

Date of Publication  
November 11, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

4 to 10 November 2024

# Table Of Contents

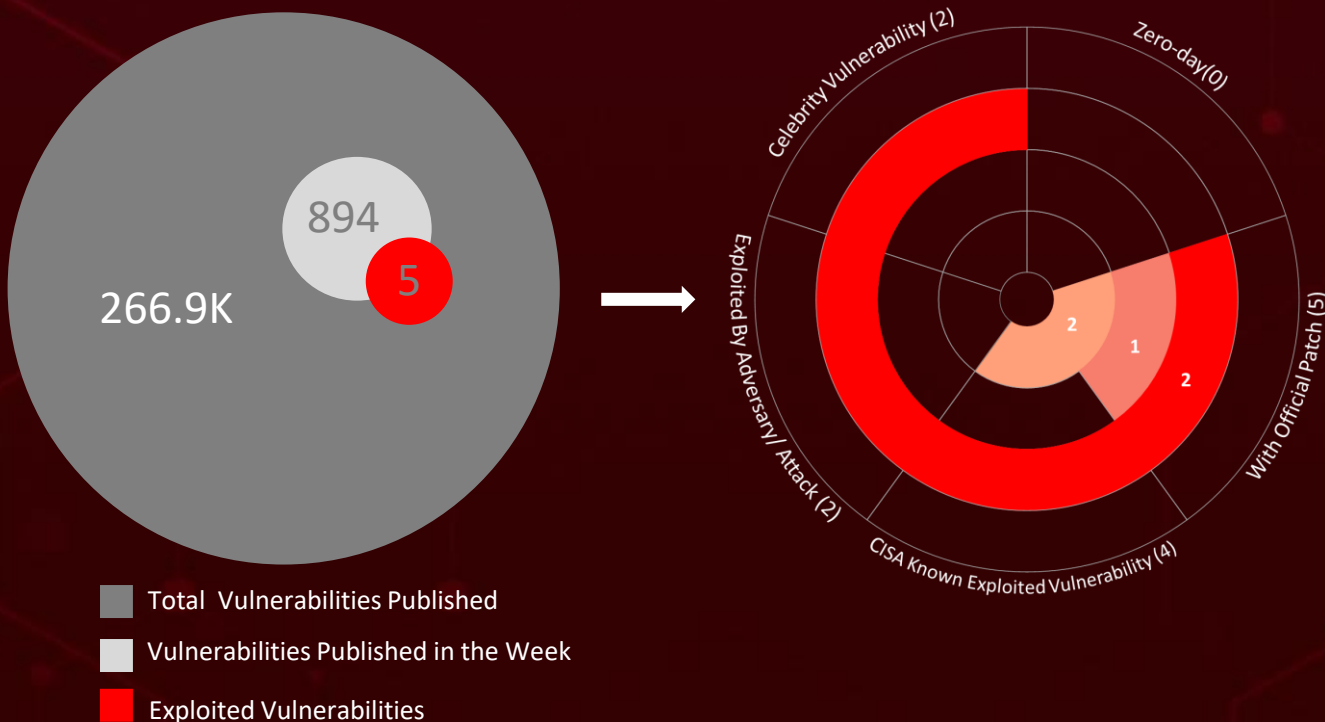
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	20

# Summary

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

Additionally, threat actors exploited the SharePoint Remote Code Execution flaw ([CVE-2024-38094](#)) to infiltrate corporate networks, deploying a Fast Reverse Proxy and custom webshell to maintain control over compromised systems.

Furthermore, this week, Iranian cyber group [Emennet Pasargad](#), now operating as Aria Sepehr Ayandehsazan (ASA), conducts global hack-and-leak operations to destabilize and undermine trust in Israel's information space. The [CRON#TRAP](#) phishing campaign uses QEMU to deploy a custom TinyCore Linux instance on Windows systems, employing virtualization to create stealthy, persistent backdoors. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

5

Attacks  
Executed

5

Vulnerabilities  
Exploited

1

Adversaries in  
Action

- [Rhadamanthys](#)
- [BeaverTail](#)
- [InvisibleFerret](#)
- [Chisel](#)
- [PivotBox](#)

- [CVE-2024-38094](#)
- [CVE-2019-0708](#)
- [CVE-2018-7600](#)
- [CVE-2024-5910](#)
- [CVE-2024-9464](#)

- [Emennet](#)  
[Pasargad](#)



# Insights

**North Korean Threat Actors** Use Advanced Obfuscation in **Contagious Interview and WageMole Campaigns** to Target Windows and macOS.

## "CopyRh(ight)adamantys"

Phishing Campaign Uses AI-Enhanced Rhadamanthys Stealer with Targeted Impersonation Tactics.

### **CVE-2024-38094:**

Threat Actors Exploit SharePoint RCE Flaw to Deploy Proxy and Webshell for Network Control.

**Emennet Pasargad**, Iranian cyber group, now conducts global hack-and-leak operations to destabilize and undermine trust in Israel's information space.

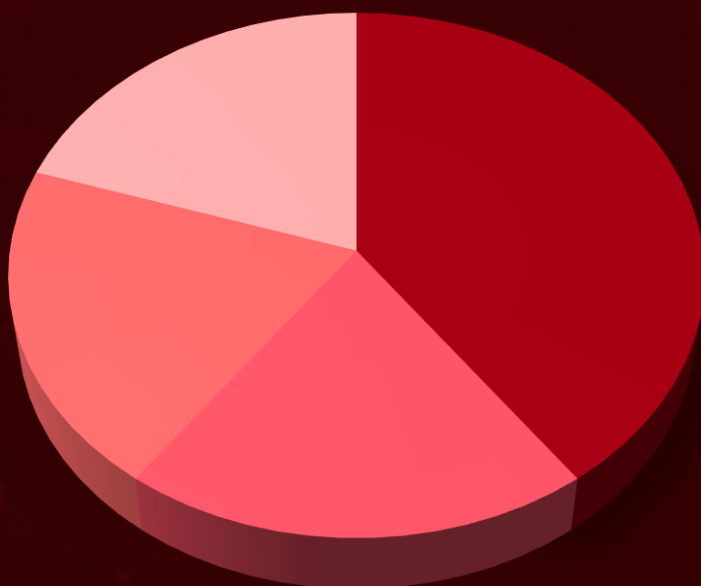
### **CVE-2024-5910:**

Critical Vulnerability in Palo Alto's Expedition Tool Enables Admin Account Takeover.

### **CRON#TRAP**

Phishing Campaign Leverages QEMU for Stealthy TinyCore Linux Deployment on Windows.

## Threat Distribution



■ Backdoor ■ Information stealer ■ Hack Tool ■ Trojan

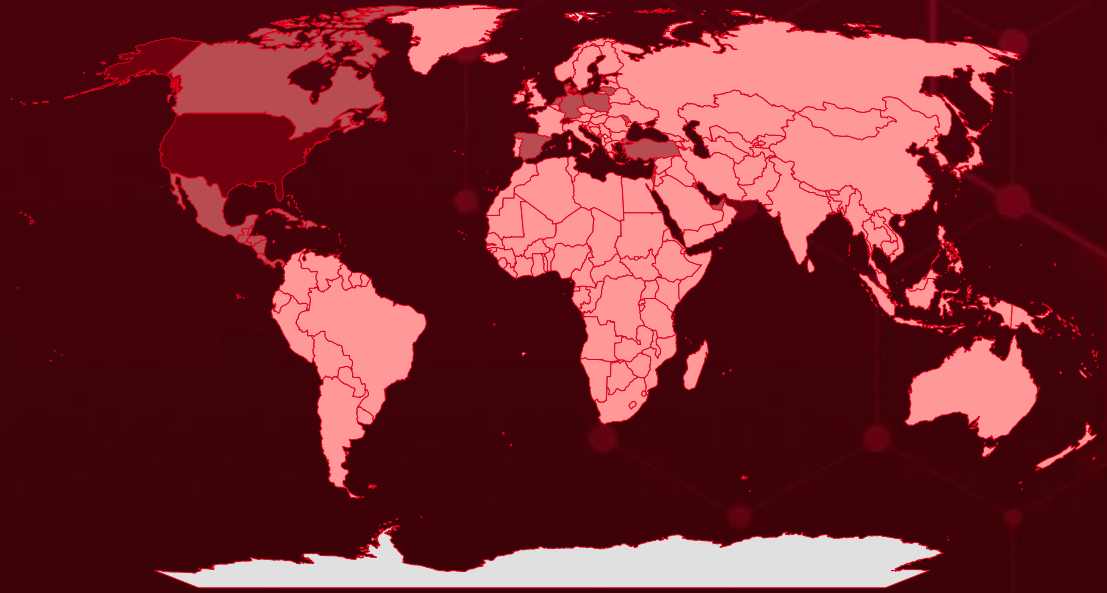


# Targeted Countries

Most



Least

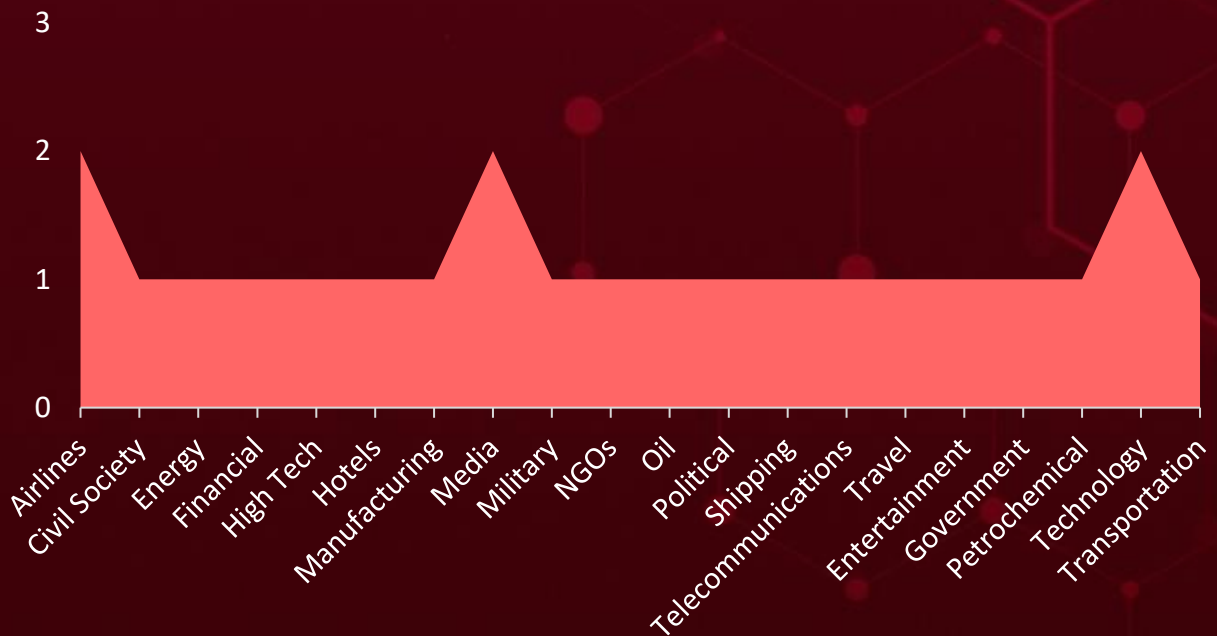


Powered by Bing

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

Countries	Countries	Countries	Countries
United States	Guatemala	South Korea	Belgium
Switzerland	United Arab Emirates	Qatar	Czech Republic (Czechia)
Malta	Honduras	Venezuela	Qatar
Germany	United States	Romania	United Kingdom
Costa Rica	Jamaica	Macau	Saint Kitts and Nevis
Liechtenstein	Andorra	Chile	Ecuador
Israel	Lithuania	Mongolia	Saudi Arabia
Moldova	Antigua and Barbuda	Saudi Arabia	Yemen
Saint Lucia	Barbuda	Norway	Slovenia
Monaco	Mexico	Serbia	Afghanistan
Denmark	Bahamas	Russia	St. Vincent & Grenadines
Montenegro	Panama	Slovakia	Albania
Haiti	Barbados	Sierra Leone	Tanzania
Netherlands	Trinidad and Tobago	Slovenia	Algeria
Lebanon	Belize	Sweden	Turkmenistan
Poland	Canada	South Korea	Egypt
Nicaragua	Grenada	Ukraine	United States Virgin Islands
San Marino	Latvia	Croatia	Angola
Bahrain	Latvia	Kiribati	Zimbabwe
Spain	Saint Vincent and the Grenadines	Sweden	Anguilla
Cuba	Nepal	Libya	Kyrgyzstan
Dominica	Palestine	Cyprus	Estonia
Kuwait	Tonga	Maldives	Lesotho
Dominican Republic	Peru	Syria	Argentina
El Salvador	Marshall Islands	Albania	
Turkey	Bulgaria	Taiwan	
		Mozambique	
		Thailand	

# Targeted Industries



## TOP MITRE ATT&CK TTPs

**T1071.001**  
Web Protocols

**T1027**  
Obfuscated  
Files or  
Information

**T1204.002**  
Malicious File

**T1041**  
Exfiltration  
Over C2  
Channel

**T1190**  
Exploit Public-  
Facing  
Application

**T1596**  
Search Open  
Technical  
Databases

**T1566**  
Phishing

**T1083**  
File and  
Directory  
Discovery

**T1219**  
Remote  
Access  
Software

**T1036**  
Masquerading

**T1218**  
System Binary  
Proxy  
Execution

**T1204**  
User Execution

**T1204.001**  
Malicious Link

**T1110.002**  
Password  
Cracking

**T1059**  
Command and  
Scripting  
Interpreter

**T1055**  
Process  
Injection

**T1059.006**  
Python

**T1574**  
Hijack  
Execution  
Flow

**T1588**  
Obtain  
Capabilities

**T1068**  
Exploitation for  
Privilege  
Escalation



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u><a href="#">Rhadamanthys</a></u>	Rhadamanthys is an information stealer featuring a versatile array of modules and a multi-layered architecture. Available on the black market and regularly updated, it poses a continual threat. Its sophisticated design enables it to evade detection while carrying out various malicious activities, including the theft and exfiltration of sensitive information.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Operational Disruption, Data Theft, Financial Loss	-
Information stealer			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
-			
IOC TYPE	VALUE		
SHA256	cf9d93951e558ed22815b34446cfa2bd2cf3d1582d8bd97912612f4d4128a64e, 48aaa2dec95537cdf9fc471dbcbb4ff726be4a0647dbdf6300fa61858c2b0099, 00fc4b8a4c65c06766608f3ef3f92385c8e147f5991dabe290e33dd14b39ad44, 0ad65fd0897a6547f6febf398708ab2d423a8f8834b53136219cb490ec3ebd13, 11ba24d023b544e28c37b6cb8afe27d06638175d7f56c2e4d4ff97bf7bd813b6		

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>BeaverTail</u></a>	BeaverTail is a JavaScript stealer malware that targets software developers through a supposed job interview process. It can steal sensitive information from web browsers, crypto wallets, and system data.	Social engineering	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Trojan			
<b>ASSOCIATED ACTOR</b>		Data theft	Windows, macOS
-			<b>PATCH LINK</b>
	-		
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	d801ad1beeab3500c65434da51326d7648a3c54923d794b2411b7b6a2960f31e, d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6, c0110cb21ae0e7fb5dec83ca90db9e250b47a394662810f230eb621b0728aa97, 9e3a9dbf10793a27361b3cef4d2c87dbd3662646f4470e5242074df4cb96c6b4, 91f96f2ddfa293806ec3effb8e05bc6941660237de90215b23281d706a2bc706		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>InvisibleFerret</u></a>	InvisibleFerret is a newly discovered, cross-platform Python backdoor malware that is part of a campaign targeting job seekers. It consists of various components for fingerprinting, remote control, keylogging, data exfiltration, browser stealing, and downloading the AnyDesk client for additional control.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		Data theft	Windows, macOS
-			<b>PATCH LINK</b>
	-		
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	5bdd872a2a49b5682b297350222eee847c0a1e52125688acb9aa8a7b9ec4de29		
SHA1	9c1fddc45a6ad5a5b738e1ead5efd46051fdfd35		
MD5	2f7e6d05caab11bac4d585108a14d3c2		




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>PivotBox</u></b>	PivotBox is a customized version of TinyBox, emulated using QEMU, which is designed to run in the background with preconfigured settings. It has been modified to include a Chisel backdoor.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Remote access, Data theft	Windows
			<b>PATCH LINK</b>
			--
<b>TYPE</b>			
Backdoor			
<b>ASSOCIATED ACTOR</b>			
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	5A8BC06587CE40B3A8D8DD4037D0EF272EFC64A69E21F6689FFE3F5FBB04A468, 4C91070877C6D116F5A27EFADDBBFBC339455628E9D6585A4EA5F9B6972BF92B		



NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>Chisel</u></b>	Chisel is an Open Source tool designed for fast TCP/UDP tunneling, secured using SSH and transported over HTTP. Developed in Go and employed by Threat Actors for establishing C2 connections.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Remote access, Data exfiltration	-
			<b>PATCH LINK</b>
			-
<b>TYPE</b>			
Hack tool			
<b>ASSOCIATED ACTOR</b>			
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	3E6A47DA0A226A4C98FB53A06EC1894B4BFD15E73D0CEA856B7D2A001CADA7E9		




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><a href="#">CVE-2024-38094</a></u>		Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019	-
	ZERO-DAY	Microsoft SharePoint Enterprise Server 2016	
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*	-
Microsoft SharePoint Remote Code Execution Vulnerability			ASSOCIATED TTPs
		CWE ID	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1078 : Valid Accounts
	CWE-502		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-0708</u>	BlueKeep	CBL Mariner Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	Emennet Pasargad
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY		
Microsoft Remote Desktop Services Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1021.001: Remote Desktop Protocol, T1068 : Exploitation for Privilege Escalation, T1059: Command and Scripting	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-7600</u>	Drupalgeddon2	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1	Emennet Pasargad
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY		
Drupal Core Remote Code Execution Vulnerability		cpe:2.3:a:drupal:drupal:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<a href="https://groups.drupal.org/security/faq-2018-002">https://groups.drupal.org/security/faq-2018-002</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-5910</a>		Palo Alto Networks' Expedition versions prior to 1.2.92	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*	-
Palo Alto Expedition Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter, T1078 : Valid Accounts, T1068 : Exploitation for Privilege Escalation	<a href="https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340">https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-9464</a>		Palo Alto Networks' Expedition versions prior to 1.2.96	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*	-
Palo Alto Expedition OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	<a href="https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340">https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES	
 <p><u><a href="#">Emennet Pasargad</a></u> (aka <u><a href="#">Holy Souls</a></u>, <u><a href="#">Vice Leaker</a></u>, <u><a href="#">Haywire Kitten</a></u>, <u><a href="#">Neptunium</a></u>, <u><a href="#">Cotton Sandstorm</a></u>, <u><a href="#">DEV-0198</a></u>, <u><a href="#">Yellow Dev 19</a></u>, <u><a href="#">Magic Kitten</a></u>, <u><a href="#">Black Magic</a></u>, <u><a href="#">ViceLeaker</a></u>, <u><a href="#">kalin3t</a></u>, <u><a href="#">Eeleyanet Gostar</a></u>, <u><a href="#">EeleyanetGostar</a></u>, <u><a href="#">Net Peygard</a></u>, <u><a href="#">Samavat</a></u>, <u><a href="#">Hackers of Savior</a></u>, <u><a href="#">Deus</a></u>, <u><a href="#">Group 42</a></u>, <u><a href="#">Voyeur</a></u>, <u><a href="#">MARNANBRIDGE</a></u>)</p>	Iran	Government, Energy, Financial, High Tech, NGOs, Civil Society, Shipping, Transportation, Political, Military, Airline, Manufacturing, Media, Travel, Hotels, Airlines, Oil, Petrochemical, Telecommunications	Israel, Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, Germany, United Kingdom, France, Italy, Spain, Poland, Romania, Netherlands, Belgium, Czech Republic, Sweden, Portugal, Greece, Hungary, Austria, Belarus, Switzerland, Bulgaria, Serbia, Denmark, Finland, Norway, Slovakia, Ireland, Croatia, Bosnia and Herzegovina, Moldova, Lithuania, Albania, Slovenia, Latvia, North Macedonia, Estonia, Luxembourg, Montenegro, Malta, Iceland, Andorra, Liechtenstein, Monaco, San Marino, Holy See, United States, Isle of Man, Faeroe Islands	
	<b>MOTIVE</b>			
	Hackivism, Espionage, Financial Gains			
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>	
	-	-	-	

## TTPs

TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, TA0006: Credential Access, TA0011: Command and Control, T1596: Search Open Technical Databases, T1589: Gather Victim Identity Information, T1589.002: Email Addresses, T1589.003: Employee Names, T1591.001: Determine Physical Locations, T1595.002: Vulnerability Scanning, T1590.001: Domain Properties, T1595.001: Scanning IP Blocks, T1650: Acquire Access, T1583: Acquire Infrastructure, T1587: Develop Capabilities, T1190: Exploit Public-Facing Application, T1110.001: Password Guessing, T1110.002: Password Cracking, T1071.001: Web Protocols, T1219: Remote Access Software

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **Emennet Pasargad** and malware **BeaverTail, InvisibleFerret, Rhadamanthys, Chisel,** and **PivotBox**.

## 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 **five exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Emennet Pasargad** and malware **BeaverTail, InvisibleFerret, Rhadamanthys, Chisel** in Breach and Attack Simulation(BAS).



# Threat Advisories

[Threat Actors Weaponized SharePoint Flaw To Infiltrate Corporate Networks](#)

[Hack, Leak, Repeat – Emennet Pasargad’s Quest to Destabilize Israel](#)

[CopyRh\(ight\)adamantys: Unmasking a Phishing Campaign with theLatest Rhadamanthys Stealer](#)

[North Korean Hackers Go After Remote Job Openings](#)

[Hackers Exploiting Critical Palo Alto Networks Vulnerability](#)

[CRON#TRAP: Leveraging Emulated Environments for Covert Cyber Operations](#)

# 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>BeaverTail</u>	SHA256	d801ad1beeab3500c65434da51326d7648a3c54923d794b2411b7b6a2960f31e, d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6, c0110cb21ae0e7fb5dec83ca90db9e250b47a394662810f230eb621b0728aa97, 9e3a9dbf10793a27361b3cef4d2c87dbd3662646f4470e5242074df4cb96c6b4, 91f96f2ddfa293806ec3effb8e05bc6941660237de90215b23281d706a2bc706, 24b89c77eaeebd4b02c8e8ab6ad3bd7abaa18893ecd469a6a04eda5e374dd305, 0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132, 0d8119f01d727beacbe6fe877541b3c11b084ffdc53c8bae436aca3dbc197076, 0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd
<u>InvisibleFerret</u>	SHA256	5bdd872a2a49b5682b297350222eee847c0a1e52125688acb9aa8a7b9ec4de29
	SHA1	9c1fddc45a6ad5a5b738e1ead5efd46051fdfd35
	MD5	2f7e6d05caab11bac4d585108a14d3c2

Attack Name	TYPE	VALUE
<u>Rhadamanthys</u>	SHA256	cf9d93951e558ed22815b34446cfa2bd2cf3d1582d8bd97912612f4d4 128a64e, 48aaa2dec95537cdf9fc471dbcb4ff726be4a0647dbdf6300fa61858c 2b0099, 00fc4b8a4c65c06766608f3ef3f92385c8e147f5991dabe290e33dd14b 39ad44, 0ad65fd0897a6547f6febf398708ab2d423a8f8834b53136219cb490e c3ebd13, 11ba24d023b544e28c37b6cb8afe27d06638175d7f56c2e4d4ff97bf7 bd813b6, 1a2399ecc38f3288206c75b55762d125d3d75254062a2c0d85c86e7f8 96736ac, 258ffcc13dbe110bcce21b91f7f075995719791fdd3c9f55ea5934984fa 4373d, 2cbc1e8a4cb5d18a867666adb3417bc88d48a74ae6500593959aec1 a1c92d2d, 342a5c7df2bdd040570f4b83c74366d4c96a90d6418149d432cb5e85 77f2f6b1, 3648e89e7449ea433a8b3ef0e5b605b5dc4157048c03b20dedc5e3b9 20fa8552, 5418e42706bca4712ff2a3db67853eb42a2310660c51cff2f9020586cf fedeb3, 69573694d16b7ccadfa208ff976bfe1b3e36837aba3e5dc4dfc80e6634 1ef61e, 6de4f65b1d738d84f8e825613092bbd360194195fe8a1c986e12a9bb 704217c1, 751f149665f87dd20cc8dff743f28e5da1ff2a5f04874d4b8569b9afcee edfec, 78200cd816acbd39b6664c6582e06500f6d46085b62b49d2f914bea5 a004197a, 783c7f4bf23072343f6247ee14e54e4af0b147553ad1ef42b4e7fb4438 6d667c, 7f99e506c17676b98dcc08e6a19f100ef933cde3e0423c6d4072f6802 a9196bb, 8d0b1174cbda6b102bb98c91ba123e9f404b9fad23b49a4e29f3cfd8d 20a577a, 90c7688e0dc23ba4530bac1d567bad920c4ef1c06cbf4b2d867eeb363 271eefe, 9102e564c3262b2c291e8ca3d67f8a55c06650aa86f617c919916f605 3c03c9b, 9327aa03760431b6d86eeb2f1a3efc36aa443b842b5116fbbe0f2a779 4c4e70e, 97286b6f3a6535ff1172ef65172e6967e3670c6b14a3313c3bf0d6c17 1b1fc85, 98e28d3423f5d414effe3c0ed6fd0f1c8154942e5e127ecee5f051e119 6ffc75, 99c0bebd8cb7b0948000a601f510fc70487f9da532be199b8641512a 2db9839, 9bdf49b27fd4d80ef087f63e0bfa0a0822686814863eca09ac506404a d76dfda,

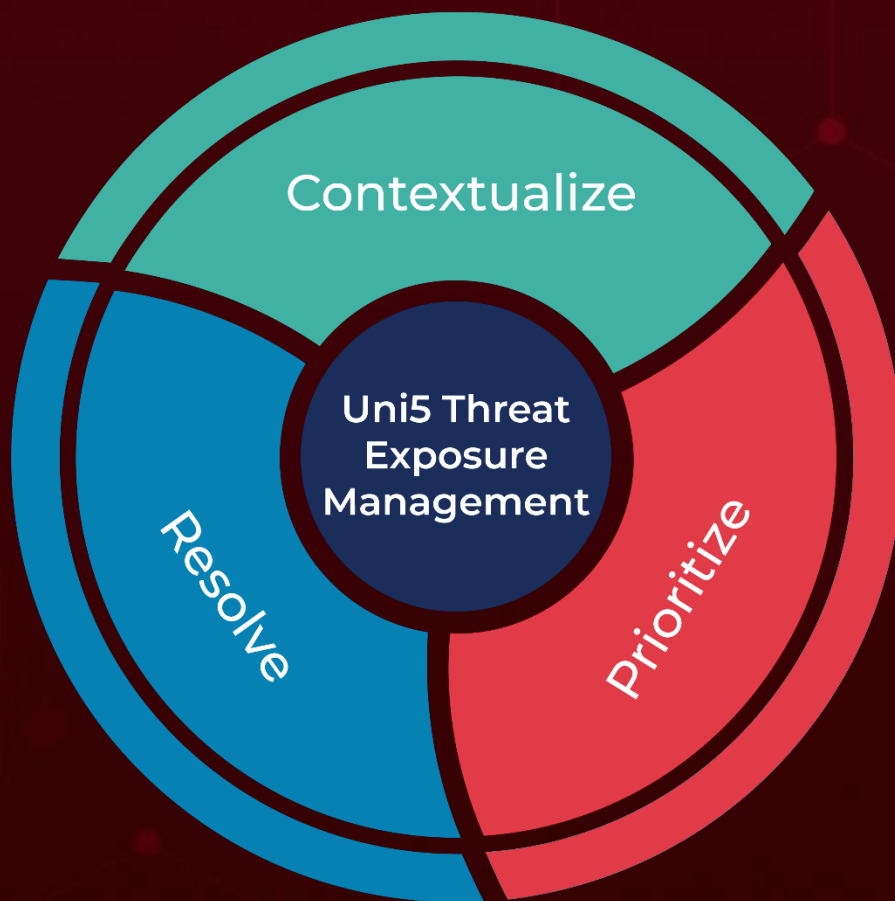
Attack Name	TYPE	VALUE
<u>Rhadamanthys</u>	SHA256	b2588061ba5ee9948bbccd320b40c6d7b8d6a693d181f3bce61e5e267f53aa7e, b936853a0c50a0cd0bc8b33103b55bd88e19c6c28768d990b954c11d714286ca, f2429f4bd09897653d0ffa41206a14cafa55356d5edc04dc0915c116867f8c27
<u>PivotBox</u>	SHA256	5A8BC06587CE40B3A8D8DD4037D0EF272EFC64A69E21F6689FFE3F5FBB04A468 4C91070877C6D116F5A27EFADDBBFBC339455628E9D6585A4EA5F9B6972BF92B
<u>Chisel</u>	SHA256	3E6A47DA0A226A4C98FB53A06EC1894B4BFD15E73D0CEA856B7D2A001CADA7E9

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

**November 11, 2024 • 05:30 AM**

© 2024 All Rights are Reserved by Hive Pro



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