Date of Publication
February 3, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

27 JANUARY to 02 FEBRUARY 2025

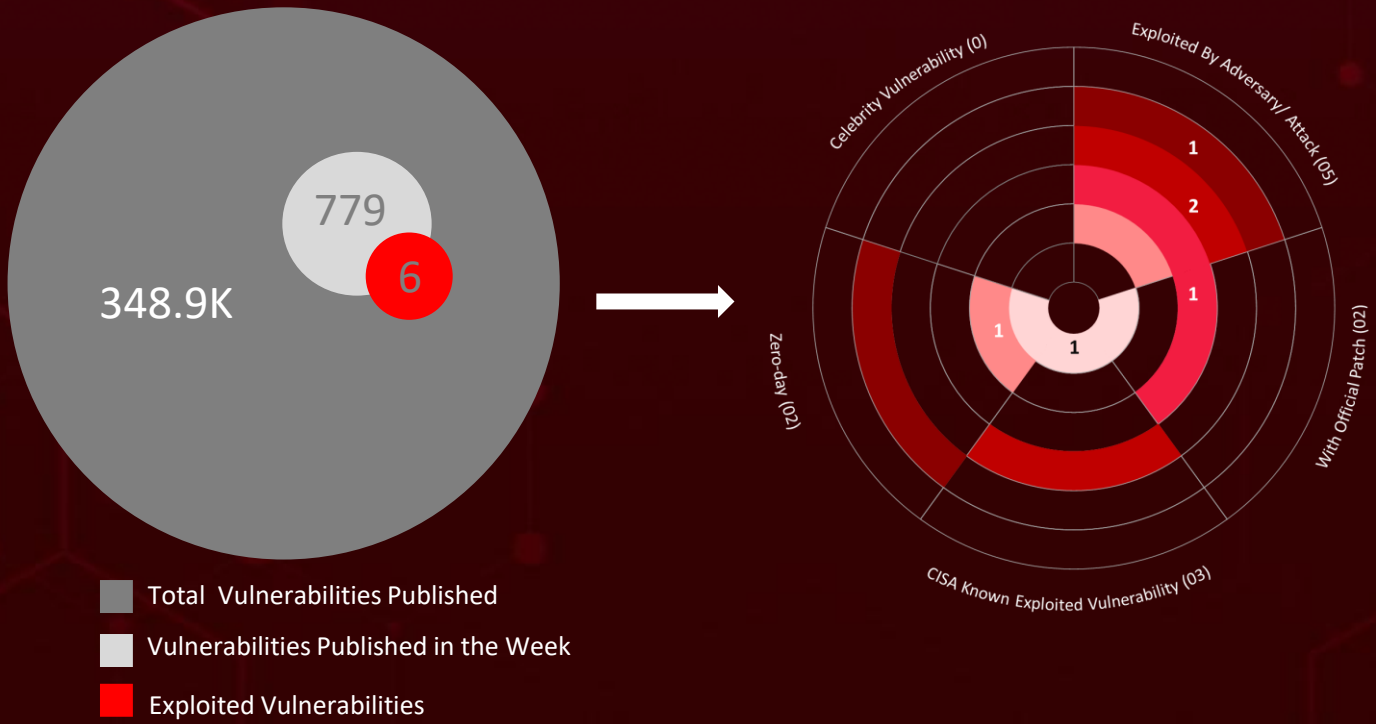
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In just the past week, **seven** attacks were executed, and **six** vulnerabilities were uncovered, highlighting the persistent danger of cyberattacks.

HiveForce Labs identifies critical security threats, including two actively exploited zero-day vulnerabilities. **CVE-2025-24085** affects Apple products, allowing malicious apps to escalate privileges on vulnerable devices, posing a significant risk of system compromise. Meanwhile, **CVE-2024-40891** targets Zyxel CPE Series devices, which have remained unpatched since July 2024. This flaw has been exploited by botnets like Mirai, raising concerns over large-scale attacks.

Ransomware threats are also escalating. **FunkSec**, emerging in late 2024, has quickly become a major player, blending AI-driven tools with cybercrime and hacktivism. Their fast-evolving ransomware demands low ransoms but causes widespread disruption. Meanwhile, the **Daixin Team** continues to target healthcare, government, and enterprise sectors, focusing on VMware ESXi servers. They were recently seen in their June 2024 attack on Dubai Municipality, where they stole 80GB of sensitive data. These growing threats underscore the urgent need for robust security measures, including regular patching, strong authentication, and proactive monitoring.



High Level Statistics

7
Attacks Executed

6
Vulnerabilities Exploited

0
Adversaries in Action

- Lumma
- TorNet
- PureCrypter
- Mirai
- FunkSec
- Aquabotv3
- Daixin Team

- CVE-2025-24085
- CVE-2024-40891
- CVE-2024-41710
- CVE-2018-10562
- CVE-2018-10561
- CVE-2023-26801

Insights

Aquabotv3 new Mirai variant making waves with DDoS-as-a-service, exploiting vulnerabilities in Mitel SIP phones

CVE-2025-24085 A critical zero-day in Apple under active exploitation, allowing malicious apps to gain elevated privileges on vulnerable devices

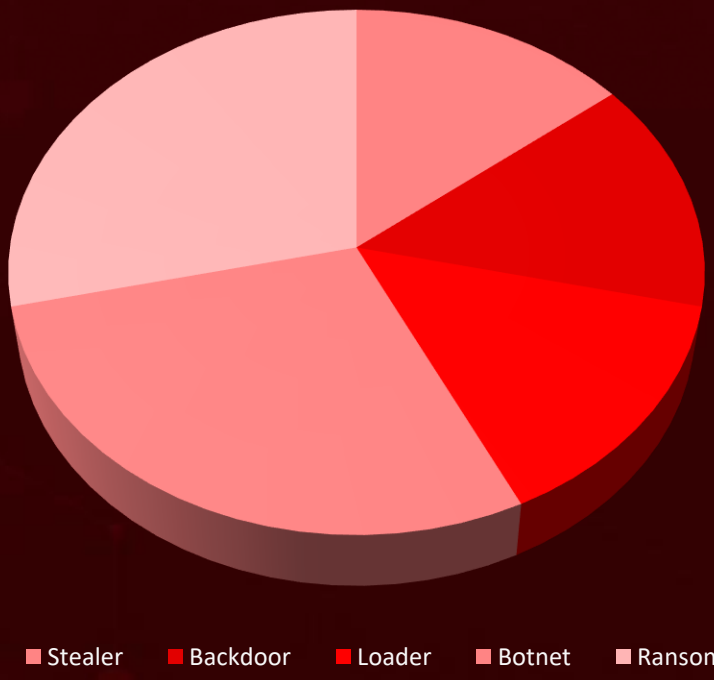
Daixin ransomware group hit Dubai Municipality, stealing 80GB of data, breachs networks through VPN flaws, phishing, and weak authentication

CVE-2024-40891 A critical zero-day in Zyxel CPE Series devices is under active attack. Unpatched since July 2024, it leaves devices wide open to exploitation

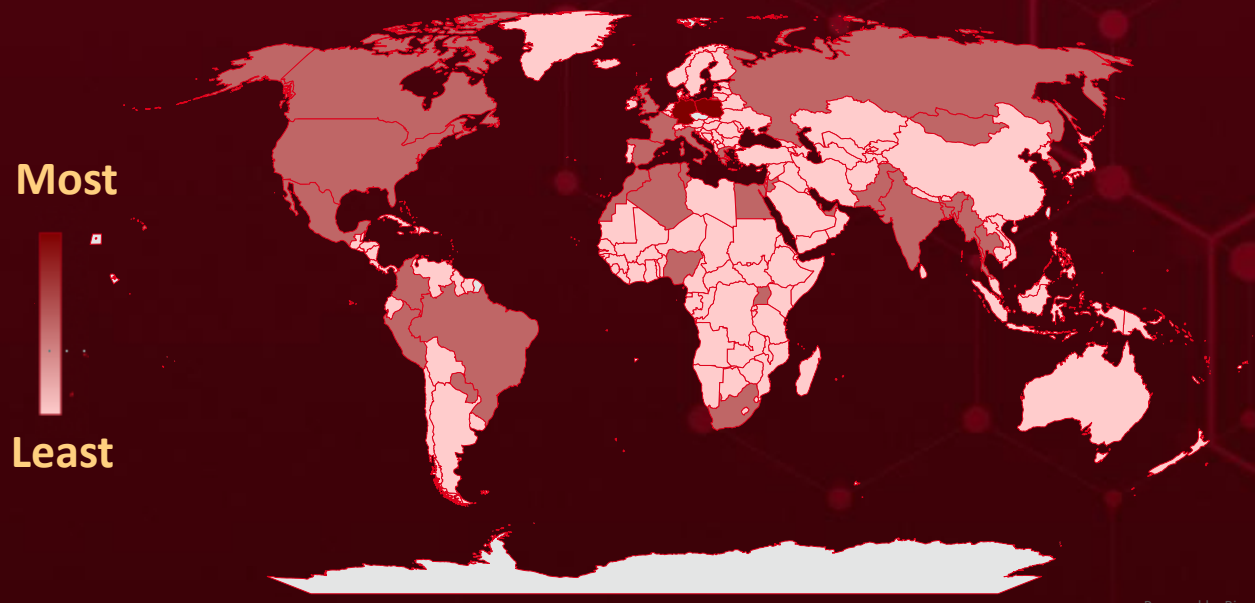
FunkSec rapidly emerging as a dominant ransomware force. Blending AI-driven tools with cybercrime and hacktivism. A fast-evolving ransomware, paired with low ransom demands, keeps security teams on edge

Lumma Stealer campaign targets Windows users with fake CAPTCHAs, malvertising, and clipboard command tricks to bypass defenses

Threat Distribution



Targeted Countries



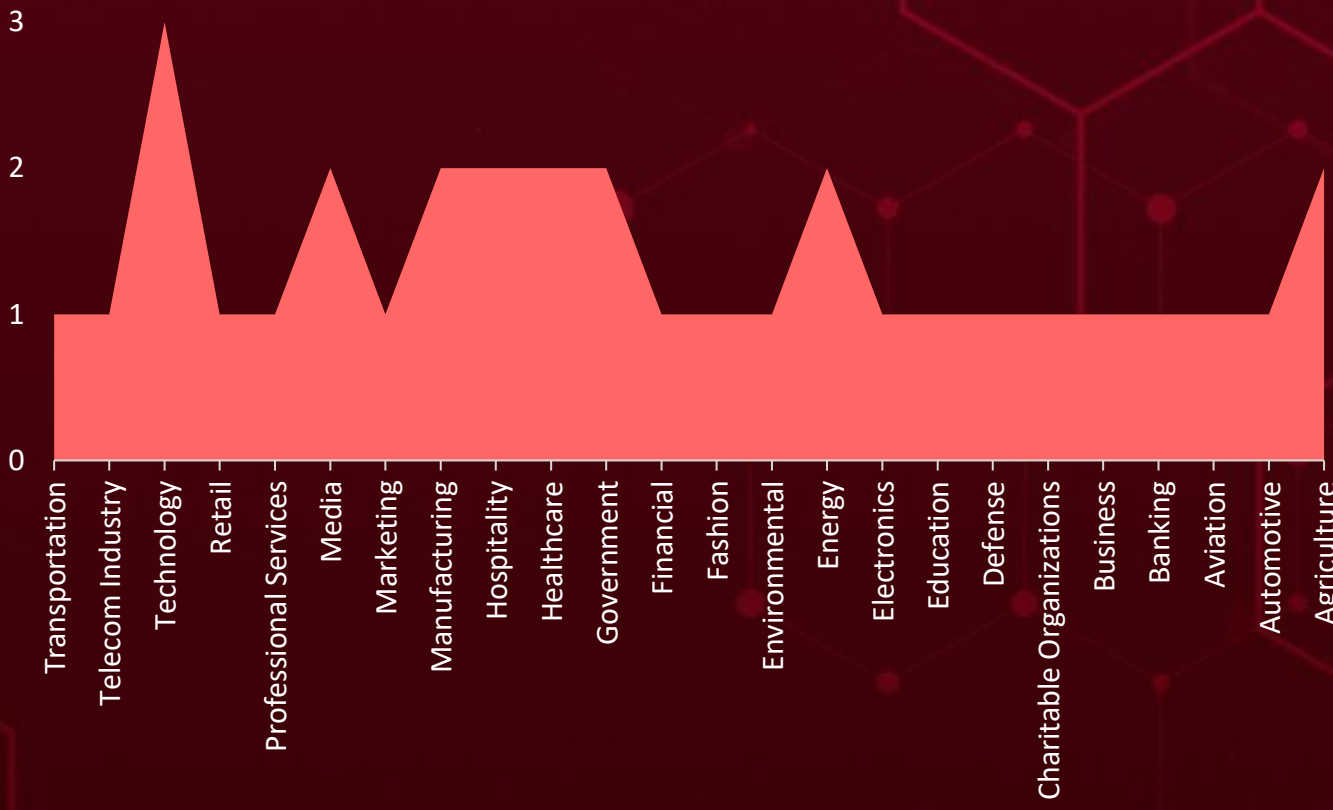
Countries
Poland
Germany
Morocco
Spain
Algeria
Brazil
United Arab Emirates
Canada
Paraguay
Colombia
Russia
Egypt
Tunisia
France
Mongolia
Myanmar
Bangladesh
Nigeria
Pakistan
Greece
Peru
India

Countries
Qatar
Israel
South Korea
Italy
Thailand
Jordan
Uganda
United Kingdom
Mexico
United States
South Africa
North Korea
Micronesia
Chad
Rwanda
Chile
Togo
China
Namibia
Antigua and Barbuda
Bosnia and Herzegovina
Comoros

Countries
Serbia
Congo
Suriname
Costa Rica
Ukraine
Côte d'Ivoire
Montenegro
Croatia
New Zealand
Cuba
Bolivia
Cyprus
Portugal
Czech Republic (Czechia)
San Marino
Denmark
Slovakia
Djibouti
Sri Lanka
Dominica
Tajikistan
Dominican Republic

Countries
Turkey
DR Congo
Mauritius
Ecuador
Monaco
Argentina
Mozambique
El Salvador
Nepal
Equatorial Guinea
Niger
Eritrea
Norway
Estonia
Panama
Eswatini
Philippines
Ethiopia
Romania
Fiji
Saint Lucia
Finland

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1140** Deobfuscate/ Decode Files or Information	**T1057** Process Discovery	**T1588.006** Vulnerabilities
T1560 Archive Collected Data	**T1204** User Execution	**T1583** Acquire Infrastructure	**T1070** Indicator Removal	**T1498** Network Denial of Service
T1027 Obfuscated Files or Information	**T1566** Phishing	**T1078** Valid Accounts	**T1059.001** PowerShell	**T1036** Masquerading
T1071 Application Layer Protocol	**T1486** Data Encrypted for Impact	**T1573.001** Symmetric Cryptography	**T1059.003** Windows Command Shell	**T1053** Scheduled Task/Job

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two-factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	using fake CAPTCHAs	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	b94ddefd39d32a753564e6871d11750fa56b993cad3ea40955139e584ad3bef8, 86d50a7fc8d245876b791efe85eb7f64cd48b9e9648b4bf8bee22dbae66fe3aa, 02a0bba5b3cc6a650d611c2f6d6a8ce6a696c230521f0de43824a19ced716acd		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TorNet	TorNet is a sophisticated .NET-based backdoor designed to give attackers remote control over compromised systems. It can download and execute arbitrary .NET assemblies directly in the victim's memory. Once active, TorNet establishes a connection with its command-and-control (C2) server while also routing the infected machine's traffic through the TOR network. This dual connection not only facilitates secure communication with the attackers but also helps mask their activities.	PureCrypter drops the TorNet backdoor	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	13ac538c8c6696a59f890677cf451db77b7c33539da1d380640ce549b2b70ca4, 53e7b3b72695a1eaea7146ec3cbd05d0ce2a1eba87f035ae07849feb4f59ec63		

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
PureCrypter	PureCrypter is a .NET-based malware loader obfuscated using SmartAssembly, employing compression, encryption, and obfuscation techniques to evade detection by antivirus software. Its key features include persistence, code injection, and defense mechanisms, which are configurable using Google's Protocol Buffer message format. PureCrypter has been observed distributing a range of malicious payloads, including RATs and information stealers, making it a versatile and dangerous tool in cybercriminal campaigns.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Deploy malware	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	3b4e709768d7cd0cb895de74267f45a6ef6565ebed445393878f17ae02a983e3, 84570dac910557d0d8217db746c9a8fd4a27cd3db89135731c7f3584b37df533, 7ce9af599857827317a444c5a63a08929ec97765bc2624076f4834f323a41da2, 57543fd3673c9595a73c836b153faf68e23938662c5a4b6675205734b688ae95, bff0ec65af8b2bb37fcc5202f823b5877ebdcc8efbd32e08f309cbcb4dc2570c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
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-2024-40891
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Network Overload, Widespread IoT Device Compromise	Zyxel CPE series devices
ASSOCIATED ACTOR			**PATCH LINK**
-			No Patch
IOC TYPE	**VALUE**		
SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c04910ad2f067		

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 CVEs</th></tr>
<tr><td>FunkSec</td><td rowspan="5">FunkSec is a file-encrypting ransomware strain written in Rust, believed to be crafted with the assistance of AI. Operating under the ransomware-as-a-service (RaaS) model, FunkSec employs double extortion tactics encrypting victims' data while threatening to leak stolen information to intensify ransom demands. It employs RSA and AES encryption, appends a ".funksec" extension to encrypted files, and aggressively disables security features.</td><td>-</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Data Theft, Encrypt Data</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c,
66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd,
dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac,
b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb,
5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd</td></tr>
</table>

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 CVEs</th></tr>
<tr><td>Aquabotv3</td><td rowspan="6">Aquabotv3 is the latest iteration of the Aquabot botnet, built upon the foundation of the notorious Mirai malware. At first glance, it appears to be a typical Mirai variant, equipped with standard distributed denial-of-service (DDoS) capabilities like flood attacks and bypass techniques. However, Aquabotv3 introduces a significant innovation: the ability to establish direct communication with its command-and-control (C2) server in response to specific system signals. This adaptive feature enhances the botnet's resilience, making it more difficult to detect, disrupt, and dismantle compared to its predecessors.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-41710
CVE-2018-17532
CVE-2023-26801
CVE-2022-31137
CVE-2018-10562
CVE-2018-10561</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Botnet</td><td rowspan="3">Network Compromise</td><td rowspan="2">Mitel SIP Phones, Teltonika RUT9XX, lb-link bl-lte300_firmwareRoxy Wi, Dasan GPON home routers</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>-</td><td>PATCH LINK</td></tr>
<tr><td colspan="3"></td><td>https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019 , https://wiki.teltonika-networks.com/view/RUT900_Firmware_Downloads_(legacy_WebUI) , https://github.com/roxy-wi/roxy-wi/releases/tag/v8.1.4</td></tr>
</table>

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 CVEs</th></tr>
<tr><td>Daixin Team</td><td rowspan="4">The Daixin Team is a ransomware group notorious for targeting various sectors, with a particular focus on VMware ESXi servers. Their attack methods typically involve exploiting VPN vulnerabilities, conducting phishing campaigns, and taking advantage of weak authentication mechanisms to gain initial access. Once inside a network, they exfiltrate and encrypt sensitive data to maximize the impact of their ransom demands .</td><td>Exploit VPN vulnerabilities, Phishing, and weak authentication</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt Data, Data Theft</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238,
19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD,
54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939,
EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF,
475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24085	✗	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use After Free Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/108926 , https://support.apple.com/en-us/108414

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40891	✗	Zyxel CPE Series	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:cpe:*:*:*:*:*:*	Mirai
Zyxel CPE Telnet Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41710	✗	Mitel SIP Phones	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:mitel:sip_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Mitel SIP Phones Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-88	T1059: Command and Scripting Interpreter	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-10562		Dasan GPON home routers	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Dasan GPON Routers Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-10561		Dasan GPON home routers	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Dasan GPON Routers Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication, T1059: Command and Scripting Interpreter	No Patch

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-26801</td><td>  </td><td rowspan="2">lb-link bl-lte300_firmware</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:lb-link:bl-lte300_firmware:1.0.8:*:*:*:*:*:*:*</td><td rowspan="2">Aquabotv3</td></tr>
<tr><td rowspan="3">lb-link bl-lte300_firmware Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1059: Command and Scripting Interpreter</td><td>No Patch</td></tr>
</table>

Adversaries in Action

No Active Adversaries tracked this week.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the malware **Lumma, TorNet, PureCrypter, Mirai, FunkSec, Aquabotv3, Daixin Team.**

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the malware **Lumma, TorNet, PureCrypter, FunkSec, Aquabotv3** and **Daixin Team** in Breach and Attack Simulation(BAS).

Threat Advisories

Lumma Stealer Strikes Again with Fake CAPTCHAs and Advanced Evasion

Apple Tackles First Zero-Day of 2025, Actively Exploited in the Wild

TorNet Backdoor: Stealthy Phishing Campaign Hits Poland and Germany

Critical Zyxel CPE Zero-Day Under Active Exploitation

Fast-Tracking FunkSec Ransomware with the Twist of AI-Driven Havoc

Aquabotv3: The Next Evolution of Mirai in DDoS Attacks

Daixin Team Ransomware: A Growing Cyber Threat

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
Lumma	MD5	82e5e8ec8e4e04f4d5808077f38752ba, 14d8486f3f63875ef93cfd240c5dc10b, 0ba2afe43cc4deed266354b1c2cfb5a7
	SHA256	b94ddefd39d32a753564e6871d11750fa56b993cad3ea40955139e584ad3bef8, 86d50a7fc8d245876b791efe85eb7f64cd48b9e9648b4bf8bee22dbae66fe3aa, 02a0bba5b3cc6a650d611c2f6d6a8ce6a696c230521f0de43824a19ced716acd
TorNet	SHA256	13ac538c8c6696a59f890677cf451db77b7c33539da1d380640ce549b2b70ca4, 53e7b3b72695a1eaea7146ec3cbd05d0ce2a1eba87f035ae07849feb4f59ec63
PureCrypter	SHA256	3b4e709768d7cd0cb895de74267f45a6ef6565ebed445393878f17ae02a983e3, 84570dac910557d0d8217db746c9a8fd4a27cd3db89135731c7f3584b37df533, 7ce9af599857827317a444c5a63a08929ec97765bc2624076f4834f323a41da2, 57543fd3673c9595a73c836b153faf68e23938662c5a4b6675205734b688ae95, bff0ec65af8b2bb37fcc5202f823b5877ebdcc8efbd32e08f309cbcb4dc2570c, c32d97fb9a1681a7bea3f417abde0264a2332221e317c8543e337baac9307c67, 4280eb4cfa0445a40d8e1dfafdc0eb24613f3536c5959270ef0079034b30e653,edac6216665f1c8b0a09158abdd5e7fab63a386a1c9ad31ddd5ee92a6aa811fc

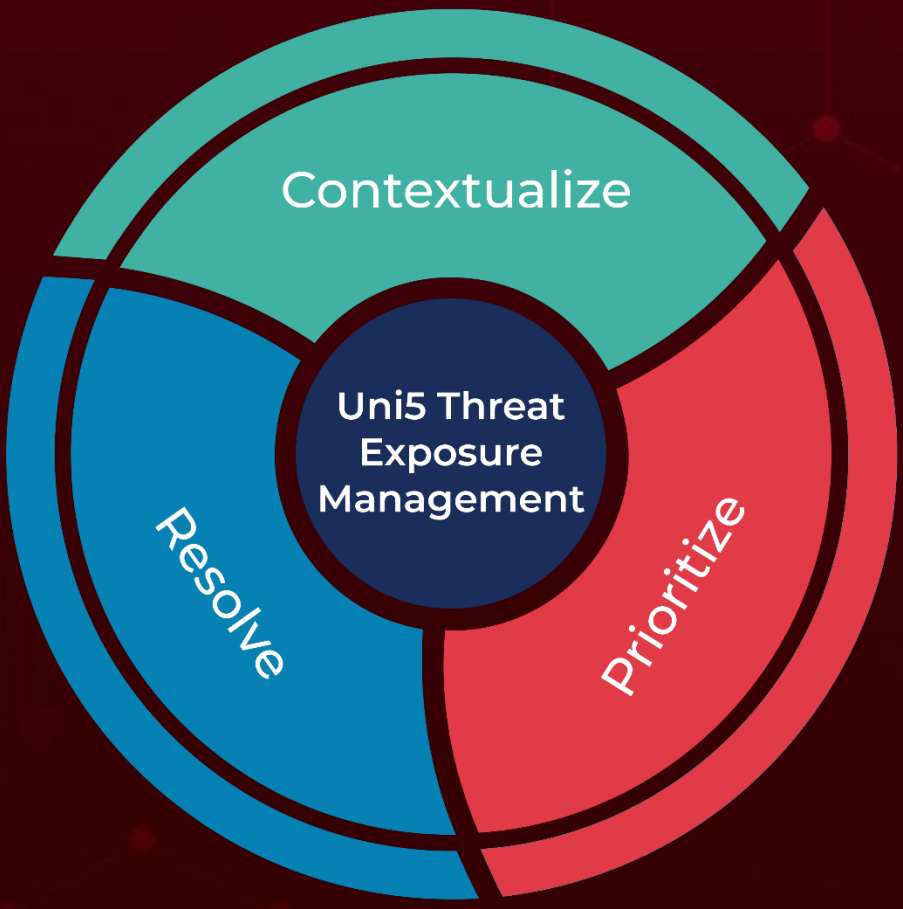
Attack Name	TYPE	VALUE
Mirai	SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c04910ad2f067
FunkSec	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
Daixin Team	SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238, 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD, 54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939, EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF, 475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28
	File Path	rclone-v1.59.2-windows-amd64\git-log.txt, rclone-v1.59.2-windows-amd64\rclone.1, rclone-v1.59.2-windows-amd64\rclone.exe, rclone-v1.59.2-windows-amd64\README.html, rclone-v1.59.2-windows-amd64\README.txt
	Tor Address	7ukmkdtyxdkdivtjad57klqnd3kdsmq6tp45rrsxqnu76zzv3jvitlqd[.]onion, 232fwh5cea3ub6qguz3pynijxfzl2uj3c73nbrayipf3gq25vtq2r4qd[.]onion

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 3, 2025 • 5:45 AM

More at www.hivepro.com