

Date of Publication  
December 2, 2024



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

25 NOVEMBER to 1 DECEMBER 2024

# Table Of Contents

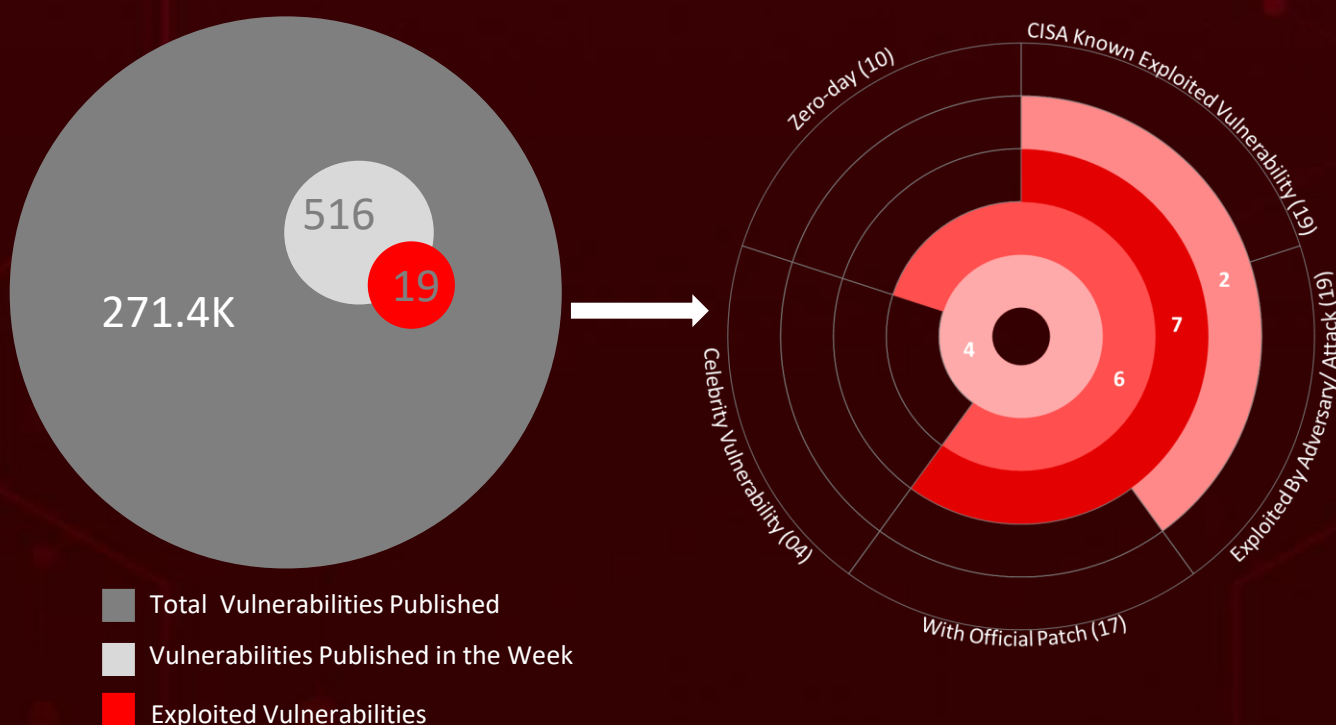
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	15
<u>Adversaries in Action</u>	25
<u>Recommendations</u>	30
<u>Threat Advisories</u>	31
<u>Appendix</u>	32
<u>What Next?</u>	35

# Summary

HiveForce Labs has identified a surge in cybersecurity threats, highlighting the increasing complexity and frequency of cyber incidents. Over the past week, **nine** major cyberattacks were detected, **nineteen** critical vulnerabilities were actively exploited, and **five** threat groups were closely monitored, reflecting a relentless rise in malicious activities.

In a parallel development, **TAG-110**, a Russia-linked threat actor associated with APT28, is conducting a cyber-espionage campaign targeting government, human rights, and educational institutions across Asia and Europe. This campaign leverages custom malware to compromise critical systems. Meanwhile, the **Matrix** threat actor has launched a disruptive Distributed Denial-of-Service (DDoS) campaign, causing widespread operational challenges for its targets.

Adding to the urgency, the Russia-based **RomCom** cybercrime group has been exploiting **two zero-day** vulnerabilities in a sophisticated attack chain, demonstrating the growing innovation in cybercriminal tactics. These developments underscore the escalating sophistication of threat actors and the urgent need for advanced, proactive cybersecurity measures to combat evolving global threats.



# High Level Statistics

9

Attacks  
Executed

19

Vulnerabilities  
Exploited

5

Adversaries in  
Action

- [WolfsBane](#)
- [FireWood](#)
- [HATVIBE](#)
- [CHERRYSPY](#)
- [RomCom](#)
- [Mirai](#)
- [GHOSTSPIDER](#)
- [SNAPPYBEE](#)
- [MASOL RAT](#)

- [CVE-2024-23692](#)
- [CVE-2023-36884](#)
- [CVE-2024-9680](#)
- [CVE-2017-18368](#)
- [CVE-2021-20090](#)
- [CVE-2024-27348](#)
- [CVE-2022-30525](#)
- [CVE-2018-10562](#)
- [CVE-2018-10561](#)
- [CVE-2017-17215](#)
- [CVE-2014-8361](#)
- [CVE-2023-46805](#)
- [CVE-2024-21887](#)
- [CVE-2023-48788](#)
- [CVE-2022-3236](#)
- [CVE-2021-26855](#)
- [CVE-2021-26857](#)
- [CVE-2021-26858](#)
- [CVE-2021-27065](#)

- [Gelsemium](#)
- [TAG-110](#)
- [RomCom](#)
- [Matrix](#)
- [Earth Estries](#)



# Insights

Hackers Corrupt  
Trusted **Avast**  
Driver to  
Neutralize System  
Defenses

Custom Malware  
Fuels **TAG-110's**  
Targeted Espionage  
Campaigns

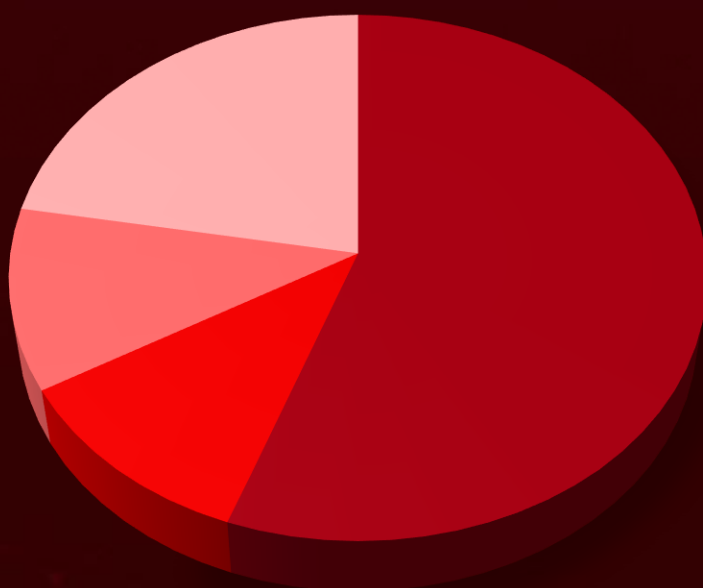
Silent Compromise **RomCom**  
Delivers Backdoor With **Zero-  
Interaction Exploits**

**WolfsBane** and **FireWood**  
Malware Signal Gelsemium's  
Cross-Platform Evolution

**Mirai Malware Evolves in  
Matrix:** Plug-and-Play Cyberattacks  
Campaign Fuels Novice Hacker Surge

**Earth Estries**  
Exploits Public Server  
Vulnerabilities to  
Expand Espionage  
Across APAC and the  
Middle East

## Threat Distribution



■ Backdoor ■ Botnet ■ Loader ■ Modular Backdoor

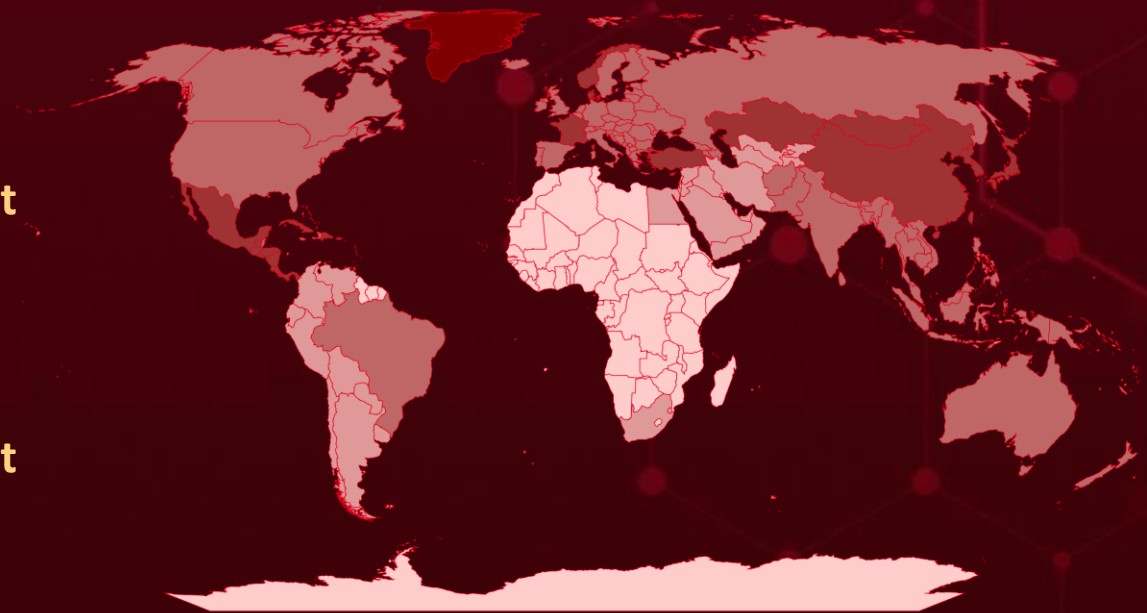


# Targeted Countries

Most



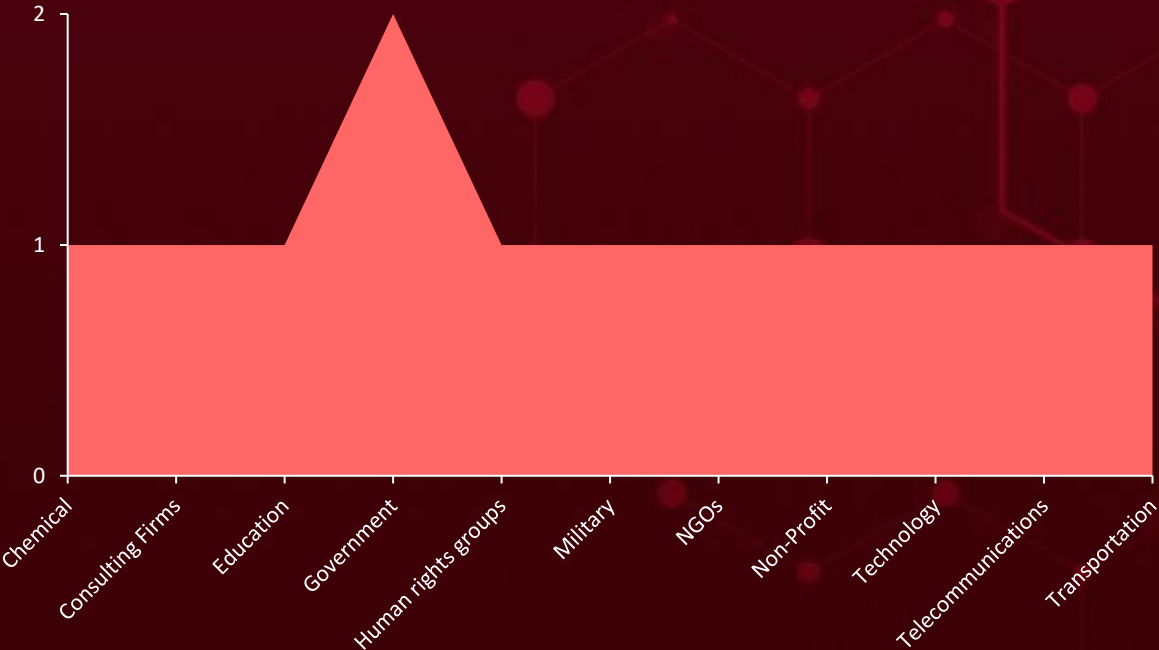
Least



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Countries	Countries	Countries	Countries
Greenland	Solomon Islands	Fiji	Hungary
Mexico	Portugal	Romania	Iceland
Turkey	Canada	Finland	North Macedonia
Norway	Vanuatu	Saint Lucia	India
China	Northern Cyprus	Aruba	Bhutan
Japan	Afghanistan	San Marino	Indonesia
Costa Rica	Thailand	Georgia	Palau
Nicaragua	Belgium	Slovakia	Ireland
Cuba	Åland	Germany	Poland
Akrotiri and Dhekelia	Belize	Spain	Italy
Cyprus	Croatia	Gibraltar	Brazil
Hong Kong	Bosnia and Herzegovina	Switzerland	Jamaica
Denmark	Albania	Greece	Russia
Macau	Saint Barthélemy	Trinidad and Tobago	Bangladesh
Dominican Republic	Curaçao	Australia	Abkhazia
Mongolia	Singapore	United Kingdom	Sri Lanka
El Salvador	Andorra	Grenada	Liechtenstein
North Korea	Svalbard	Belarus	Sweden
France	Czech Republic	Austria	Lithuania
Panama	Tuvalu	Monaco	Brunei
Puerto Rico	Anguilla	Guernsey	Luxembourg
South Korea	Moldova	Montenegro	Tonga
Taiwan	Armenia	Haiti	Barbados
Guatemala	Bermuda	Myanmar	Bulgaria
Honduras	Estonia	Azerbaijan	Malaysia
Kazakhstan	Pakistan	Netherlands	Ukraine
Nepal	Philippines	Bahamas	Maldives
		New Zealand	United States

# Targeted Industries



## TOP MITRE ATT&CK TTPs

<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1027</u></b> Obfuscated Files or Information	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1573</u></b> Encrypted Channel	<b><u>T1036</u></b> Masquerading
<b><u>T1071.001</u></b> Web Protocols	<b><u>T1041</u></b> Exfiltration Over C2 Channel	<b><u>T1543</u></b> Create or Modify System Process	<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1583</u></b> Acquire Infrastructure
<b><u>T1587</u></b> Develop Capabilities	<b><u>T1587.001</u></b> Malware	<b><u>T1071</u></b> Application Layer Protocol	<b><u>T1005</u></b> Data from Local System	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1548</u></b> Abuse Elevation Control Mechanism	<b><u>T1546</u></b> Event Triggered Execution	<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1036.005</u></b> Match Legitimate Name or Location	<b><u>T1068</u></b> Exploitation for Privilege Escalation





# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>WolfsBane</u>	WolfsBane showcases exceptional complexity through its refined deployment framework, incorporating a dropper, launcher, and backdoor. Its use of custom-built libraries for network interactions, along with rootkits to obscure its operations, reflects a modular design and precision similar to its Windows counterpart.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Gelsemium			-
IOC TYPE	VALUE		
SHA256	ccf8e4d6e661ceaea598851923bb8b983bd820ffd02448b8245e6ac780977784, fddec9ff14ebd957038f9c24843bff935c4f73651e9704b553dec116851f7ae5, 1ec286f2194199206e4ce345f1bf322b6b0b4c947b1cf32db59cca2d89370738		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>FireWood</u>	The FireWood backdoor builds on the Project Wood lineage by employing kernel-level rootkits to conceal processes and advanced encryption techniques like TEA to guarantee secure communication.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor			
ASSOCIATED ACTOR		Information Theft, Persistence	-
Gelsemium			PATCH LINK
	-		
IOC TYPE	VALUE		
SHA256	cff20753e36a4c942dc4dab5a91fd621a42330e17a89185a5b7262280bcd9263		

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
<u>HATVIBE</u>	HATVIBE is a custom HTML Application (HTA) loader designed to deploy additional malware, including the CHERRYSPY backdoor. It ensures persistence by using a scheduled task to execute the HTA file through mshta.exe. HATVIBE also employs two layers of obfuscation to evade detection.	Phishing, Exploitation of vulnerable web-facing services	CVE-2024-23692
		IMPACT	AFFECTED PRODUCT
		Malware Deployment, Persistence	Rejetto HTTP File Server
			PATCH LINK
			<a href="https://www.rejetto.com/hfs/">https://www.rejetto.com/hfs/</a>
TYPE			
Loader			
ASSOCIATED ACTOR			
TAG-110			
IOC TYPE	VALUE		
SHA256	332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>CHERRYSPY</u>	CHERRYSPY is a custom Python backdoor designed for espionage. HATVIBE typically downloads it along with a Python interpreter, which is used for execution. Once activated, CHERRYSPY establishes a secure communication channel with a hard-coded C2 server via HTTP POST requests.	Phishing, Exploitation of vulnerable web-facing services	CVE-2024-23692
		IMPACT	AFFECTED PRODUCT
		Information Theft, Remote Access	Rejetto HTTP File Server
			PATCH LINK
			<a href="https://www.rejetto.com/hfs/">https://www.rejetto.com/hfs/</a>
TYPE			
Backdoor			
ASSOCIATED ACTOR			
TAG-110			
IOC TYPE	VALUE		
Domains	internalsecurity[.]us, errorreporting[.]net		

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	
<u>RomCom</u>	The RomCom backdoor maintains persistence by hijacking DLLs loaded by explorer.exe or wordpad.exe. It identifies debuggers by registering an exception handler and checks the system state before execution. Furthermore, it employs a browser stealer module to gather passwords, cookies, and session data.	Exploiting vulnerabilities	CVE-2023-36884 CVE-2024-9680	
		IMPACT	AFFECTED PRODUCTS	
TYPE		Information Theft, Remote Access	Microsoft Office, Windows, Mozilla Firefox, and Firefox ESR	
Backdoor			PATCH LINKS	
ASSOCIATED ACTOR			<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884</a> , <a href="https://www.mozilla.org/en-US/firefox/new/">https://www.mozilla.org/en-US/firefox/new/</a> , <a href="https://www.mozilla.org/en-US/firefox/enterprise/#download">https://www.mozilla.org/en-US/firefox/enterprise/#download</a>	
RomCom				
IOC TYPE	VALUE			
SHA256	05681ff7cae6b28f5714628a269caa5115da49c94737ce82ec09b4312e40fd26, 068117b406940ac510ed59efd1d7c7651f645a31bd70db6de16aba12c055aae6, 28950cff484550312f2c91e17d7da89300981f17b19a7cd9c5432a4b76e281d2			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mirai</u>	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. Mirai gained widespread attention in 2016 for executing some of the largest DDoS attacks, causing significant disruption. Its open-source release has led to the creation of several variants.	Exploiting default or hardcoded credentials	CVE-2017-18368 CVE-2021-20090 CVE-2024-27348 CVE-2022-30525 CVE-2022-30075 CVE-2018-10562 CVE-2018-10561 CVE-2018-9995 CVE-2017-17215 CVE-2017-17106 CVE-2014-8361
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Network Overload, Widespread IoT Device Compromise	Buffalo WSR firmware, Apache HugeGraph-Server, Zyxel, TP-Link, Dasan, TBK DVR devices, Huawei HG532 router, Zivif webcams, Realtek SDK
ASSOCIATED ACTOR			PATCH LINKS
Matrix			<a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware</a> , <a href="https://www.buffalo-technology.com/service-support/downloads/software-firmware-updates/">https://www.buffalo-technology.com/service-support/downloads/software-firmware-updates/</a> , <a href="https://hugegraph.apache.org/docs/download/download/">https://hugegraph.apache.org/docs/download/download/</a> , <a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a> , <a href="https://www.tp-link.com/us/support/download/archer-ax50/">https://www.tp-link.com/us/support/download/archer-ax50/</a> , <a href="https://www.huawei.com/en/psirt/security-notice/huawei-sn-20171130-01-hg532-en">https://www.huawei.com/en/psirt/security-notice/huawei-sn-20171130-01-hg532-en</a> , <a href="https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055">https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055</a>
IOC TYPE	VALUE		
SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a		

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
<b>GHOSTSPIDER</b>		Exploiting public-facing server vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2023-48788 CVE-2022-3236 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>	GHOSTSPIDER is a sophisticated, multi-modular backdoor designed with multiple layers to load different modules for specific tasks. It communicates with its command-and-control (C&C) server using a custom protocol secured by Transport Layer Security (TLS), ensuring encrypted and secure communication.	Information Theft, Remote Access, Persistence	Ivanti Connect Secure and Policy Secure, Fortinet FortiClientEMS, Sophos Firewall, Microsoft Exchange Server
Modular Backdoor			<b>PATCH LINKS</b>
<b>ASSOCIATED ACTOR</b>			<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a> , <a href="https://fortiguard.fortinet.com/p/sirt/FG-IR-24-007">https://fortiguard.fortinet.com/p/sirt/FG-IR-24-007</a> , <a href="https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce">https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a>
Earth Estries			
IOC TYPE	VALUE		
IPv4	139[.]59[.]108[.]43, 185[.]105[.]1[.]243		

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
<b>SNAPPYBEE</b> <a href="#">(aka Deed RAT)</a>	SNAPPYBEE is a modular backdoor designed for sustained access and espionage. It enables activities such as data exfiltration, system surveillance, and the execution of malicious commands by the attacker.	Exploiting public-facing server vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2023-48788 CVE-2022-3236 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065
		IMPACT	AFFECTED PRODUCTS
TYPE		Espionage, Information Theft, Remote Access, Persistence	Ivanti Connect Secure and Policy Secure, Fortinet FortiClientEMS, Sophos Firewall, Microsoft Exchange Server
Modular Backdoor			PATCH LINKS
ASSOCIATED ACTOR			<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a> , <a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-007">https://fortiguard.fortinet.com/psirt/FG-IR-24-007</a> , <a href="https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce">https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a>
Earth Estries			
IOC TYPE	VALUE		
SHA256	fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5		

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
MASOL RAT (aka Backdr-NQ)	MASOL RAT is a cross-platform backdoor first observed in attacks aimed at Southeast Asian governments. It mainly targets Linux servers, offering remote access and the capability to execute commands.	Exploiting public-facing server vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2023-48788 CVE-2022-3236 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Espionage, Information Theft, Remote Access, Persistence	Ivanti Connect Secure and Policy Secure, Fortinet FortiClientEMS, Sophos Firewall, Microsoft Exchange Server
ASSOCIATED ACTOR			PATCH LINKS
Earth Estries			<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a> , <a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-007">https://fortiguard.fortinet.com/psirt/FG-IR-24-007</a> , <a href="https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce">https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a>
IOC TYPE	VALUE		
SHA256	44ea2e85ea6cffba66f5928768c1ee401f3a6d6cd2a04e0d681d695f93cc5a1f		

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
<u>CVE-2024-23692</u>		Rejetto HTTP File Server	TAG110
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:rejetto:http_file_server:*:*:*:*:*	HATVIBE and CHERRYSPY
Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	<a href="https://www.rejetto.com/hfs/">https://www.rejetto.com/hfs/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-36884</u>		Microsoft Office and Windows	RomCom
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	RomCom backdoor
Microsoft Windows Search Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362	T1059: Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884</a>










CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-9680</u>		Mozilla Firefox and Firefox ESR	RomCom
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEY	cpe:2.3:a:mozilla:firefox:*:*:*:esr:*:*:*	RomCom backdoor
Mozilla Firefox Use-After-Free Vulnerability		cpe:2.3:a:mozilla:firefox:*:*:*:*:-:*:*:*	
		cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	<a href="https://www.mozilla.org/en-US/firefox/new/">https://www.mozilla.org/en-US/firefox/new/</a> , <a href="https://www.mozilla.org/en-US/firefox/enterprise/#download">https://www.mozilla.org/en-US/firefox/enterprise/#download</a>





CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-18368</u>		Zyxel P660HN-T1A Routers	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:zyxel:p660hn-t1a_v2:-:*:*:*:*:*:*	Mirai botnet
Zyxel P660HN-T1A Routers Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	<a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-20090</u>		Buffalo WSR firmware	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:buffalo:wsr-2533dhpl2-bk_firmware:*:*:*:*:*:* cpe:2.3:h:buffalo:wsr-2533dhpl2-bk:-:*:*:*:*:*:*	Mirai botnet
Arcadyan Buffalo Firmware Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1202: Indirect Command Execution	<a href="https://www.buffalo-technology.com/service-support/downloads/software-firmware-updates/">https://www.buffalo-technology.com/service-support/downloads/software-firmware-updates/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-27348</u>		Apache HugeGraph-Server	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apache:hugegraph:*:*:*:*:*:*	Mirai botnet
Apache HugeGraph-Server Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1222: File and Directory Permissions Modification	<a href="https://hugegraph.apache.org/docs/download/download/">https://hugegraph.apache.org/docs/download/download/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-30525</u>		Zyxel Multiple Firewalls	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:zyxel:- .*.*.*.*.*.*.*.*	Mirai botnet
Zyxel Multiple Firewalls OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	<a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-10562</u>		Dasan GPON home routers	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dasannetworks:gpou_router_firmware:-:.*.*.*.*.*.*.*.* cpe:2.3:h:dasannetworks:gpou_router:-:.*.*.*.*.*.*.*.*	Mirai botnet
Dasan GPON Routers Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-10561</u>		Dasan GPON home routers	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dasannetworks:gpon_router_firmware:- :*:*:*:*:*:*	Mirai botnet
Dasan GPON Routers Command Injection Vulnerability		cpe:2.3:h:dasannetworks:gpon_router:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059: Command and Scripting Interpreter	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-17215</u>		Huawei HG532 router: All versions	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:huawei:hg532:- :*:*:*:*:*:*	Mirai botnet
Huawei HG532 RCE Vulnerability		cpe:2.3:o:huawei:hg532_firmware:- :*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<a href="https://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en">https://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2014-8361</u>		Realtek SDK: All versions	Matrix
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:dlink:dir-905l_firmware:*:*:*:*:*:*	Mirai botnet
Realtek SDK Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	<a href="https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055">https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46805</u>		Ivanti Connect Secure and Policy Secure	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21887</u>		Ivanti Connect Secure and Policy Secure	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-48788</u>		Fortinet FortiClientEMS	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	<a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-007">https://fortiguard.fortinet.com/psirt/FG-IR-24-007</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-3236</u>		Sophos Firewall	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sophos:firewall:*:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
Sophos Firewall Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	<a href="https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce">https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-26855</u>		Microsoft Exchange Server	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2021-26857</a>		Microsoft Exchange Server	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)			<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857</a>
	CWE ID		
	CWE-502		
		T1059: Command and Scripting Interpreter	


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2021-26858</a>		Microsoft Exchange Server	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)			<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a>
	CWE ID		
	CWE-20		
		T1505.003: Web Shell	


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-27065</u>		Microsoft Exchange Server	Earth Estries
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GHOSTSPIDER, SNAPPYBEE, MASOL RAT
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1505.003: Web Shell	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a>




# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div>Gelsemium</div>	China	Education, Gaming, Government, High-Tech, NGOs and religious organizations	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	WolfsBane, FireWood	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1587: Develop Capabilities; T1587.001: Malware; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1037: Boot or Logon Initialization Scripts; T1037.004: RC Scripts; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1574: Hijack Execution Flow; T1574.006: Dynamic Linker Hijacking; T1547: Boot or Logon Autostart Execution; T1547.013: XDG Autostart Entries; T1546: Event Triggered Execution; T1546.004: Unix Shell Configuration Modification; T1548: Abuse Elevation Control Mechanism; T1548.001: Setuid and Setgid; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestamp; T1070.009: Clear Persistence; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1222: File and Directory Permissions Modification; T1222.002: Linux and Mac File and Directory Permissions Modification; T1027: Obfuscated Files or Information; T1027.009: Embedded Payloads; T1014: Rootkit; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1082: System Information Discovery; T1083: File and Directory Discovery; T1056: Input Capture; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><u><b>TAG-110 (aka UAC-0063)</b></u></div>	Russia	Government entities, Human rights groups, and Educational institutions	Central Asia, Europe, and East Asia
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-23692	HATVIBE and CHERRYSPY	Rejetto HTTP File Server
<b>TTPs</b>			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1190: Exploit Public-Facing Application; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography;			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>RomCom (aka Storm-0978, Tropical Scorpis, UNC2596, Void Rabisu, DEV-0978)</u></p>	Russia	Construction, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Shipping and Logistics, Transportation	Europe and North America
	<b>MOTIVE</b>		
	Information theft and espionage, Financial gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2023-36884, CVE-2024-9680	RomCom backdoor	Microsoft Office and Windows, Mozilla Firefox and Firefox ESR

TTPs
<p>TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; T1189: Drive-by Compromise; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1068: Exploitation for Privilege Escalation; T1622: Debugger Evasion; T1480: Execution Guardrails; T1027: Obfuscated Files or Information; T1027.011: Fileless Storage; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1614: System Location Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Browser Session Hijacking; T1005: Data from Local System; T1114: Email Collection; T1114.001: Local Email Collection; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1657: Financial Theft;</p>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Matrix</u>	Russia	All	Asia, Americas
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	CVE-2017-18368, CVE-2021-20090, CVE-2024-27348, CVE-2022-30525, CVE-2022-30075, CVE-2018-10562, CVE-2018-10561, CVE-2018-9995, CVE-2017-17215, CVE-2017-17106, CVE-2014-8361	Mirai botnet	Zyxel P660HN-T1A Routers, Buffalo WSR Firmware, Apache HugeGraph-Server, Zyxel Multiple Firewalls, TP-Link Router AX50 Firmware, Dasan GPON home Routers, TBK DVR devices, Huawei HG532 router: All Versions, Zivif PR115-204-P-RS Webcams, Realtek SDK: All versions
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1059: Command and Scripting Interpreter; T1059.006: Python; T1543: Create or Modify System Process; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1036: Masquerading; T1110: Brute Force; T1046: Network Service Discovery; T1210: Exploitation of Remote Services; T1563: Remote Service Session Hijacking; T1563.001: SSH Hijacking; T1005: Data from Local System; T1102: Web Service; T1573: Encrypted Channel; T1496: Resource Hijacking; T1499: Endpoint Denial of Service; T1499.002: Service Exhaustion Flood;			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Earth Estries (aka Salt Typhoon, FamousSparrow, GhostEmperor, UNC2286)</u></p>	China	Engineering, Government, Hospitality and law firms, Chemical, Consulting Firms, Military, NGOs, Non-Profit Organizations, Technology, Telecommunications, Transportation	Brazil, Burkina Faso, Canada, France, Guatemala, Israel, Lithuania, Saudi Arabia, South Africa, Taiwan, Thailand, UK, APAC, Middle East, Africa, Parts of the Americas
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2023-46805, CVE-2024-21887, CVE-2023-48788, CVE-2022-3236, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065	GHOSTSPIDER, SNAPPYBEE (aka Deed RAT), MASOL RAT	Ivanti Connect Secure and Policy Secure, Fortinet FortiClientEMS, Sophos Firewall, Microsoft Exchange Server
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1071.001: Web Protocols; T1059.003: Windows Command Shell; T1112: Modify Registry; T1070.004: File Deletion; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1588.002: Tool; T1588: Obtain Capabilities; T1105: Ingress Tool Transfer; T1588.006: Vulnerabilities; T1587: Develop Capabilities; T1587.001: Malware			



# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nineteen exploited vulnerabilities** and block the indicators related to the threat actors **Gelsemium, TAG-110, RomCom, Matrix, Earth Estries**, and malware **WolfsBane, FireWood, HATVIBE, CHERRYSPY, RomCom, Mirai, GHOSTSPIDER, SNAPPYBEE, MASOL RAT**.

## 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

- Run a Scan to discover the assets impacted by the **nineteen exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Gelsemium, TAG-110, RomCom, Matrix, Earth Estries**, and malware **FireWood, WolfsBane, Kill-Floor, HATVIBE, Mirai, SNAPPYBEE** in Breach, and Attack Simulation(BAS).

# Threat Advisories

[WolfsBane and FireWood: Gelsemium's Expanding Arsenal Targets Linux Systems](#)

[When Trust Turns Toxic: Exploiting Avast Drivers in BYOVD Attacks](#)

[TAG-110: A Persistent Threat to Asia and Europe](#)

[RomCom Leverages Dual Zero-Day Exploits in Widespread Campaign](#)

[Matrix DDoS Campaign Exposes Alarming IoT Vulnerabilities](#)

[Growing Threat of Earth Estries Group Behind Major Telecom Breaches](#)

# 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
<u>WolfsBane</u>	SHA256	ccf8e4d6e661ceaea598851923bb8b983bd820ffd02448b8245e6ac780977784, fddec9ff14ebd957038f9c24843bff935c4f73651e9704b553dec116851f7ae5, 1ec286f2194199206e4ce345f1bf322b6b0b4c947b1cf32db59cca2d89370738
	SHA1	44947903b2bc760ac2e736b25574be33bf7af40b, 0ab53321bb9699d354a032259423175c08fec1a4, 8532eca04c0f58172d80d8a446ae33907d509377, b2a14e77c96640914399e5f46e1dec279e7b940f
	Domain	dsdsei[.]com
<u>FireWood</u>	SHA256	cff20753e36a4c942dc4dab5a91fd621a42330e17a89185a5b7262280bcd9263
	SHA1	0fef89711da11c550d3914debc0e663f5d2fb86c
	Domain	asidomain[.]com
<u>HATVIBE</u>	SHA256	332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725
<u>CHERRYSPY</u>	Domains	internalsecurity[.]us, errorreporting[.]net, lanmangraphics[.]com, retaildemo[.]info, tieringservice[.]com, enrollmenttdm[.]com
<u>RomCom</u>	SHA1	a4aad0e2ac1ee0c8dd25968fa4631805689757b6, ca6f8966a3b2640f49b19434ba8c21832e77a031, 21918cfd17b378eb4152910f1246d2446f9b5b11,

Attack Name	TYPE	VALUE
<b>RomCom</b>	SHA1	703a25f053e356eb6ece4d16a048344c55dc89fd, abb54c4751f97a9fc1c9598fed1ec9fb9e6b1db6, a9d445b77f6f4e90c29e385264d4b1b95947add5
	IPv4	194[.]87[.]189[.]171, 178[.]236[.]246[.]241, 62[.]60[.]238[.]81, 147[.]45[.]78[.]102, 46[.]226[.]163[.]67, 62[.]60[.]237[.]116, 62[.]60[.]237[.]38, 194[.]87[.]189[.]19, 45[.]138[.]74[.]238, 176[.]124[.]206[.]88
	SHA256	05681ff7cae6b28f5714628a269caa5115da49c94737ce82ec09b431 2e40fd26, 068117b406940ac510ed59efd1d7c7651f645a31bd70db6de16aba1 2c055aae6, 28950cff484550312f2c91e17d7da89300981f17b19a7cd9c5432a4b 76e281d2, 28b2a0f5441a5c50c73bb2044e48c7e404b848b84da9d1043771c78 3e17647d8, 3e3a7116eeadf99963077dc87680952cca87ff4fe60a552041a2def6b 45cbeea, ff8ecccc561e07a4d3b1a229b307cd1e787fe9fe21a781f361e3f0175 0def89c, 2ba51d7e338242bc6a8109317b91dd13137e296693c535ceacc1288 775acc81f, 65778e3afc448f89680e8de9791500d21a22e2279759d8d93e2ece2 bc8dae04d, 0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5 b866b2a, 6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a5 42c7b261d
<b>Mirai</b>	MD5	df521f97af1591efff0be31a7fe8b925, d653fa6f1050ac276d8ded0919c25a6f, 866c52bc44c007685c49f5f7c51e05ca
	SHA1	ada6c6646cc86e12a09355944700deb8abd2a55, 339c5f229ae62f7139bf7de6f8c6ab136213e8c1, 83bb15de9ff6d7501897689e97907fe80f329604
	SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbb a2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2 214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c0491 0ad2f067

Attack Name	TYPE	VALUE
<u>GHOSTSPIDER</u>	IPv4	139[.]59[.]108[.]43, 185[.]105[.]11[.]243, 143[.]198[.]92[.]175, 139[.]99[.]114[.]108, 139[.]59[.]236[.]31, 104[.]194[.]153[.]65
	Domains	billing[.]clothworls[.]com, helpdesk[.]stnekpro[.]com, jasmine[.]lhousewares[.]com, private[.]royalnas[.]com, telcom[.]grishamarkovgf8936[.]workers[.]dev
<u>SNAPPYBEE</u>	SHA256	fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5, fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098, 25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b, 6d64643c044fe534dbb2c1158409138fcded757e550c6f79ead15e69a7865bc, b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac, 05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870, 1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296
	IPv4	158[.]247[.]222[.]165, 91[.]245[.]253[.]27
	Domains	api[.]solveblemten[.]com, esh[.]hooovernamosong[.]com
<u>MASOL RAT</u>	SHA256	44ea2e85ea6cffba66f5928768c1ee401f3a6d6cd2a04e0d681d695f93cc5a1f

# 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  
**December 2, 2024 • 4:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)