Date of Publication
May 19, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

12 to 18 MAY 2025

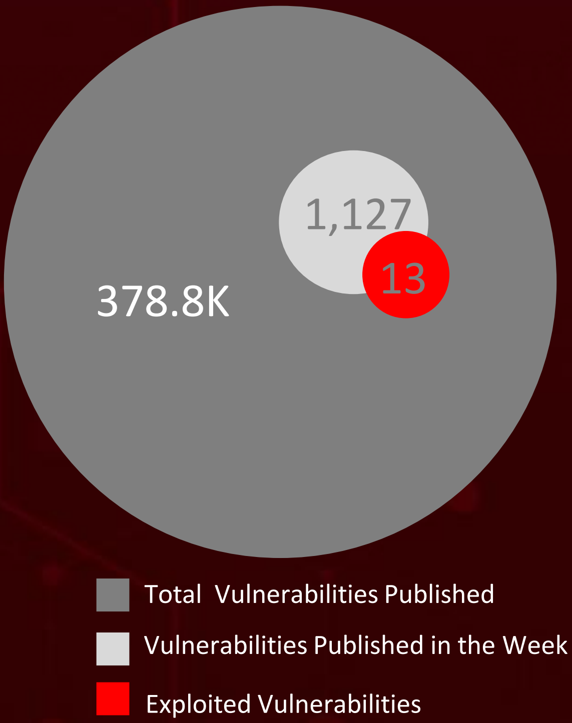
Table Of Contents

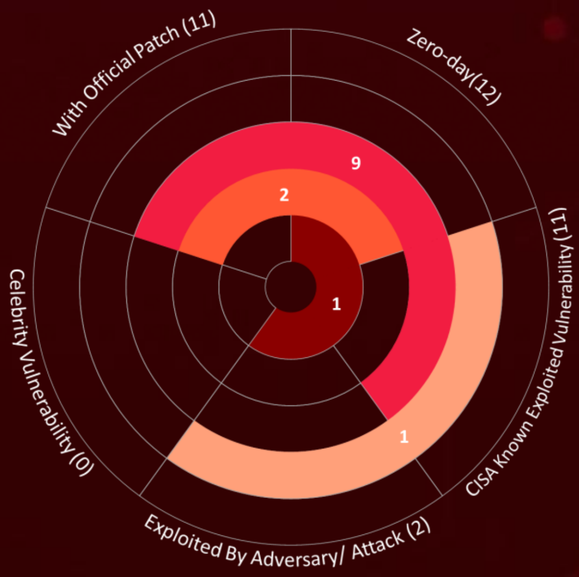
Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **seven** attacks, reported **thirteen** vulnerabilities, and identified **two** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Ivanti patched two critical **zero-days** in Endpoint Manager Mobile that allowed remote code execution and authentication bypass. **CVE-2025-4664** is a medium-severity Chrome zero-day that leaks cross-origin data via crafted pages, exposing sensitive tokens. Active exploitation requires user interaction; update Chrome now.

Additionally, **APT36** has intensified its cyber-espionage against India, leveraging geopolitical crises with precision attacks. Using phishing lures and advanced malware, they blend technical skill with psychological warfare. **CVE-2025-4632**, a critical path traversal flaw in Samsung MagicINFO 9 Server, is actively exploited for system access and Mirai botnet deployment. These rising threats pose significant and immediate dangers to users worldwide.





High Level Statistics

7
Attacks Executed

- Crimson
- Poseidon
- ElizaRAT
- PupkinStealer
- Mirai
- LZRD
- TransferLoader

13
Vulnerabilities Exploited

- CVE-2025-27920
- CVE-2024-11120
- CVE-2024-6047
- CVE-2025-32756
- CVE-2025-4632
- CVE-2025-4427
- CVE-2025-4428
- CVE-2025-30400
- CVE-2025-32701
- CVE-2025-32706
- CVE-2025-32709
- CVE-2025-30397
- CVE-2025-4664

2
Adversaries in Action

- APT36
- Marbled Dust

Insights

CVE-2025-32756 a critical buffer overflow in Fortinet is being actively exploited for remote attacks.

Supply Chain Attack: The rand-user-agent npm package was compromised to deliver a Remote Access Trojan, enabling attackers to steal data and execute remote commands.

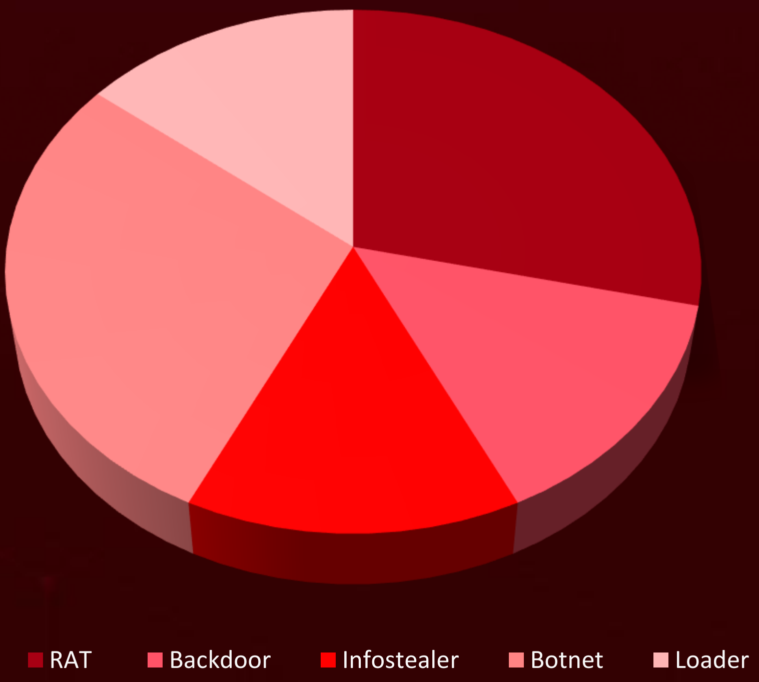
PoisonSeed is a phishing campaign that hijacks email platforms to spread crypto scams using seed phrase poisoning to steal wallets and drain funds.

Microsoft's May 2025 Patch Tuesday fixes 83 vulnerabilities, including **five zero-day** flaws are actively exploited in the wild, urging immediate updates to prevent exploitation.

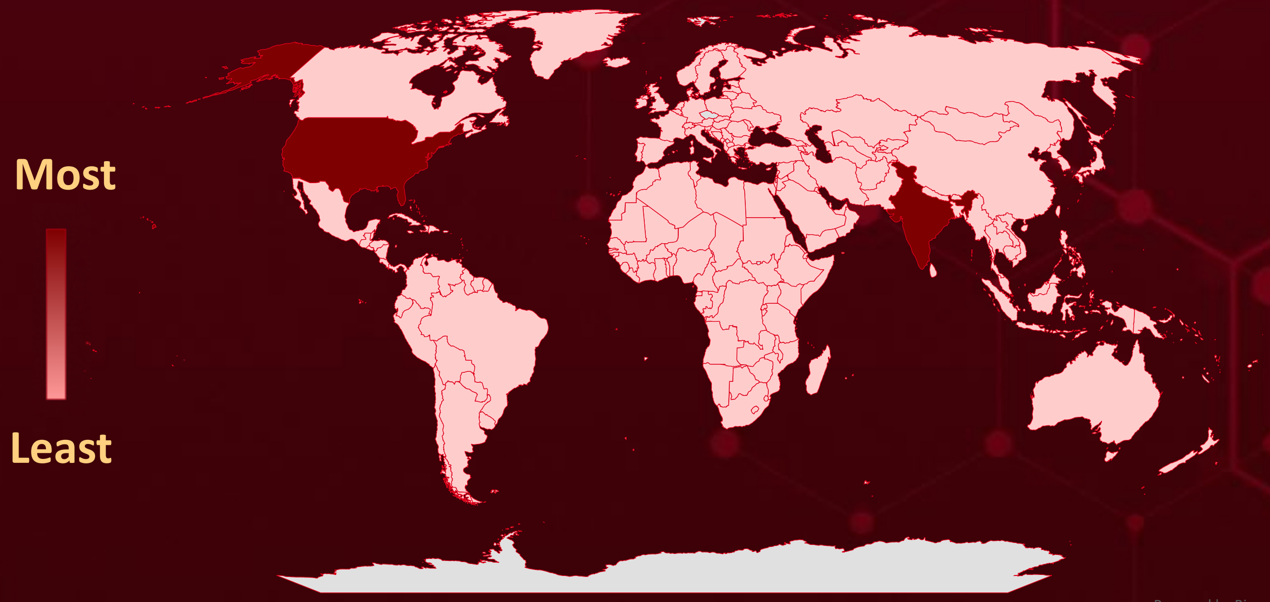
Türkiye-linked Marbled Dust exploited CVE-2025-27920 in Output Messenger to target Kurdish military systems.

TransferLoader is a modular malware loader using obfuscation and persistence to evade detection, linked to Morpheus ransomware attacks on U.S. law firms.

Threat Distribution



Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

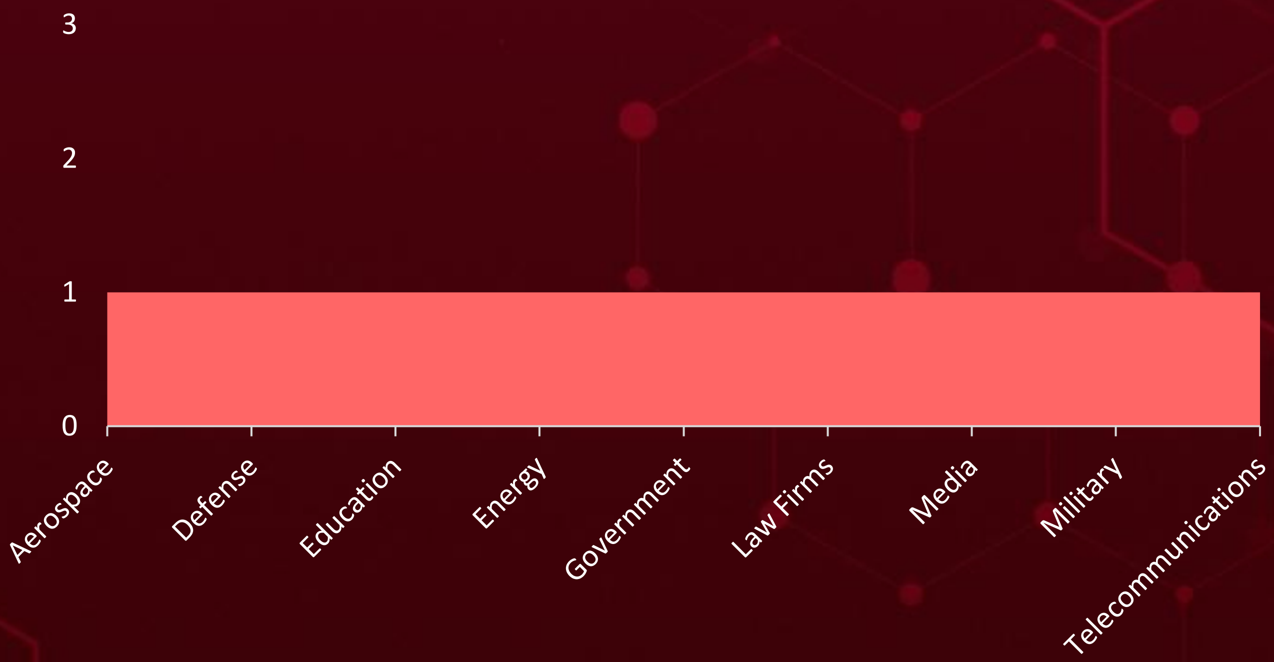
	Countries
🟥	United States
🟥	India
	Switzerland
	China
	Poland
	France
	Sweden
	Germany
	Tanzania
	Indonesia
	Ukraine
	Jordan
	Spain
	Argentina
	Malta
	Austria
	Barbados
	Netherlands
	Belarus
	Sierra Leone
	Belgium
	United Arab Emirates
	Belize
	Madagascar
	Ethiopia

	Countries
	Benin
	Oman
	Bhutan
	Saint Lucia
	Bolivia
	South Sudan
	Bosnia and Herzegovina
	Tonga
	Botswana
	Malawi
	Brazil
	Mexico
	Brunei
	Myanmar
	Bulgaria
	Nigeria
	Burkina Faso
	Papua New Guinea
	Burundi
	Romania
	Cabo Verde
	Saudi Arabia
	Cambodia
	Solomon Islands
	Cameroon
	State of Palestine

	Countries
	Turkmenistan
	Chad
	Luxembourg
	Chile
	Maldives
	Albania
	Mauritania
	Colombia
	Moldova
	Comoros
	Morocco
	Congo
	Nauru
	Costa Rica
	Nicaragua
	Côte d'Ivoire
	North Macedonia
	Croatia
	Palau
	Cuba
	Peru
	Cyprus
	Qatar
	Czech Republic (Czechia)
	Denmark
	San Marino

	Countries
	Mongolia
	Rwanda
	Djibouti
	Serbia
	Dominica
	Slovakia
	Dominican Republic
	South Africa
	DR Congo
	Sri Lanka
	Ecuador
	Suriname
	Egypt
	Taiwan
	El Salvador
	Timor-Leste
	Equatorial Guinea
	Tunisia
	Eritrea
	Uganda
	Estonia
	Lithuania
	Malaysia
	Fiji
	Algeria
	Mauritius
	French Guiana

Targeted Industries



TOP MITRE ATT&CK TTPs

- **T1059** Command and Scripting Interpreter
- **T1190** Exploit Public-Facing Application
- **T1588** Obtain Capabilities
- **T1588.006** Vulnerabilities
- **T1068** Exploitation for Privilege Escalation
- **T1566** Phishing
- **T1588.005** Exploits
- **T1027** Obfuscated Files or Information
- **T1203** Exploitation for Client Execution
- **T1204** User Execution
- **T1204.001** Malicious Link
- **T1204.002** Malicious File
- **T1105** Ingress Tool Transfer
- **T1140** Deobfuscate/ Decode Files or Information
- **T1566.001** Spearphishing Attachment
- **T1133** External Remote Services
- **T1547** Boot or Logon Autostart Execution
- **T1036** Masquerading
- **T1195** Supply Chain Compromise
- **T1041** Exfiltration Over C2 Channel

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crimson	Crimson Malware is a remote access trojan used by APT36 to spy on Indian government and military entities. It steals data, monitors activity, and spreads via phishing emails with malicious attachments.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote Control, Data Theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
APT36			-

IOC TYPE	VALUE
SHA256	d1a1eaefe6bd2e245bba369e966d7a8eab9ed6ad1fa827321e5889cc8d43f976
MD5	026e8e7acb2f2a156f8afff64fd54066, fb64c22d37c502bde55b19688d40c803, 70b8040730c62e4a52a904251fa74029, 3efec6ffcbfe79f71f5410eb46f1c19e

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
Poseidon	Poseidon is a powerful Linux backdoor used by APT36 to infiltrate Indian government and defense networks, steal sensitive data, and maintain remote control over compromised systems, often delivered through trojanized versions of the Kavach authentication tool.	Kavach 2FA tool	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Compromise systems	Linux
ASSOCIATED ACTOR			**PATCH LINK**
APT36			-

IOC TYPE	VALUE
SHA256	541cefaad8d9554bdc5ce9cde24e4556c2444111ea13bd9965bd4a50e60f9265, 682d5e53a456668f15809d9ab499651e1342fc602e7f5bc85e30fe29933f7634, 7e2020c4a838bd7463478188bfaa97e66cf3365d3aef03f1b4398eaddacfc6b9

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ElizaRAT	ElizaRAT is a remote access trojan (RAT) targeting Windows systems, first identified in 2024. It is primarily spread through phishing emails and malicious attachments. The malware enables attackers to steal credentials, capture screenshots, and remotely control infected devices.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote Control, Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	b30a9e31b0897bfe6ab80aebcd0982eecf68e9d3d3353c1e146f72195cef0ef5, 263f9e965f4f0d042537034e33699cf6d852fb8a52ac320a0e964ce96c48f5e5

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
PupkinStealer	PupkinStealer is a lightweight but dangerous malware that quietly steals browser passwords, Telegram and Discord session data, desktop files, and screenshots. Once executed, it zips up the stolen info and exfiltrates it via a Telegram bot, making it a stealthy threat aimed at quick data theft and account hijacking.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Infostealer		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	9309003c245f94ba4ee52098dadbaa0d0a4d83b423d76c1bfc082a1c29e0b95f
MD5	fc99a7ef8d7a2028ce73bf42d3a95bce

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mirai	Mirai is a well-known malware that targets Internet of Things (IoT) devices by exploiting weak or default passwords. Once infected, these devices are added to a botnet to carry out large-scale Distributed Denial of Service (DDoS) attacks. Its open-source release has led to the creation of several variants.	Exploiting vulnerabilities	CVE-2024-11120 CVE-2024-6047
TYPE		IMPACT	AFFECTED PRODUCT
Botnet		Network Overload, Compromise systems	GeoVision Devices
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714, 11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114, 8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e, ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516, 03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3

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
LZRD	LZRD is a Mirai-based malware botnet variant that actively exploits vulnerabilities in GeoVision IoT devices and other platforms to infect and control large numbers of devices. It uses command injection attacks to download and execute its payload, enabling a range of DDoS attack methods.	Exploiting vulnerabilities	CVE-2024-11120 CVE-2024-6047
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Botnet		Network Overload, Compromise systems	GeoVision Devices
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TransferLoader	TransferLoader is a sophisticated malware loader active since at least February 2025, featuring embedded components like a downloader, backdoor, and backdoor loader. It enables attackers to execute arbitrary commands, deploy additional payloads such as ransomware, and evade detection through advanced anti-analysis techniques.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Malware execution, Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	b55ba0f869f6408674ee9c5229f261e06ad1572c52eaa23f5a10389616d62efec3

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-27920</td><td>✗</td><td rowspan="2">Output Messenger before 2.0.63</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✓</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>CISA KEV</b></td><td rowspan="2">cpe:2.3:a:output_messenger:out_put_messenger:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Output Messenger Directory Traversal Vulnerability</td><td>✗</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-22</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application</td><td>https://www.outputmessenger.com/cve-2025-27920/</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-2024-11120</td><td>✗</td><td rowspan="2">GeoVision VS12
GeoVision VS11
GeoVision DSP_LPR_V3
GeoVision LX 4 V2
GeoVision LX 4 V3</td><td rowspan="2">-</td></tr>
<tr><th>ZERO-DAY</th></tr>
<tr><td>✓</td><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">Mirai, LZRD</td></tr>
<tr><td rowspan="3">GeoVision Devices OS Command Injection Vulnerability</td><td>✓</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-78</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application</td><td>-</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-6047	✗	GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*	Mirai, LZRD
GeoVision Devices OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32756	✗	FortiCamera Version 2.1.0 through 2.1.3 FortiCamera 2.0 All Versions FortiCamera 1.1 All Versions FortiMail Version 7.6.0 through 7.6.2 FortiMail Version 7.4.0 through 7.4.4 FortiMail Version 7.2.0 through 7.2.7 FortiMail Version 7.0.0 through 7.0.8 FortiNDR Version 7.6.0 FortiNDR Version 7.4.0 through 7.4.7 FortiNDR Version 7.2.0 through 7.2.4 FortiNDR 7.1 All Versions FortiNDR Version 7.0.0 through 7.0.6 FortiNDR 1.1 – 1.5 All Versions FortiRecorder Version 7.2.0 through 7.2.3 FortiRecorder Version 7.0.0 through 7.0.5 FortiRecorder Version 6.4.0 through 6.4.5 FortiVoice Version 7.2.0 FortiVoice Version 7.0.0 through 7.0.6 FortiVoice Version 6.4.0 through 6.4.10	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortivoice:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortirecorder:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortindr:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:forticamera:*:*:*:*:*:*:*:*	-
Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-121	T1059: Command and Scripting Interpreter;
		T1068: Exploitation for Privilege Escalation;
		T1053.003: Scheduled Task/Job: Cron
			https://fortiguard.fortinet.com/psirt/FG-IR-25-254

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4632	✗	Samsung MagicInfo 9 Server Versions prior to 21.1052	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:samsung:magicinfo_9_server:*:*:*:*:*:*:*:*	-
Samsung MagicINFO 9 Server Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://eu.community.samsung.com/t5/samsung-solutions/update-magicinfo-server-v9-21-1052-0-setup-file/ta-p/11374265

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4427	✗	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4428	✗	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30400	✗	Windows: 10 21H2 - 11 24H2 Windows Server: 2012 Gold - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Microsoft DWM Core Library Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32701	✗	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Windows Common Log File System Driver Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32701

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32706	✗	Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Windows Common Log File System Driver Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32706

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32709	✗	Windows: 10 21H2 - 11 24H2 Windows Server: 2012 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-327069

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30397	✗	Windows: 10 - 11 Windows Server: 2008 - 2025 Microsoft Internet Explorer: 11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_internet_explorer:-:*:*:*:*:*:*:*	-
Scripting Engine Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter; T1204.001: User Execution: Malicious Link; T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4664	✗	Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium Loader Insufficient Policy Enforcement Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-346	T1528: Steal Application Access Token; T1189 : Drive-by Compromise; T1204: User Execution	https://www.google.com/intl/en/chrome/?standalone=1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT36 (alias Mythic Leopard, Transparent Tribe, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156)	Pakistan	Government, Military, Defense, Aerospace, Education, Media, Energy, Telecommunications	India
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Crimson RAT, Poseidon, ElizaRAT	Windows, Linux, Android

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1598: Phishing for Information; T1070: Indicator Removal; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1430: Location Tracking; T1409: Stored Application Data; T1115: Clipboard Data; T1573: Encrypted Channel; T1071: Application Layer Protocol; T1598.003: Spearphishing Link; T1583.001: Domains; T1566.001: Spearphishing Attachment; T1204.001: Malicious Link; T1059.005: Visual Basic; T1547.001: Registry Run Keys /Startup Folder; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery: T1083: File and Directory Discovery; T1005: Data from Local: System; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel; T1218.005: Mshta; T1071.001: Web Protocols; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1036.005: Match Legitimate Name or Location; T1070.004: File Deletion; T1056.001: Keylogging; T1583: Acquire Infrastructure; T1027.013: Encrypted/Encoded File; T1566.002: Spearphishing Link; T1608.004: Drive-by Target; T1608: Stage Capabilities

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Marbled Dust (alias Silicon, Cosmic Wolf, Sea Turtle, Teal Kurma, UNC1326)	Turkey	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2025-27920	-	Output Messenger
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA0042: Resource Development; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1037: Boot or Logon Initialization Scripts; T1036: Masquerading; T1212: Exploitation for Credential Access; T1046: Network Service Discovery; T1071.004: DNS; T1041: Exfiltration Over C2 Channel; T1082: System Information Discovery; T1027: Obfuscated Files or Information; T1587.004: Exploits; T1574: Hijack Execution Flow; T1587: Develop Capabilities			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **thirteen exploited vulnerabilities** and block the indicators related to the threat actors **APT36, Marbled Dust,** and malware **Crimson, Poseidon, ElizaRAT, PupkinStealer, Mirai, LZRD, TransferLoader.**

Uni5 Users

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

- Running a Scan to discover the assets impacted by the **thirteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT36,** and malware **Crimson, PupkinStealer, Mirai, TransferLoader** in Breach and Attack Simulation(BAS).

Threat Advisories

APT36's Dark Playbook: Crimson Codes and Crisis Lures Strike India

Popular npm Package ‘rand-user-agent’ Compromised in Supply Chain Attack

PupkinStealer: The Silent Thief Hiding in Plain Sight

Hackers Exploit Zero-Day Flaw in EOL GeoVision Devices

Espionage Ops Exploit Output Messenger Vulnerability

Exploited in the Wild: Fortinet Urges Patch for Critical Zero-Day

Samsung Patches Actively Exploited MagicINFO 9 Server Zero-Day

Ivanti Addresses Critical Zero-Day Vulnerabilities in EPMM

Microsoft Shuts Down Five Zero-Days in Latest Patch Rollout

CVE-2025-4664: Google Chrome’s Zero-Day Flaw Exploited in the Wild

TransferLoader: The Malware That Outsmarts Security

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Crimson	MD5	026e8e7acb2f2a156f8afff64fd54066, fb64c22d37c502bde55b19688d40c803, 70b8040730c62e4a52a904251fa74029, 3efec6ffcbfe79f71f5410eb46f1c19e, b03211f6feccd3a62273368b52f6079d
	SHA256	d1a1eaefe6bd2e245bba369e966d7a8eab9ed6ad1fa827321e5889cc8d43f976
Poseidon	SHA256	541cefaad8d9554bdc5ce9cde24e4556c2444111ea13bd9965bd4a50e60f9265, 682d5e53a456668f15809d9ab499651e1342fc602e7f5bc85e30fe29933f7634, 7e2020c4a838bd7463478188bfaa97e66cf3365d3aef03f1b4398eaddacfc6b9
ElizaRAT	SHA256	b30a9e31b0897bfe6ab80aebcd0982eecf68e9d3d3353c1e146f72195cef0ef5, 263f9e965f4f0d042537034e33699cf6d852fb8a52ac320a0e964ce96c48f5e5
PupkinStealer	MD5	fc99a7ef8d7a2028ce73bf42d3a95bce
	SHA256	9309003c245f94ba4ee52098dadbaa0d0a4d83b423d76c1bfc082a1c29e0b95f
TransferLoader	SHA256	b55ba0f869f6408674ee9c5229f261e06ad1572c52eaa23f5a10389616d62efe

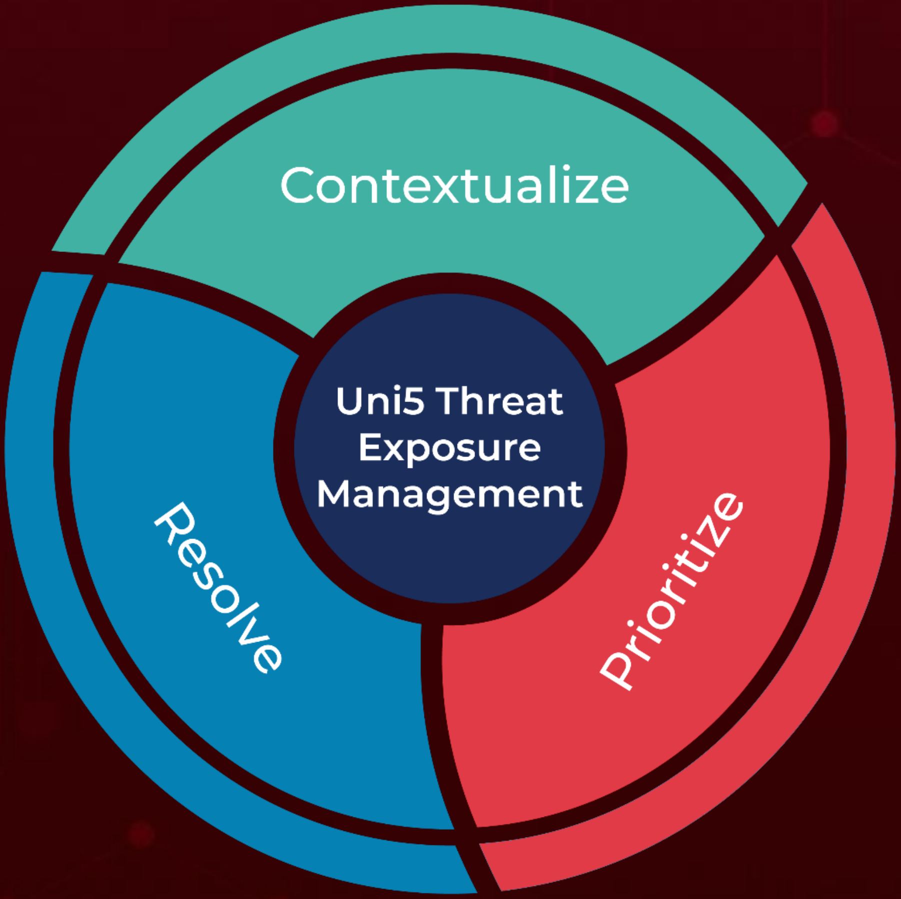
Attack Name	TYPE	VALUE
Mirai	SHA256	f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714, 11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114, 8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e, ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516, 03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3, 0333c6ac43c6e977e9a1c5071194d3cf8aa01222194c6e7f2fd13e631d03522d, 7a8a46ace3b9261c2c7a399dcae037ce4f185f52f94b893d5bc00cd1228fb13a, 50c5b6c971c503240b91787d31f9314ded38d4f2700ff90deb032478b30aa0c5, bb2ab0879282c5c7f92a51e6482d3eb60a84ab184eca258ea550d9ed04bc5eda, 074a261bf281da36cc91cd13f86c7a8f75fdf96807d525c24b22c48fe01584a3, 5e721c013a6e8b2246aae86974f2163d3b57a7e6608a318ab84c44b1650e650a, de3c9ecb51564e4298ce7e4ff749be0a42d37824d2fd3d5b7fbab86a04105b88, aaba1ce1f182122a7ea05683623ab2d9bd05a3507e0dfc95e8e4165f629f80a8, 3f465182b5c594784e406a6a5de2f398bcc2e2ffc92d049a7990f37c267550a6, 3d6a544b1f03df23e734a65b9f1e808ff513ad881f09745a3959d696075c057e, 5180e3050a4a5cff52dcd8e8bb39fb6cf59a264a8fb6ddcc239615b340f1b99a, 2cc4d952856a8f2e1dd73b175d730d9cc7a04c73cf6452c8d0411eedf3aed5d5, dc21419b73566651b4c1e85879c0c98a4dcff8f7d206d9a97882200503658e9c, 866b2dbbd1978be007460835e8f3d2e02c1b321f856a18ba3e53030d4effe69a, 64ca8dd1a2702e0463bab19a0b826f79c55cfd46e4e1b41c6c33d7e7aa2c7530, 9f05425478d03e4a2fd5b990fe5625d93c468b80a3880bb52475aa7561548582, bf6984ccc9fb21beba3f492420901be0b0bace8d4530e6d2850f039622f1b96f, 58f7d61e3e474d5f5eccbba79556070220f52fa011b7cd24bdd96c23c338cd4b

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

May 19, 2025 • 11:00 PM

More at www.hivepro.com