

Date of Publication  
January 13, 2025



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

06 to 12 JANUARY 2025

# Table Of Contents

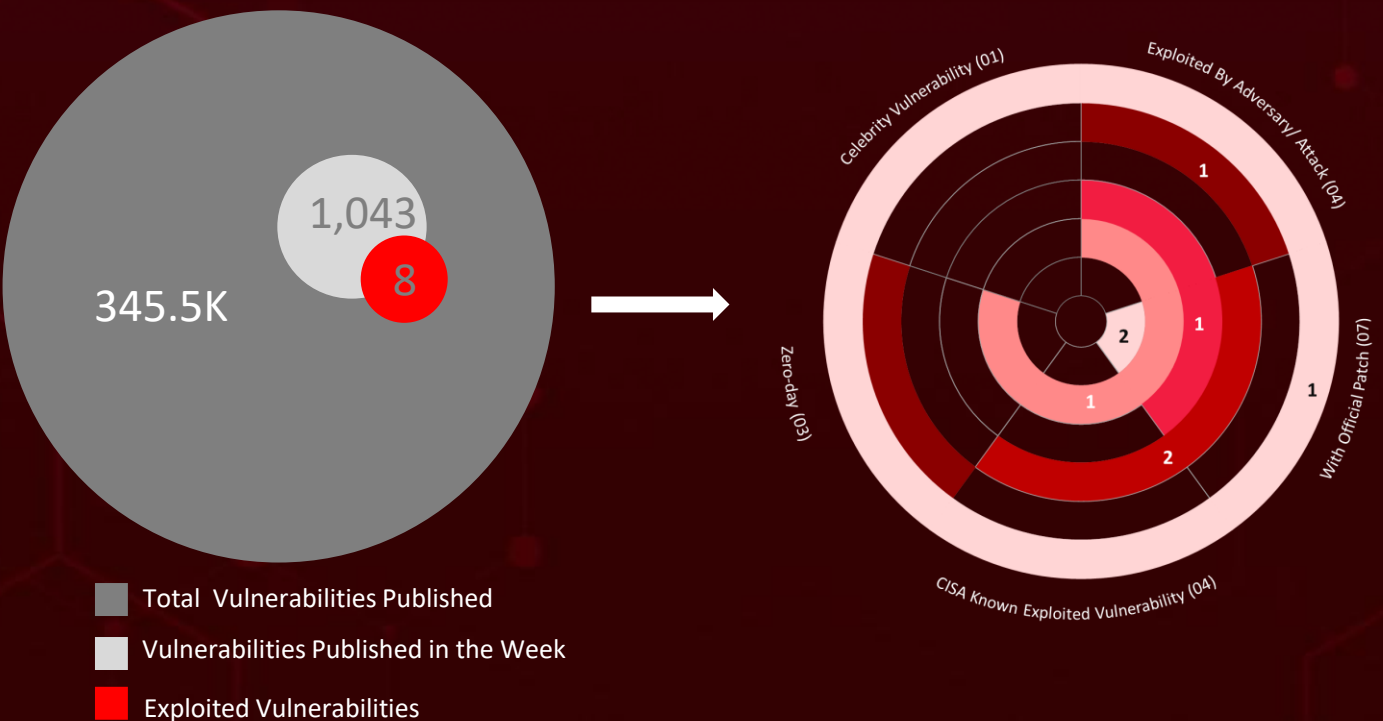
<a href="#"><u>Summary</u></a>	03
<a href="#"><u>High Level Statistics</u></a>	04
<a href="#"><u>Insights</u></a>	05
<a href="#"><u>Targeted Countries</u></a>	06
<a href="#"><u>Targeted Industries</u></a>	07
<a href="#"><u>Top MITRE ATT&amp;CK TTPs</u></a>	07
<a href="#"><u>Attacks Executed</u></a>	08
<a href="#"><u>Vulnerabilities Exploited</u></a>	17
<a href="#"><u>Adversaries in Action</u></a>	22
<a href="#"><u>Recommendations</u></a>	23
<a href="#"><u>Threat Advisories</u></a>	24
<a href="#"><u>Appendix</u></a>	25
<a href="#"><u>What Next?</u></a>	27

# Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **ten** attacks were executed, **eight** vulnerabilities were uncovered, and **one** active adversaries was identified, underscoring the persistent danger of cyberattacks.

HiveForce Labs has uncovered a significant security threat in which threat actors are exploiting **CVE-2021-26855** in Microsoft Exchange Server to deploy the **EAGERBEE** backdoor, specifically targeting government organizations and internet service providers (ISPs) in the Middle East. Recent investigations revealed the use of a sophisticated service injector, designed to stealthily embed the backdoor into active system services, thereby improving its persistence and evasion capabilities. In addition, previously undocumented plugins are deployed after the backdoor installation, further complicating the detection and mitigation of the attack.

In parallel, critical vulnerabilities in Mitel MiCollab, including **CVE-2024-41713**, **CVE-2024-55550**, and **CVE-2024-35286**, have been identified, exposing organizations to significant risks. These vulnerabilities could allow unauthorized access, jeopardizing the confidentiality, integrity, and availability of affected systems. CVE-2024-41713 and CVE-2024-35286 can also be chained together, enabling more sophisticated attacks that could lead to system compromise, data theft, and disruption of enterprise operations. Additionally, the **Gayfemboy** botnet, an advanced Mirai variant exploiting a 0-day vulnerability in Four-Faith industrial routers, has been identified. With over 15,000 active nodes, this botnet has conducted massive DDoS attacks, peaking at 100GB of traffic, posing a growing and immediate risk to global users.



# High Level Statistics

10

Attacks  
Executed

8

Vulnerabilities  
Exploited

1

Adversaries in  
Action

- [EAGERBEE](#)
- [Gayfemboy](#)
- [DRYHOOK](#)
- [PHASEJAM](#)
- [SPAWNANT](#)
- [SPAWNMOLE](#)
- [SPAWNSNAIL](#)
- [SPAWNSLOTH](#)
- [Hexalocker](#)
- [Skuld Stealer](#)
- [CVE-2024-43405](#)
- [CVE-2021-26855](#)
- [CVE-2024-41713](#)
- [CVE-2024-55550](#)
- [CVE-2024-35286](#)
- [CVE-2024-12856](#)
- [CVE-2025-0282](#)
- [CVE-2025-0283](#)
- [UNC5337](#)



# Insights

## CVE-2024-43405

Critical flaw in Nuclei allows signature bypass and malicious code execution, with a public PoC available

**EAGERBEE backdoor** has evolved, now employing a sophisticated service injector to embed backdoors into active system services for enhanced persistence and evasion

## HexaLocker

active since mid-2024, now combines data theft with file encryption, amplifying its impact. Leveraging double extortion and anti-analysis tools

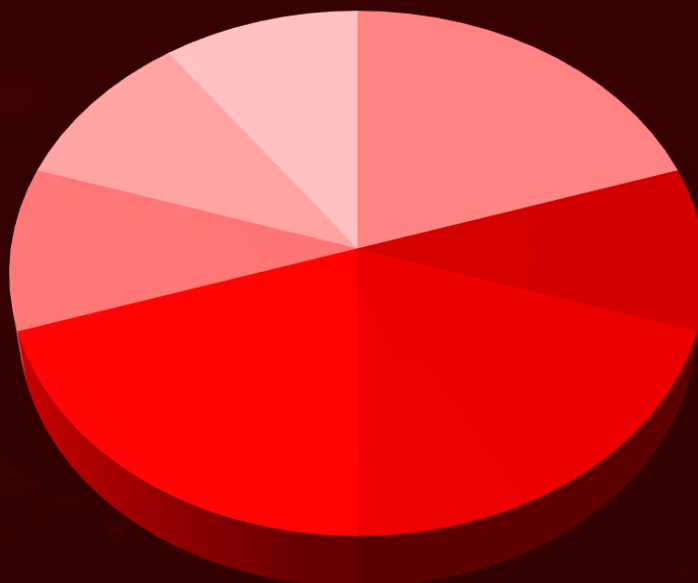
## Critical Mitel MiCollab Flaws

enabling authentication bypass and unauthorized file access. These vulnerabilities can be chained for advanced attacks, risking system compromise

**Gayfemboy botnet**, a sophisticated Mirai variant, targets a 0-day vulnerability in Four-Faith industrial routers, boasting 15,000+ active nodes and launching DDoS attacks peaking at 100GB traffic

**Ivanti Zero-day Flaw** exploited by threat actors to deploy malwares like DRYHOOK, PHASEJAM and SPAWN ecosystem

## Threat Distribution



■ Backdoor   ■ Botnet   ■ Stealer   ■ Dropper  
■ Web Shell   ■ Rootkit   ■ Ransomware

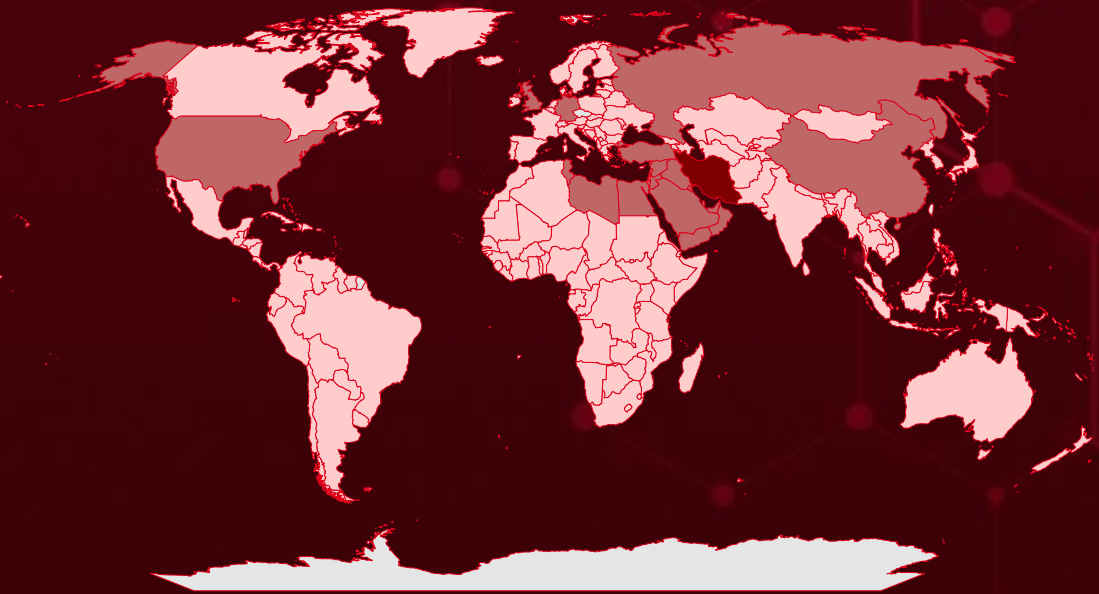


# Targeted Countries

Most



Least



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

Countries
Iran
Tunisia
Bahrain
United States
China
Singapore
Egypt
United Arab Emirates
Germany
Oman
Qatar
Russia
Saudi Arabia
Iraq
Syria
Israel
Turkey
Jordan
United Kingdom
Kuwait
Yemen
Lebanon

Countries
Libya
Senegal
Myanmar
Uganda
Brunei
Papua New Guinea
Bulgaria
Sudan
Burkina Faso
Mexico
Burundi
Nigeria
Cabo Verde
Bangladesh
Cambodia
Somalia
Cameroon
Timor-Leste
Canada
Venezuela
Central African Republic
Mongolia

Countries
Chad
Netherlands
Chile
Bahamas
Algeria
Poland
Colombia
Samoa
Comoros
Belarus
Congo
Spain
Costa Rica
Belgium
Côte d'Ivoire
Belize
Croatia
Bosnia and Herzegovina
Cuba
Zimbabwe
Cyprus
Moldova

Countries
North Korea
Honduras
Norway
Hungary
Pakistan
Iceland
Panama
India
Paraguay
Indonesia
Philippines
Antigua and Barbuda
Portugal
Argentina
Romania
Ireland
Rwanda
Armenia
Saint Lucia
Italy
San Marino
Jamaica

# Targeted Industries



## TOP MITRE ATT&CK TTPs

**T1588.006**  
Vulnerabilities

**T1588**  
Obtain  
Capabilities

**T1059**  
Command and  
Scripting  
Interpreter

**T1083**  
File and  
Directory  
Discovery

**T1057**  
Process  
Discovery

**T1082**  
System  
Information  
Discovery

**T1016**  
System Network  
Configuration  
Discovery

**T1027**  
Obfuscated  
Files or  
Information

**T1003**  
OS Credential  
Dumping

**T1562**  
Impair  
Defenses

**T1505.003**  
Web Shell

**T1068**  
Exploitation for  
Privilege  
Escalation

**T1070**  
Indicator  
Removal

**T1140**  
Deobfuscate/D  
ecode Files or  
Information

**T1584**  
Compromise  
Infrastructure

**T1036**  
Masquerading

**T1555**  
Credentials from  
Password Stores

**T1078**  
Valid Accounts

**T1569**  
System  
Services

**T1041**  
Exfiltration Over  
C2 Channel



# 🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>EAGERBEE</u></b>	<p>The EAGERBEE backdoor showcases advanced capabilities, including a service injector for seamless deployment and plugins designed for delivering payloads, accessing files, and enabling remote control. EAGERBEE further enhances its operations by loading additional modules from remotely-hosted PE files managed by C2 server. In its most recent campaign, EAGERBEE employs an injector DLL to activate the backdoor. Once operational, it gathers system information and exfiltrates the collected data to a remote server via a TCP socket.</p>	Exploiting Vulnerabilities	CVE-2021-26855
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		System Compromise	Microsoft Exchange Server
-			<b>PATCH LINK</b>
	<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>		
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	9d93528e05762875cf2d160f15554f44, c651412abdc9cf3105dfbaf54766c44, 26d1adb6d0bcc65e758edaf71a8f665d		

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
<a href="#"><u>Gayfemboy</u></a>	The Gayfemboy botnet represents a highly evolved variant of Mirai, leveraging a 0-day vulnerability in Four-Faith industrial routers to establish its foothold. Operating with remarkable sophistication, it boasts over 40 distinct grouping categories and maintains more than 15,000 daily active nodes.	Exploiting Vulnerabilities	CVE-2024-12856
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Botnet			
<b>ASSOCIATED ACTOR</b>		DDOS attack	Four-Faith F3x24 and F3x36
-			<b>PATCH LINK</b>
	No patch		
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA1	3287158c35c93a23b79b1fbb7c0e886725df5faa, ba9224828252e0197ea5395dad9bb39072933910, fe72a403f2620161491760423d21e6a0176852c3		

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><u>DRYHOOK</u></b>	<p>DRYHOOK is a Python-based malware designed to steal credentials. Specifically, it modifies a system component called DSAuth.pm, which is responsible for handling authentication, in order to capture successful login attempts. When executed, the malicious script accesses the file located at /home/perl/DSAuth.pm, reading its contents into a buffer. It then employs regular expressions to search for and replace specific lines of code, effectively manipulating the authentication process to exfiltrate sensitive information.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Stealer			
<b>ASSOCIATED ACTOR</b>		UNC5337	Steal Data
	<b>PATCH LINK</b>		
			<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	61bb586dc4e047ab081ef6ca65684e48		

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><u>PHASEJAM</u></b>	<p>PHASEJAM is a malicious bash shell script that targets Ivanti Connect Secure appliances. Its primary functionality includes embedding a web shell into the getComponent.cgi and restAuth.cgi files, providing attackers with remote access to the system. Additionally, PHASEJAM disrupts system upgrades by modifying the DSUpgrade.pm file, effectively preventing crucial security updates. The malware also alters the remotedebg executable, enabling the execution of arbitrary commands when a specific parameter is provided. These capabilities allow attackers to maintain persistent control over the compromised system.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Dropper			
<b>ASSOCIATED ACTOR</b>		System Compromise	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
UNC5337			<b>PATCH LINK</b>
	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>		
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	d18e5425ecd9608ecb992606b974e15d		

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><u>SPAWNANT</u></b>	<p>SPAWNANT is an ELF32 executable that installs three malicious components from the SPAWN family, each serving a distinct purpose. The three are component, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH. Together, these components enable SPAWNANT to maintain persistence across system upgrades. This ensures that SPAWNANT and its supporting components remain active, even after system upgrades, securing the attacker's foothold for long-term exploitation.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Installer/ Dropper		Drops other Malware	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5337			<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
File path	/root/lib/libupgrade.so		

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><u>SPAWNMOLE</u></b>	<p>SPAWNMOLE is a tunneler that embeds itself into the web process, quietly monitoring network traffic. It takes control of the accept function to inspect incoming connections, filtering out any malicious traffic from the attacker. SPAWNMOLE stays inactive until it detects a specific pattern of magic bytes, which triggers its malicious behavior. Once activated, it redirects the harmful traffic to a remote host provided by the attacker, while allowing harmless traffic to flow to the legitimate web server without alteration. This stealthy method enables SPAWNMOLE to deliver its payload while avoiding detection.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Tunneler/ Web Shell		Deliver Payloads	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5337	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>		
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	a638fd203ddb540d0484d8e00490df06, 4f79c70cce4207d0ad57a339a9c7f43c		
Domain	libdsproxy[.]so		

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><u>SPAWNSNAIL</u></b>	<p>SPAWNSNAIL is an SSH backdoor specifically targeting Ivanti devices. It has the capability to inject a chosen binary into other processes, enabling it to run a local SSH backdoor when injected into the dsmdm process.</p> <p>Additionally, SPAWNSNAIL can inject further malware into the dslogserver, expanding its control and enabling additional malicious activities on the compromised system. This allows attackers to maintain persistent access and deploy further threats with minimal detection.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		System Compromise	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5337	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>		
IOC TYPE	VALUE		
MD5	e7d24813535f74187db31d4114f607a1		
Domain	libdsmeeting[.]so		

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>SPAWNSLOTH</u>	<p>SPAWNSLOTH is a log tampering utility designed to manipulate system logs, effectively hiding traces of malicious activity. By altering or erasing log entries, SPAWNSLOTH helps attackers cover their tracks, making it difficult to detect their presence or the actions they've taken on the compromised system.</p>	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Log Tampering/ Rootkit		Manipulate system logs	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5337	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>		
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	4acfc5df7f24c2354384f7449280d9e0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>HexaLocker</u>	<p>HexaLocker ransomware, first identified in mid-2024, has evolved with a significant update in its latest version. This update integrates the open-source Skuld Stealer, a tool specifically designed to extract sensitive data from infected systems before initiating file encryption. The newest iteration of HexaLocker, written in Go, showcases more advanced capabilities, including the ability to download and execute Skuld Stealer, enabling attackers to harvest valuable information before encrypting the victim's files.</p>	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Encrypt Data, Steal Data	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-	-		
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	0347aa0b42253ed46fdb4b95e7ffafa40ba5e249dfb5c8c09119f327a1b4795a, 28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de506333b960, d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15aded2e05		




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>Skuld</u>	<p>Skuld is an open-source tool designed to target Windows systems and steal sensitive user data from a wide range of applications, including Discord, web browsers, cryptocurrency wallets, and more. Once deployed on a victim's machine, Skuld extracts valuable information such as login credentials, personal data, and wallet keys. Its ability to compromise various applications makes Skuld a versatile and dangerous tool for attackers looking to collect and exploit user information.</p>	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Stealer			-
<b>ASSOCIATED ACTOR</b>		Steal Data	<b>PATCH LINK</b>
-			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c350988d8		
URL	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe		




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
<a href="#"><u>CVE-2024-43405</u></a>		Nuclei prior to version 3.3.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:projectdiscovery:nuclei:*:*:*:*:go:*:*	-
ProjectDiscovery Nuclei Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	<a href="https://github.com/projectdiscovery/nuclei/releases"><u>https://github.com/projectdiscovery/nuclei/releases</u></a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2021-26855</u></a>	ProxyLogon	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	EAGERBEE backdoor
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application; T1078: Valid Accounts	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855"><u>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</u></a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-41713</u></a>		MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1016: System Network Configuration Discovery	<a href="https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029">https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-55550</u></a>		MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1078: Valid Accounts	<a href="https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029">https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-35286</a>		MiCollab Version 9.8.0.33 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*	-
Mitel MiCollab SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1016: System Network Configuration Discovery	<a href="https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin240014001-v10.pdf">https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin240014001-v10.pdf</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-12856</a>		Four-Faith F3x24 and F3x36	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:h:four-faith:f3x24:*:*:*:*:*:*:*	Gayfemboy Botnet
Four-Faith OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
CWE-78	T1499: Endpoint Denial of Service; T1078.001: Default Accounts	No patch	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-0282</u>		Ivanti Connect Secure: 22.7R2 through 22.7R2.4 Ivanti Policy Secure: 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	UNC5337
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2025-0283</a></u>		Ivanti Connect Secure: 22.7R2.4 and prior, 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.2 and prior Ivanti Neurons for ZTA gateways: 22.7R2.3 and prior	UNC5337
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1068: Exploitation for Privilege Escalation; T1210: Exploitation of Remote Services	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b><u>UNC5337</u></b>	China	All	Worldwide
	<b>MOTIVE</b>		
	Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2025-0282, CVE-2025-0283	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
<b>TTPs</b>			
TA0001: Initial Access; TA0042: Resource Development; TA0002: Execution; TA0004: Privilege Escalation; T1059: Command and Scripting Interpreter; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1565: Data Manipulation; T1068: Exploitation for Privilege Escalation; T1505.003: Web Shell; T1003: OS Credential Dumping; T1070: Indicator Removal; T1562.001: Disable or Modify Tools; T1562: Impair Defenses			



# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actor **UNC5337** and malware **EAGERBEE, Gayfemboy, DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH, Hexalocker, Skuld Stealer.**

## 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 **eight exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UNC5337** and malware **Gayfemboy, Hexalocker, and Skuld Stealer** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Nuclei Vulnerability Exposes Systems to Malicious Code](#)

[Eagerbee Unmasked: Sophisticated Malware Strikes Middle East](#)

[Critical Flaws in Mitel MiCollab: Path Traversal and SQL Injection Risks Unveiled](#)

[Gayfemboy Botnet: Evolution of a Potent Threat](#)

[Critical Ivanti Zero-day Flaw Exploited in the Wild](#)

[HexaLocker Ransomware Returns with a Vengeance](#)

# 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>EAGERBEE</u>	MD5	9d93528e05762875cf2d160f15554f44, c651412abdc9cf3105dfbaf54766c44, 26d1adb6d0bcc65e758edaf71a8f665d
<u>Gayfemboy</u>	SHA1	3287158c35c93a23b79b1fbb7c0e886725df5faa, ba9224828252e0197ea5395dad9bb39072933910, fe72a403f2620161491760423d21e6a0176852c3
	SHA256	3ee4d3222dd1856ca58de9715342d5c83562578f869c3482b538ab2c8eb 3c832, a0241e3e2a8fb48e2fa0a4ebb72054309f70c79de286b1d00f640347f81e 69bd
<u>DRYHOOK</u>	MD5	61bb586dc4e047ab081ef6ca65684e48
<u>PHASEJAM</u>	MD5	d18e5425ecd9608ecb992606b974e15d
	File Path	/tmp/s
<u>SPAWNANT</u>	File Path	/root/lib/libupgrade.so

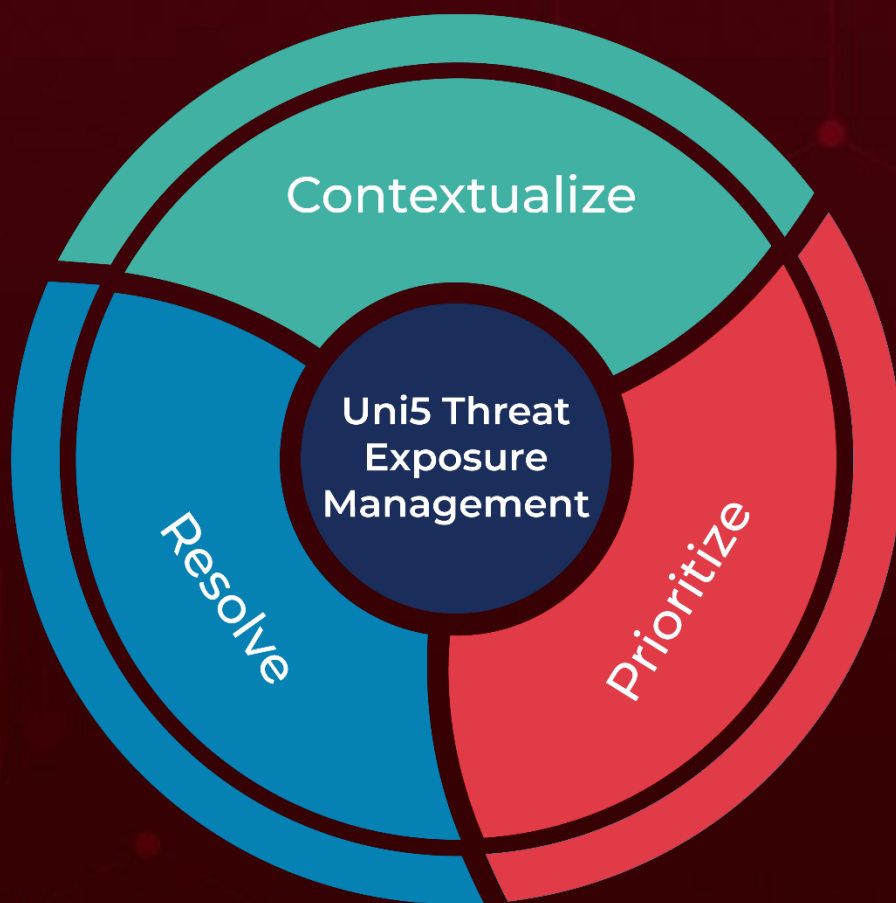
Attack Name	TYPE	VALUE
<u>SPAWNMOLE</u>	File Path	/root/home/lib/libsocks5.so
	MD5	a638fd203ddb540d0484d8e00490df06, 4f79c70cce4207d0ad57a339a9c7f43c
	Domain	libdsproxy[.]so
<u>SPAWNSNAIL</u>	File Path	/root/home/lib/libsshd.so
	MD5	e7d24813535f74187db31d4114f607a1
	Domain	libdsmeeting[.]so
<u>SPAWNSLOTH</u>	File Path	/tmp/.liblogblock.so
	MD5	4acfc5df7f24c2354384f7449280d9e0
<u>HexaLocker</u>	SHA256	0347aa0b42253ed46fdb4b95e7ffafa40ba5e249dfb5c8c09119f327a1b 4795a, 28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de5063 33b960, d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15ad ed2e05
<u>Skuld</u>	SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c35 0988d8
	URL	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe

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

# What Next?

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

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



REPORT GENERATED ON

**January 13, 2025 • 7:10 AM**

© 2025 All Rights are Reserved by Hive Pro



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