858 turns **Fortinet SSO** into an open door, letting attackers hijack administrative control across vulnerable organizations.

Threat Landscape



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

Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21858	Ni8mare	n8n version 1.65.0 - 1.120.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:n8n:n8n:*:*:*:*:*:*:*:*	-
n8n Unauthenticated Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552: Unsecured Credentials	https://github.com/n8n-io/n8n/releases

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-13915	IBM API Connect Authenticati on Bypass Vulnerability	IBM API Connect	✗	✗	✓
CVE-2026-0625	D-Link DSL Gateway Command Injection via DNS Configuration Endpoint Vulnerability	D-Link DSL Gateway	✓	✗	✗
CVE-2025-37164	Hewlett Packard Enterprise OneView Code Injection Vulnerability	Hewlett Packard Enterprise OneView	✗	✓	✓
CVE-2026-20805	Desktop Window Manager Information Disclosure Vulnerability	Desktop Window Manager	✓	✓	✓
CVE-2026-21265	Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	Secure Boot Certificate Expiration	✗	✗	✓
CVE-2023-31096	Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	Windows Agere Soft Modem Driver	✗	✗	✓
CVE-2025-64155	Fortinet FortiSIEM OS Command Injection Vulnerability	Fortinet FortiSIEM OS	✗	✗	✓
CVE-2026-21858	n8n Unauthenticated Remote Code Execution Vulnerability	n8n	✗	✗	✓
CVE-2026-23550	WordPress Modular DS Privilege Escalation Vulnerability	WordPress Modular DS	✗	✗	✓
CVE-2026-20045	Cisco Unified Communications Products Code Injection Vulnerability	Cisco Unified Communications Products	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-20393	Cisco Multiple Products Improper Input Validation Vulnerability	Cisco Multiple Products	✓	✓	✓
CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office	✓	✓	✓
CVE-2026-24061	GNU InetUtils Argument Injection Vulnerability	GNU InetUtils	✗	✓	✓
CVE-2026-24858	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability	Fortinet Multiple Products	✓	✓	✓
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti EPMM	✓	✓	✓
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti EPMM	✓	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
GlassWorm	Worm	-	macOS	-	Phishing
VVS Stealer	Stealer	-	Windows	-	Social Engineering
DNSChanger	Trojan	CVE-2026-0625	D-Link DSL Gateways	EOL	Exploiting Vulnerability
GhostDNS	Botnet	CVE-2026-0625	D-Link DSL Gateways	EOL	Exploiting Vulnerability
DCRat	RAT	-	Windows	-	Phishing
GoBruteforcer	Botnet	-	Linux	-	Brute Force
Astaroth	Banking Trojan	-	WhatsApp	-	Phishing
RustyWater	RAT	-	Windows	-	Phishing
RushDrop	Dropper	-	Linux	-	-
DriveSwitch	Loader	-	Linux	-	Dropped by RushDrop
SilentRaid	Backdoor	-	Linux	-	Dropped by DriveSwitch
Bulbature	Backdoor	-	Linux	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
AsyncRAT	RAT	-	Windows	-	Phishing
VoidLink	Malware Framework	-	Linux	-	-
LOTUSLITE	Backdoor	-	Windows	-	Phishing
Evelyn Stealer	Stealer	-	Windows	-	Social Engineering
Amnesia RAT	RAT	-	Windows	-	Social Engineering
GOGITTER	Downloader	-	Windows	-	Phishing
GITSHELLPAD	Backdoor	-	Windows	-	Phishing
GOSHELL	Loader	-	Windows	-	Phishing
SHEETCREEP	Backdoor	-	Windows	-	Phishing
FIREPOWER	Backdoor	-	Windows	-	Phishing
MAILCREEP	Backdoor	-	Windows	-	Phishing
CoolClient	Backdoor	-	Windows	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Tsundere Bot	Bot	-	Windows	-	Social Engineering
XWorm	RAT	-	Windows	-	Social Engineering

Adversaries Summary

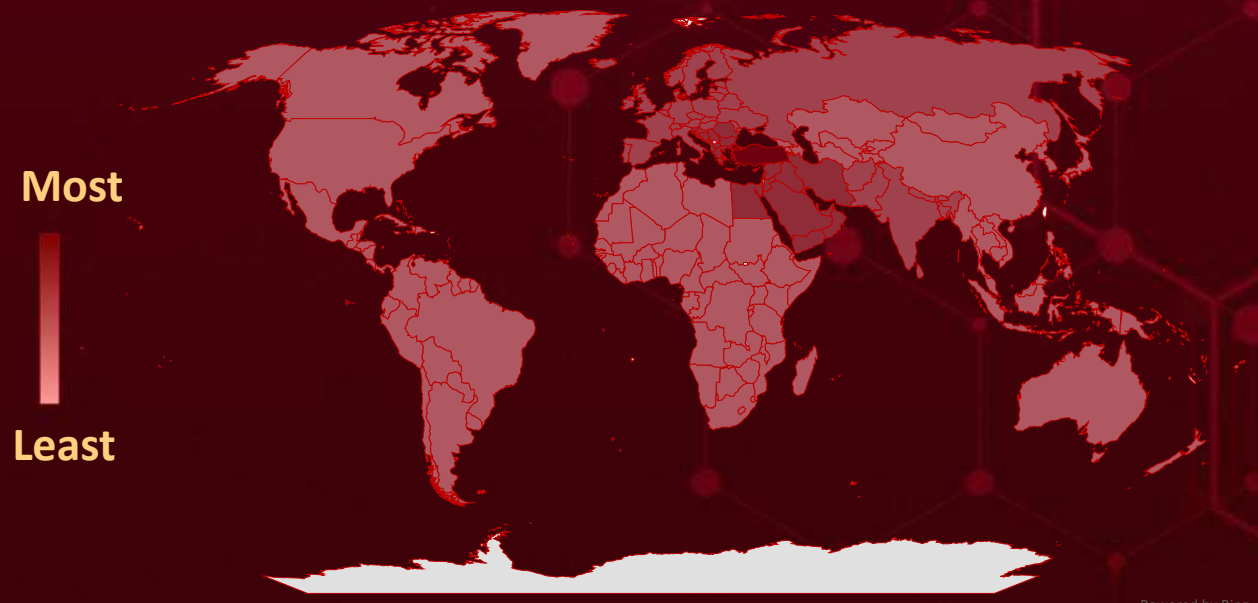
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT36	Information theft and espionage	Pakistan	-	-	Windows
MuddyWater	Information theft and espionage	Iran	-	RustyWater	-
UAT-7290	Information theft and espionage	China	-	RushDrop, DriveSwitch, SilentRaid, Bulbature	-
Mustang Panda	Information theft and espionage	China	-	CoolClient	Windows
TA584	Information theft and espionage	-	-	Tsundere Bot, XWorm	Windows

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
IBM	API Platform	IBM API Connect V10.0.8.0 - V10.0.8.5, V10.0.11.0
D-Link	DSL Gateway	D-Link DSL-526B, DSL-2640B, DSL-2740R, DSL-2780B
hp	Infrastructure Mgmt	HPE OneView (Before 11.0)
Microsoft	Operating System	Windows 10-11 25H2, Windows Server 2012-2025
	Application	Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise
FORTINET	SIEM	FortiSIEM 7.4.0, 7.3.x, 7.2.x, 7.1.x, 7.0.x, 6.7.x
	Operating System	Fortinet FortiOS (Before 7.0.19, 7.2.13, 7.4.11, 7.6.6)
	Application	Fortinet FortiManager (Before 7.0.16, 7.2.13, 7.4.10, 7.6.6) Fortinet FortiAnalyzer (Before 7.0.16, 7.2.12, 7.4.10, 7.6.6) Fortinet FortiProxy (7.0, 7.2, Before 7.4.13, 7.6.6)
n8n	Application	n8n version 1.65.0 - 1.120.0

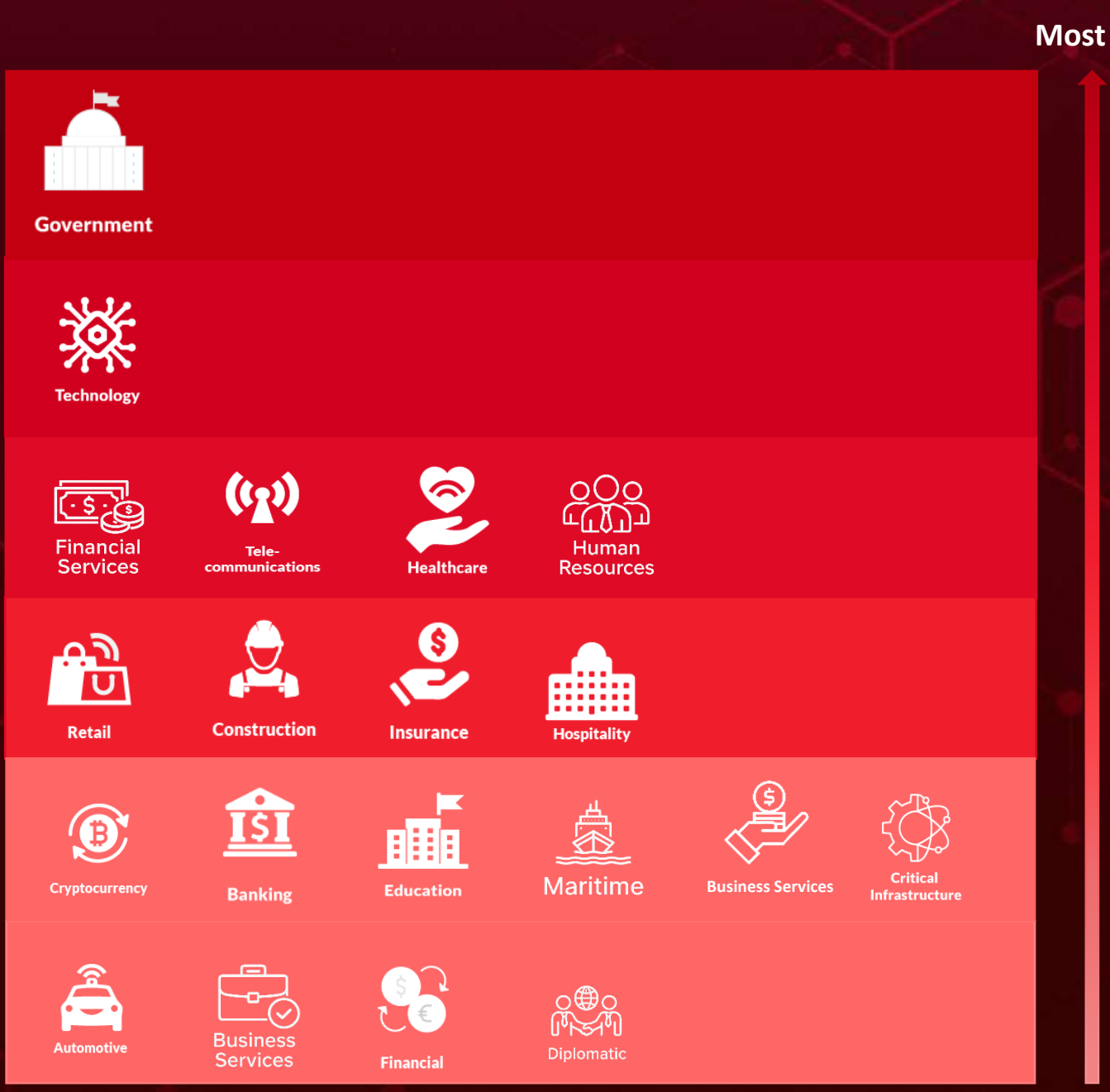
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
cisco	Unified Communications	Cisco UCM, IM & Presence, Unity Connection, Webex Calling (before 14SU5, 15SU4)
	Email Security	Cisco SEG, SEWM (prior to 15.0.5-016, 15.5.4-012, 16.0.4-016)
	WordPress Plugin	Modular Connector (Before 2.5.2)
ivanti	Application	Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior
	Application	GNU InetUtils telnetd versions 1.9.3 - 2.7

Targeted Countries



Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	Turkey		Iran		Germany		Switzerland		Holy See
	Cyprus		Serbia		Andorra		Luxembourg		Fiji
	Qatar		Iraq		Hungary		United Kingdom		Honduras
	Bahrain		Albania		Sweden		Maldives		Canada
	Slovenia		Syria		Iceland		Malta		Chad
	Bosnia and Herzegovina		Israel		Moldova		Armenia		Gabon
	North Macedonia		Jordan		India		South Africa		Chile
	Bulgaria		Lebanon		Belarus		Rwanda		Tajikistan
	Saudi Arabia		Russia		Austria		Greenland		China
	Croatia		Nepal		Netherlands		Togo		Brunei
	United Arab Emirates		Ukraine		Ireland		Grenada		Indonesia
	Kuwait		Czech Republic		Norway		Peru		Uruguay
	Yemen		Pakistan		Italy		Guatemala		Colombia
	Montenegro		Denmark		Poland		Cameroon		Belize
	Egypt		Spain		Bangladesh		Guinea		Azerbaijan
	Oman		Estonia		Bhutan		Suriname		Papua New Guinea
	Greece		Monaco		Latvia		Guinea-Bissau		Comoros
	Romania		Finland		San Marino		Central African Republic		Eritrea
			Belgium		Afghanistan		Guyana		Bahamas
			France		Slovakia		Palau		Eswatini
			Portugal		Liechtenstein		Haiti		Costa Rica
					Sri Lanka		Benin		

Targeted Industries



TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1027** Obfuscated Files or Information	**T1071** Application Layer Protocol	**T1566** Phishing
T1204 User Execution	**T1068** Exploitation for Privilege Escalation	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1203** Exploitation for Client Execution
T1059.001 PowerShell	**T1070** Indicator Removal	**T1041** Exfiltration Over C2 Channel	**T1071.001** Web Protocols	**T1105** Ingress Tool Transfer
T1082 System Information Discovery	**T1005** Data from Local System	**T1090** Proxy	**T1083** File and Directory Discovery	**T1543** Create or Modify System Process
T1140 Deobfuscate/Decode Files or Information	**T1547.001** Registry Run Keys / Startup Folder	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1036** Masquerading

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
DCRat	SHA256	91696f9b909c479be23440a9e4072dd8c11716f2ad3241607b542b202ab831ce, bf374d8e2a37ff28b4dc9338b45bbf396b8bf088449d05f00aba3c39c54a3731, 11c1cfce546980287e7d3440033191844b5e5e321052d685f4c9ee49937fa688
GoBruteforcer	SHA256	ab468da7e50e6e73b04b738f636da150d75007f140e468bf75bc95e8592468e5, 4fbea12c44f56d5733494455a0426b25db9f8813992948c5fbb28f38c6367446
AsyncRAT	SHA256	eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286, c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd, 02aa8cabeea2a0120a31adbf0886f821d10953fc6d4d9cd1959568093c48b04d, 279b157c99432100bab17e6f23bd90cb397582324b091010d8cf1ec2683d3e4d, 6da6e608ba1bf369e01785d677c8fc95e551ee847d420a1be885677871a30134
VoidLink	SHA256	05eac3663d47a29da0d32f67e10d161f831138e10958dcd88b9dc97038948f69, 15cb93d38b0a4bd931434a501d8308739326ce482da5158eb657b0af0fa7ba49, 6850788b9c76042e0e29a318f65fceb574083ed3ec39a34bc64a1292f4586b41, 6dcfe9f66d3aef1efd7007c588a59f69e5cd61b7a8eca1fb89a84b8ccef13a2b, 28c4a4df27f7ce8ced69476cc7923cf56625928a7b4530bc7b484eec67fe3943,

Attack Name	TYPE	VALUE
VoidLink	SHA256	e990a39e479e0750d2320735444b6c86cc26822d86a40d37d6e163d0fe058896, 4c4201cc1278da615bacf48deef461bf26c343f8cbb2d8596788b41829a39f3f
GOGITTER	URLs	hxxps[:]//d2i8rh3pkr4ltc[.]cloudfront[.]net/adobe_installation[.]php?file=Adobe_Acrobat_Reader_Installation_Setup, hxxps[:]//adobereader-upgrade[.]in/adobe_update[.]php?file=Adobe_Acrobat_Reader_Installation, hxxps[:]//adobecloud[.]site/adobe_installer[.]php?file=Adobe_Acrobat_Installer, hxxps[:]//adobe-acrobat[.]in/adobe_reader_setup[.]php?file=Adobe_Acrobat_Reader_Installation_Setup
CoolClient	MD5	F518D8E5FE70D9090F6280C68A95998F, 1A61564841BBBB8E7774CBBEB3C68D5D, AEB25C9A286EE4C25CA55B72A42EFA2C, 6B7300A8B3F4AAC40EEECFD7BC47EE7C
	SHA256	FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA, 941993f885957176d75f24ef3f8935ecb589bb9b445bb0d71fb18b65e61b6ee4
	Domains	account[.]hamsterxnxx[.]com, popnike-share[.]com, japan[.]Lenovoappstore[.]com
Tsundere Bot	IPv4	85[.]236[.]25[.]119
XWorm	SHA256	bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99, 441c49b6338ba25519fc2cf1f5cb31ba51b0ab919c463671ab5c7f34c5ce2d30
	IPv4	80[.]64[.]19[.]148, 85[.]208[.]84[.]208, 178[.]16[.]52[.]242, 94[.]159[.]113[.]64

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-13915</td><td>  </td><td rowspan="2">IBM API Connect V10.0.8.0 - V10.0.8.5, V10.0.11.0</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:ibm:api_connect:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">IBM API Connect Authentication Bypass Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-305</td><td>T1556: Modify Authentication Process, T1136: Create Account, T1190: Exploit Public-Facing Application</td><td>https://www.ibm.com/support/pages/node/7255149</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-0625	✗	D-Link DSL-526B (versions <= 2.01), D-Link DSL-2640B (versions <= 1.07), D-Link DSL-2740R (versions < 1.17), D-Link DSL-2780B (versions <= 1.01.14)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:dlink:dsl:*:*:*:*:*:*:*:*	DNSChanger, GhostDNS
D-Link DSL Gateway Command Injection via DNS Configuration Endpoint Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584.002: DNS Server	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-37164	✗	HPE OneView (Before 11.0)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:hpe:oneview:*:*:*:*:*:*:*:*	-
Hewlett Packard Enterprise OneView Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US, https://myenterpriselicense.hpe.com/cwp-ui/product-details/HPE_OV_CVE_37164_Z7550-98077/-/sw_free, https://support.hpe.com/connect/s/softwaredetails?collectionId=MTX-64daeb5ed0df44a0&tab=releaseNotes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20805		Windows 10 - 11 25H2, Windows Server 2012, 2016, 2019, 2025, 2022	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Desktop Window Manager Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059.006: Python, T1082: System Information Discovery, T1588.007: Artificial Intelligence	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-20805

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21265	✗	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2025, 2022, 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1329	T1542: Pre-OS Boot, T1553: Subvert Trust Controls	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21265

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-31096	✗	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation, T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-31096

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-64155</td><td>✗</td><td rowspan="2">Fortinet FortiSIEM (7.4.0, 7.3.0-7.3.4, 7.2.0-7.2.6, 7.1.0-7.1.8, 7.0.0-7.0.4, 6.7.0-6.7.10)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Fortinet FortiSIEM OS Command Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-25-772</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-23550</td><td>✗</td><td rowspan="2">Modular DS Modular Connector (Before 2.5.2)</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:modulards:modular_connector:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">WordPress Modular DS Privilege Escalation Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-284</td><td>T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1098: Account Manipulation</td><td>https://help.modulards.com/en/article/modular-ds-security-releases-modular-connector-260-and-252-dm3mv0/</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-20045</td><td>  </td><td rowspan="2">Cisco Unified Communications Manager, Unified Communications Manager Session Management Edition, Unified Communications Manager IM & Presence Service, Unity Connection, Webex Calling Dedicated Instance: versions before 14SU5, 15SU4</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:cisco:unified_communications_manager:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unified_communications_manager_im_and_presence_service:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unity_connection:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:webex_calling_dedicated_instance:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco Unified Communications Products Code Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20393		Cisco Secure Email Gateway (SEG): Versions prior to 15.0.5-016, 15.5.4-012, 16.0.4-016 Cisco Secure Email and Web Manager (SEWM): Versions prior to 15.0.2-007, 15.5.4-007, 16.0.4-010	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:-:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*:*:*	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21509		Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	-
Microsoft Office Security Feature Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-807	T1566: Phishing, T1204: User Execution, T1559: Inter-Process Communication, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-24061</td><td>  </td><td rowspan="2">GNU InetUtils telnetd versions 1.9.3 - 2.7</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:gnu:inetutils:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">GNU InetUtils Argument Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-88</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1098: Account Manipulation, T1082: System Information Discovery</td><td>https://codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b , https://codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc , https://cgit.git.savannah.gnu.org/cgit/inetutils.git</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-24858</td><td>  </td><td rowspan="2">Fortinet FortiOS (Before 7.0.19, 7.2.13, 7.4.11, 7.6.6) Fortinet FortiManager (Before 7.0.16, 7.2.13, 7.4.10, 7.6.6) Fortinet FortiAnalyzer (Before 7.0.16, 7.2.12, 7.4.10, 7.6.6) Fortinet FortiProxy (7.0, 7.2, Before 7.4.13, 7.6.6)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-288</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1136: Create Account, T1005: Data from Local System</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-060 , https://docs.fortinet.com/upgrade-tool/fortigate</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-1281</td><td>✗</td><td rowspan="2">Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior</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:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td>Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability</td><td>✓</td><td></td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-1340</td><td>✗</td><td rowspan="2">Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior</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:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GlassWorm	GlassWorm is a self-propagating supply chain malware discovered in late 2025 that targets Visual Studio Code extensions by injecting "invisible" Unicode characters to hide malicious code from human reviewers. It utilizes the Solana blockchain for an "unkillable" command-and-control (C2) infrastructure, ensuring it remains active even if servers are taken down.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential theft, remote control	macOS
Worm			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VVS Stealer	VVS Stealer is a Python-based information-stealing malware targeting Discord users to exfiltrate credentials, tokens, and browser data. It uses PyArmor obfuscation to evade static and signature-based detection and is distributed as a PyInstaller executable requiring no external dependencies. Core capabilities include Discord token theft, session hijacking via JavaScript injection, browser credential harvesting, screenshot capture, and persistence through the Windows Startup folder.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Account compromise, Privacy loss, Credential exposure	Windows
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
DNSChanger	DNSChanger operates by modifying DNS server settings to redirect systems to attacker-controlled servers instead of legitimate ISP or organizational DNS servers. It is distributed using steganography techniques and, rather than directly infecting the PC, primarily compromises unsecured routers once introduced into the environment.	Exploiting Vulnerability	CVE-2026-0625
		IMPACT	**AFFECTED PLATFORMS**
TYPE		Traffic redirection, Persistent compromise, Surveillance	D-Link DSL-2740R, D-Link DSL-2640B, D-Link DSL-2780B, D-Link DSL-526B
Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
-			EOL

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GhostDNS	GhostDNS scans for router IP addresses using weak or no passwords, accesses their settings, and replaces the default DNS configuration with attacker-controlled servers.	Exploiting Vulnerability	CVE-2026-0625
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Network-wide compromise, Credential theft, Service disruption	D-Link DSL-2740R, D-Link DSL-2640B, D-Link DSL-2780B, D-Link DSL-526B
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			EOL

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DCRat	DCRat is a Russian-linked remote access trojan capable of remote control, keylogging, and process injection, including process hollowing into legitimate binaries such as aspnet_compiler.exe.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Full remote control, Data exfiltration	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
GoBruteforcer	GoBruteforcer is a modular Go-based botnet that compromises Linux servers by brute-forcing weak credentials on internet-exposed services such as FTP, MySQL, PostgreSQL, and phpMyAdmin, spreading through a structured infection chain that includes web shells, downloaders, IRC bots, and dedicated brute-forcer modules.	Brute Force	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Server takeover, Data compromise, Credential theft	Linux
Botnet			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Astaroth (aka Guildma)	Astaroth banking malware has evolved to include WhatsApp-based worm propagation capabilities. This campaign abuses WhatsApp Web to harvest victim contact lists and distribute malicious ZIP archives containing obfuscated Visual Basic Script downloaders. The malware operates with dual functionality: a propagation module that sustains self-reinforcing infection loops through social engineering, and a banking module that silently monitors browsing activity to steal financial credentials when victims access banking URLs.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Banking credential theft, Stealthy persistence	WhatsApp
Banking Trojan			**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
RustyWater	RustyWater Rust-based RAT deployed by Iran's MuddyWater APT targeting diplomatic, maritime, financial, and telecom entities in the Middle East. Delivered via spear-phishing with malicious Word documents. Features anti-debugging, registry persistence, encrypted strings, and asynchronous C2 communication over HTTP/HTTPS. Represents MuddyWater's evolution from PowerShell/VBS loaders to modern compiled implants.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise, Espionage	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
MuddyWater			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RushDrop	RushDrop Linux dropper used by China-nexus APT UAT-7290 targeting telecommunications infrastructure in South Asia and Southeastern Europe. Contains three embedded binaries (DriveSwitch, SilentRaid, BusyBox) that it decodes and deploys after anti-VM checks. Also known as ChronosRAT. Initiates the infection chain for deeper network compromise and espionage operations.	-	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Initial Access, Malware Deployment	Linux
Dropper			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-7290			

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
DriveSwitch	DriveSwitch Peripheral Linux malware component deployed by UAT-7290 as part of the RushDrop infection chain. Its sole purpose is to execute the main SilentRaid implant on compromised systems. Acts as an intermediary executor between the dropper and the primary backdoor. Targets edge devices in telecom infrastructure.	Dropped by RushDrop dropper	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Malware Execution, Persistence	Linux
ASSOCIATED ACTOR			**PATCH LINK**
UAT-7290			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SilentRaid	SilentRaid is a C++ Linux backdoor (also called MystRodX) used by UAT-7290 for persistent access to telecom networks. Features plugin-based architecture supporting remote shell, port forwarding, file operations, and credential harvesting. Resolves C2 domains via Google DNS and performs anti-analysis checks. Primary implant for espionage operations against South Asian critical infrastructure.	Dropped and executed via RushDrop/DriveSwitch chain	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		System Compromise, Persistent Access, Espionage, Data Theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
UAT-7290			-

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
Bulbature	Bulbature is a Linux implant first disclosed in late 2024, used to convert compromised edge devices into Operational Relay Boxes (ORBs). Deployed by China-nexus actors including UAT-7290 to create proxy infrastructure for offensive operations. Has compromised over 75,000 hosts across 139 countries. Supports reverse shell capabilities and dynamic C2 switching.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		System compromise	Linux
ASSOCIATED ACTOR			**PATCH LINK**
UAT-7290			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an Open-source Windows RAT ranked 6th most prevalent malware globally in 2024. Distributed via phishing using Dropbox URLs, TryCloudflare tunnels, and malicious attachments. Capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment. Its modular architecture has spawned numerous variants like VenomRAT and NonEuclid RAT.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		System Compromise, Credential Theft	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
VoidLink	VoidLink is an advanced cloud-native Linux malware framework written in Zig, discovered December 2025, developed by Chinese-affiliated actors. Designed for long-term stealth access to AWS, GCP, Azure, Alibaba, Tencent, Kubernetes, and Docker environments. Features 37 plugins for reconnaissance, credential harvesting, lateral movement, and anti-forensics. Targets software engineers for potential supply chain attacks.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Malware framework		System compromise, Espionage	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSLITE	LOTUSLITE is a C++ backdoor designed for covert espionage operations, communicating with a hard-coded, IP-based command-and-control server to receive instructions and exfiltrate collected data. While its functionality remains deliberately minimal, it supports essential remote tasking and data theft capabilities, complemented by a reliable persistence mechanism that allows it to survive system reboots.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Data Theft, System Compromise	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
Evelyn Stealer	Evelyn Stealer is a data-harvesting malware tailored to siphon sensitive information from developer environments, with a particular focus on credentials and cryptocurrency-related assets. Once deployed, it gathers detailed system information and abuses DLL injection to extract browser-stored credentials, while also stealing files, clipboard contents, and saved Wi-Fi credentials. The malware further expands its capabilities by capturing screenshots and targeting cryptocurrency wallets, enabling comprehensive data theft, with all stolen data exfiltrated to attacker-controlled infrastructure over FTP.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Amnesia RAT	Amnesia RAT is a multifunctional remote access trojan designed for large-scale data theft and sustained system surveillance. It targets browser credentials and active sessions, Telegram Desktop accounts, seed phrases exposed via files or clipboard activity, application data from platforms such as Discord and Steam, and cryptocurrency wallets and financial assets. In parallel, the malware gathers system intelligence and enables real-time monitoring through screen, audio, and activity capture, while also supporting process control and strong persistence. This combination of credential theft, session hijacking, financial targeting, and continuous surveillance allows attackers to achieve full account takeover, identity abuse, and launch follow-on compromise campaigns.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Microsoft Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GOGITTER	GOGITTER is a newly identified, downloader developed in Golang that retrieves malicious payloads from a private GitHub repository controlled by threat actors. Designed as a 64-bit executable, the malware operates quietly on infected systems, first checking for the presence of a VBScript file named windows_api.vbs across specific system locations before proceeding with its operations.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Downloads additional payloads	Windows
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GITSHELLPAD	GITSHELLPAD is a newly discovered backdoor developed in Golang that uses private GitHub repositories as its command-and-control (C2) channel, allowing attackers to blend malicious traffic with legitimate GitHub activity. Once deployed, the malware registers the compromised system with the operator's infrastructure and continuously polls the repository for instructions, enabling remote command execution and ongoing control over the victim machine. To manage infected hosts, the backdoor leverages GitHub's REST API to automatically create uniquely named directories within an attacker-controlled repository, effectively organizing victims and facilitating discreet command exchange through a trusted platform.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
Backdoor			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
GOSHELL	GOSHELL is a Golang-based shellcode loader designed to deploy a Cobalt Strike Beacon on targeted systems whose hostnames are hardcoded within the malware, ensuring execution only on selected machines. The loader retrieves payloads packaged in RAR archives, extracts them using system utilities such as tar, and removes the tools afterward to minimize forensic traces, while the primary deployed component functions as the main backdoor for continued access.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Loads additional payloads	Windows
Loader			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SHEETCREEP	SHEETCREEP is a lightweight C#-based backdoor that abuses Google Sheets as its command-and-control (C2) channel, allowing attackers to discreetly send commands and receive data through a trusted cloud service. The malware is typically delivered in a ZIP archive containing a malicious shortcut (LNK) file and a payload disguised as a PNG image, tricking users into executing the file while concealing its true purpose. Once triggered, the backdoor establishes communication with attacker-controlled resources via Google Sheets, enabling remote command execution and persistent access while blending malicious activity with legitimate network traffic.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
Backdoor			
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
FIREPOWER	FIREPOWER is a PowerShell-based backdoor, designed to provide attackers with persistent remote access to compromised systems. Once executed, the malware generates a unique victim identifier using the format ComputerName==Username, allowing operators to track infected hosts, and then establishes communication with a Firebase Realtime Database used as its command-and-control channel. Through this setup, attackers can remotely issue commands, manage infected machines, and maintain ongoing control while blending malicious traffic with legitimate cloud service communications.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Execute commands, System compromise	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MAILCREEP	MAILCREEP is a Golang-based backdoor that abuses the Microsoft Graph API to establish its command-and-control (C2) channel, allowing attackers to communicate with compromised systems through legitimate Microsoft cloud services.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
Backdoor			
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
CoolClient	CoolClient is a backdoor commonly delivered with encrypted loader components containing configuration data, shellcode, and in-memory DLL modules executed through DLL sideloading using legitimate signed applications. Once deployed, it collects key system and user information such as host details, operating system version, memory size, network identifiers, user accounts, and loaded driver data to profile the compromised environment. Both older and newer variants support functions including file upload and deletion, keylogging, TCP tunneling, reverse proxy capabilities, and in-memory plugin execution for further payload delivery. The latest version adds clipboard monitoring to capture copied data and introduces the ability to extract HTTP proxy credentials from network traffic, while primarily using TCP for command-and-control communications with optional UDP support for flexibility.		-
		IMPACT	AFFECTED PRODUCTS
TYPE			Microsoft Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Mustang Panda		Steal Data, System Compromise	-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Tsundere Bot	Tsundere Bot is a newly identified malware family that combines loader and backdoor capabilities, enabling attackers to deploy additional payloads while maintaining remote access to compromised systems. Analysis of its infrastructure revealed control panels labeled “Tsundere Netto” and “Tsundere Reborn,” from which the malware derives its name. The bot requires Node.js to operate on infected machines, with installers generated directly from the command-and-control panel and delivered as MSI packages or PowerShell scripts.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE			Windows
Bot			
ASSOCIATED ACTOR		Steal Data, Execute Script	PATCH LINK
TA584			-

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">XWorm</td><td rowspan="5">XWorm is a remote access trojan (RAT) active since 2022 that provides attackers with extensive remote control over compromised systems while also incorporating limited ransomware capabilities. Sold on underground forums and widely adopted by threat actors with varying skill levels, the malware is frequently used in opportunistic campaigns to steal data and maintain persistent access across infected environments.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>RAT</td><td rowspan="3">Remote Control</td><td rowspan="2">Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>TA584</td><td>-</td></tr>
</table>

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
APT36 (aka Transparent Tribe, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134)	Pakistan	Government, Academic	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1112: Modify Registry; T1055: Process Injection; T1036: Masquerading; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1202: Indirect Command Execution; T1497: Virtualization/Sandbox Evasion; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1555: Credentials from Password Stores; T1539: Steal Web Session Cookie; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1113: Screen Capture; T1115: Clipboard Data; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1565.001: Stored Data Manipulation; T1047: Windows Management Instrumentation

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, G0069)</td><td>Iran</td><td rowspan="3">Diplomatic, Maritime, Financial, and Telecom Entities</td><td rowspan="3">Middle East</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>RustyWater</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; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1106: Native API; T1047: Windows Management Instrumentation; T1620: Reflective Code Loading; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1027: Obfuscated Files or Information; T1036: Masquerading; T1055: Process Injection; T1082: System Information Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-7290	China	Critical Infrastructure, Telecommunications	South Asia, Southeastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RushDrop, DriveSwitch, SilentRaid, Bulbature	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; TA0043: Reconnaissance; TA0042: Resource: Development; T1595: Active Scanning; T1587: Develop Capabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1110: Brute Force; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1027: Obfuscated Files or Information; T1497: Virtualization/Sandbox Evasion; T1140: Deobfuscate/Decode Files or Information; T1564: Hide Artifacts; T1027.002: Software Packing; T1552: Unsecured Credentials; T1082: System Information Discovery; T1016: System Network Configuration: Discovery; T1083: File and Directory Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1132: Data Encoding; T1573: Encrypted Channel; T1090: Proxy; T1572: Protocol Tunneling; T1041: Exfiltration Over C2 Channel; T1595.002: Vulnerability: Scanning; T1587.001: Malware; T1588.005: Exploits; T1110.001: Password Guessing; T1059.004: Unix Shell; T1497.001: System Checks; T1564.001: Hidden Files and Directories; T1552.001: Credentials In Files; T1071.001: Web Protocols; T1573.002: Asymmetric Cryptography; T1090.002: External Proxy; T1588.006: Vulnerabilities		

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Mustang Panda (aka HoneyMyte, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)</td><td>China</td><td rowspan="2">Government</td><td rowspan="2">Myanmar, Mongolia, Malaysia, Russia, Pakistan</td></tr>
<tr><td>MOTIVE
Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>CoolClient</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1543: Create or Modify System Process; T1543.003: Windows Service; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1056: Input Capture; T1056.001: Keylogging; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1083: File and Directory Discovery; T1115: Clipboard Data; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service; T1090: Proxy; T1070: Indicator Removal; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1569: System Services; T1489: Service Stop</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
TA584</td><td>-</td><td rowspan="3">Healthcare, Government, Financial Services, Education, Business Services, Hospitals, Technology, Retail, Insurance, Construction, Automotive</td><td rowspan="3">Antigua and Barbuda, Bahamas, Barbados, Belize, Canada, Costa Rica, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, United States, United Kingdom, Ireland, Germany, Australia</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCT</th></tr>
<tr><td>-</td><td>Tsundere Bot, XWorm</td><td>Windows</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0042: Resource Development; T1566: Phishing; T1566.002: Spearphishing Link; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1055: Process Injection; T1055.012: Process Hollowing; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub_Technique
TA0001: Initial Access	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1195: Supply Chain Compromise	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	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
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub_Technique
TA0003: Persistence	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location

Tactic	Technique	Sub_Technique
TA0005: Defense Evasion	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.007: Msiexec
		T1218.010: Regsvr32
		T1218.011: Rundll32
	T1497: Virtualization/Sandbox Evasion	
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1620: Reflective Code Loading	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.005: Cached Domain Credentials
		T1003.002: Security Account Manager
		T1003.003: NTDS

Tactic	Technique	Sub_Technique
TA0006: Credential Access	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.005: Password Managers
		T1555.003: Credentials from Web Browsers
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	T1518.001: Security Software Discovery
		T1614.001: System Language Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.006: Windows Remote Management
	T1210: Exploitation of Remote Services	

Tactic	Technique	Sub_Technique
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1113: Screen Capture	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1011: Exfiltration Over Other Network Medium	
	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.002: External Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1568.003: DNS Calculation

Tactic	Technique	Sub_Technique
TA0040: Impact	T1489: Service Stop	
	T1496: Resource Hijacking	
	T1490: Inhibit System Recovery	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1485: Data Destruction	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.005: Botnet
		T1583.006: Web Services
	T1584: Compromise Infrastructure	
	T1608: Stage Capabilities	
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.004: Digital Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
TA0043: Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning

Top 5 Takeaways

#1

In January, there were eight zero-day vulnerabilities, with the standout "celebrity" vulnerability, **Ni8mare** (CVE-2026-21858), taking center stage. Meanwhile, **CVE-2026-20045** is being actively exploited to target Cisco Unified Communications products, allowing attackers to execute arbitrary code on internet-facing deployments.

#2

Supply chain and platform-abuse attacks are on the rise, with sophisticated malware like **GlassWorm** targeting Visual Studio Code extensions using invisible Unicode characters and blockchain-based C2 infrastructure. As attackers increasingly leverage legitimate platforms for malicious purposes, organizations must strengthen code review processes, enhance endpoint detection, and monitor for anomalous network behavior.

#3

Cyberattacks hit **196** countries in January, with **Turkey, Cyprus, Qatar, Bahrain,** and **Slovenia** facing the brunt of the threats. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region was immune as adversaries expanded their reach globally across the Middle East, Europe, and beyond.

#4

The **Government, Technology, Telecommunications, Financial Services,** and **Human Resources** sectors were prime targets, with data theft, espionage campaigns, and sophisticated backdoors wreaking havoc. As attackers refine their tactics using cloud-native malware and legitimate API abuse, organizations in these industries must stay ahead with proactive security measures.

#5

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **GlassWorm, VoidLink, Astaroth, RustyWater, AsyncRAT, CoolClient, Tsundere Bot, and XWorm.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **16 significant vulnerabilities** and block the indicators related to the **5 active threat actors, 26 active malware,** and **164 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 **16 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
VVS Stealer	SHA256	307d9cefa7a3147eb78c69eded273e47c08df44c2004f839548963268d19dd87, 7a1554383345f31f3482ba3729c1126af7c1d9376abb07ad3ee189660c166a2b, c7e6591e5e021daa30f949a6f6e0699ef2935d2d7c06ea006e3b201c52666e07
DCRat	SHA256	91696f9b909c479be23440a9e4072dd8c11716f2ad3241607b542b202ab831ce, bf374d8e2a37ff28b4dc9338b45bbf396b8bf088449d05f00aba3c39c54a3731, 11c1cfce546980287e7d3440033191844b5e5e321052d685f4c9ee49937fa688
GoBruteforcer	SHA256	ab468da7e50e6e73b04b738f636da150d75007f140e468bf75bc95e8592468e5, 4fbea12c44f56d5733494455a0426b25db9f8813992948c5fbb28f38c6367446
Astaroth	SHA256	bb0f0be3a690b61297984fc01befb8417f72e74b7026c69ef262d82956df471e, 9081b50af5430c1bf5e84049709840c40fc5fdd4bb3e21eca433739c26018b2e
RustyWater	SHA256	03457a4428dfe510acc1f147d54a2000a658d562d0edcff2b5ff0897cf6ea516, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79
SilentRaid	SHA256	723c1e59accbb781856a8407f1e64f36038e324d3f0bdb606d35c359ade08200, 59568d0e2da98bad46f0e3165bcf8adadbf724d617ccebcfdaeafbb097b81596, 961ac6942c41c959be471bd7eea6e708f3222a8a607b51d59063d5c58c54a38d
AsyncRAT	SHA256	eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286,

Attack Name	TYPE	VALUE
AsyncRAT	SHA256	c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd, 02aa8cabeea2a0120a31adbf0886f821d10953fc6d4d9cd1959568093c48b04d, 279b157c99432100bab17e6f23bd90cb397582324b091010d8cf1ec2683d3e4d, 6da6e608ba1bf369e01785d677c8fc95e551ee847d420a1be885677871a30134
VoidLink	SHA256	05eac3663d47a29da0d32f67e10d161f831138e10958dcd88b9dc97038948f69, 15cb93d38b0a4bd931434a501d8308739326ce482da5158eb657b0af0fa7ba49, 6850788b9c76042e0e29a318f65fceb574083ed3ec39a34bc64a1292f4586b41, 6dcfe9f66d3aef1efd7007c588a59f69e5cd61b7a8eca1fb89a84b8ccef13a2b, 28c4a4df27f7ce8ced69476cc7923cf56625928a7b4530bc7b484eec67fe3943, e990a39e479e0750d2320735444b6c86cc26822d86a40d37d6e163d0fe058896, 4c4201cc1278da615bacf48deef461bf26c343f8cbb2d8596788b41829a39f3f
LOTUSLITE	SHA256	2c34b47ee7d271326cfff9701377277b05ec4654753b31c89be622e80d225250
Evelyn Stealer	SHA256	aba7133f975a0788dd2728b4bbb1d7d948e50571a033a1e8f47a2691e98600c5, 92af258d13494f208ccf76f53a36f288060543f02ed438531e0675b85da00430
Amnesia	SHA256	359fe8df31c903153667fbe93795929ad6172540b3ee7f9eff4bcc1da6d08478
GOGITTER	URLs	hxxps[:]//d2i8rh3pkr4ltc[.]cloudfront[.]net/adobe_installation[.]php?file=Adobe_Acrobat_Reader_Installation_Setup, hxxps[:]//adobereader-upgrade[.]in/adobe_update[.]php?file=Adobe_Acrobat_Reader_Installation, hxxps[:]//adobecloud[.]site/adobe_installer[.]php?file=Adobe_Acrobat_Installer, hxxps[:]//adobe-acrobat[.]in/adobe_reader_setup[.]php?file=Adobe_Acrobat_Reader_Installation_Setup

Attack Name	TYPE	VALUE
GITSHELLPAD	SHA256	8f495603be80b513820a948d51723b616fac33f0f382fa4a141e39e12fff40cf, 6c60e5b28e352375d101eb0954fa98d229de3b94f22d5815af8948ebed1f44dd, af01c12019a3a3aa64e8a99d7231e0f2af6084298733bba3d7d41db13091cbac, 5d9b2e61ed45b6407b778a18ff87792265fa068d7c4580ae54fbf88af435679f, 95a2fb8b6c7b74a7f598819810ddb0a505f3d5cf392b857ff8e75c5a1401110e, fff79ce90b1af67e0b6d16a850e85861c948f988eda39ef46457241bbe3df170
	MD5	0d86b8039cffc384856e17912f308616, f454e2724a63cbbfda26daff1d8bb610, 10a7725f807056cb0383a1cae38d49b4, e26b3fece2fe296654406ef8045ffda1, f4813d65cd7246f716fcbd8f7fd3e63d, f2284f62625f117c57384b1c5b8b8f58
	SHA1	6a11c0e5f1d1e22e89b4921c7a371dbf9cf54709, 6036098059fa1311866ce6ad2723c4d0d1f00138, 54bfe1ffba8bff3571093ade5038dc98ef5f46ce, 6d1dbd92f7ed7381c7bfca681c3139daeab692f1, 3d48ab9567c6080471459b34dfc12c89418be8a2, 3c17dbf975af8eb7a67e6908f522c93c2c0662e5
GOSHELL	SHA256	a83d833f0c8dc0f7eaad65d93d7f3da2d905d83f9eefd420af8939b2e0e921a3
SHEETCREEP	MD5	87c7d69c6131406afdd0a08e89329d0a, 0729db72ab4ad9b2ac7a82918c744388, f9a2da8f12179414663a230f11edca20, 556a567a2c5c27a6aa5660e2e6bcce7b
	SHA1	a55c18a82203cf1efafac6f3c47642ab60c74ffc, daeeb031a9617e6f1b7bf4d85de9c75f62021c82, cdecfe8e1cacd1af204a5da52f6c02eb16fdea8b, e9d9d8c0c818ba9208e61eaf49af4c1b37f4eb59
	SHA256	b56062033df06738b66c38b3fa2f82a7e8c558336a4790c83c7faad595172167, 71794df37a107472e8d0829387741953f9e6c7778519b11f061c79ff6fb0f386, 9eebbf8899a1cf4156a872e9b8cde2a8f6ab364b80895505109384405c622cc58, bb11bea463ab1b976c3716591f93eccc71c1a2d1c389a371416b140cd8faa6f0

Attack Name	TYPE	VALUE
FIREPOWER	MD5	12669c29e00057abf20c73a434eb3dd2, cd5aab2b0f8d2b42e7a6537303d6345d, 0f7730a78490c61964b3bfc05eb59ea7, 119b836b4e1e7be8c3be8fe921f72bfb, 41a3752e6ea83d25731f22e1c17f59e2, 12669c29e00057abf20c73a434eb3dd2, e48f1000c86b93cf428a13a0b7384e0d
	SHA1	a38eab1ac01201b651b2efdebc78e994402976f1, e9eeda092500d7c7f278672d35f733e0e26f0e2c, ac06003a774af5a8e4be349fc6f0e65cea116370, e333ae0948ede0cf1368deec53a1eda18210e75e, aa9b4410004d43e4e5cc1fc2cda1956bc5663b03, a38eab1ac01201b651b2efdebc78e994402976f1, 8f9843607ff0ed83ca58e21612b41d6e744beb81
	SHA256	889b4b1e13b66aff349282eae3999783f5542f961b433a7d4653c5281e7f4d3e, 20d72c8580b4d5ef4f771c91ce1d1207e5416fa789d8216a73a0abb8e030644f, de14ca6d93dadbc1ec216700d76ad2d0e7b9ebceb95de68c631d0a1c01c915c4, 644dda0ea5db1eb5f07ccfccddb909c6ee57235c4465adbfc342da6867cdb71a, 309a39ba10cd7c7075837b63d247fa45764f5496fdae215e95a3f4b65ab6dfc3, 889b4b1e13b66aff349282eae3999783f5542f961b433a7d4653c5281e7f4d3e, 989ad43bb9e328d786664247c3af4c17be28932760113708a9c6de977d69652c
	URLs	hxxps[:]//webdevurl-cc389-default-rtdb[.]firebaseio[.]com, hxxps[:]//govs-services-in-default-rtdb[.]firebaseio[.]com, hxxps[:]//gov-service-in-default-rtdb[.]firebaseio[.]com
MAILCREEP	MD5	ed4dd29c57a38f2bb1934acbaeadeeba
	SHA1	7bc5d288ec260765a146136194d815ff3c697df8
	SHA256	a97cc81a2f7c05bfc498b71999176c2aeb6e3ad273e48eb1f5c1c5647419c642

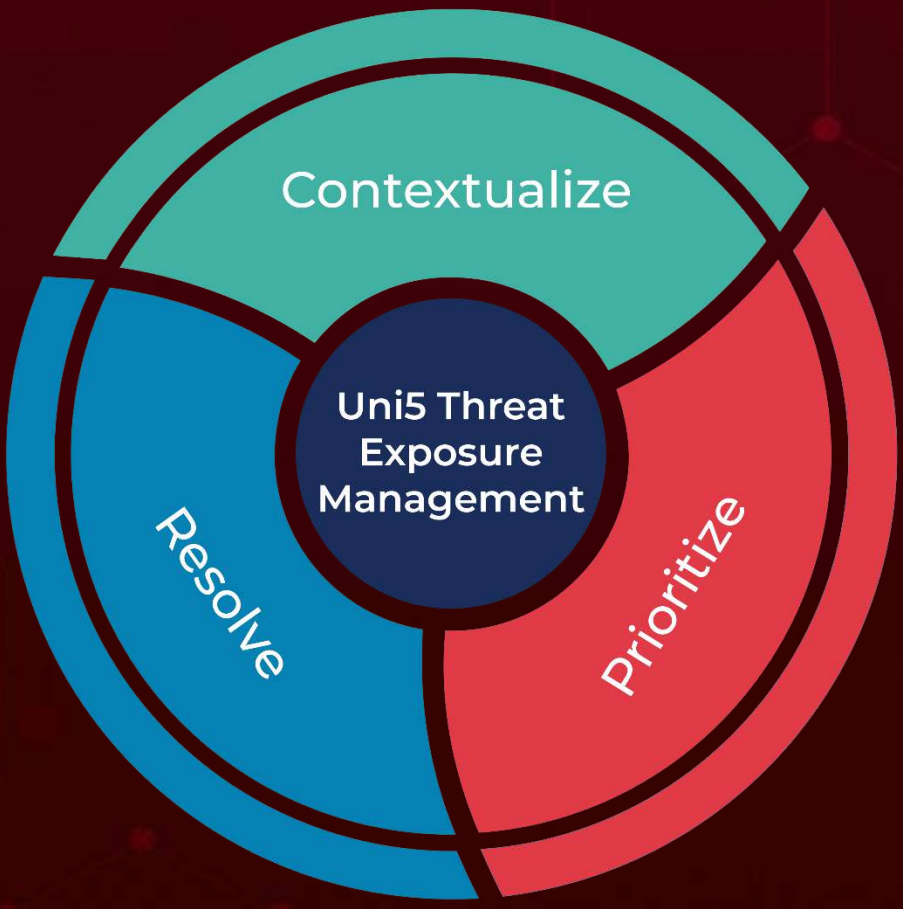
Attack Name	TYPE	VALUE
CoolClient	MD5	F518D8E5FE70D9090F6280C68A95998F, 1A61564841BBBB8E7774CBBEB3C68D5D, AEB25C9A286EE4C25CA55B72A42EFA2C, 6B7300A8B3F4AAC40EEECFD7BC47EE7C
	SHA256	FD434AC879122DEDB754BD4835822DBC185ACE3A3E75E5898FFB40C213A7C4BA, 941993f885957176d75f24ef3f8935ecb589bb9b445bb0d71fb18b65e61b6ee4
	Domains	account[.]hamsterxnxx[.]com, popnike-share[.]com, japan[.]Lenovoappstore[.]com
Tsundere Bot	IPv4	85[.]236[.]25[.]119
XWorm	SHA256	bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99, 441c49b6338ba25519fc2cf1f5cb31ba51b0ab919c463671ab5c7f34c5ce2d30
	IPv4	80[.]64[.]19[.]148, 85[.]208[.]84[.]208, 178[.]16[.]52[.]242, 94[.]159[.]113[.]64

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

February 2, 2026 • 11:30 PM

More at www.hivepro.com