

Date of Publication  
December 23, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

16 to 22 DECEMBER 2024

# Table Of Contents

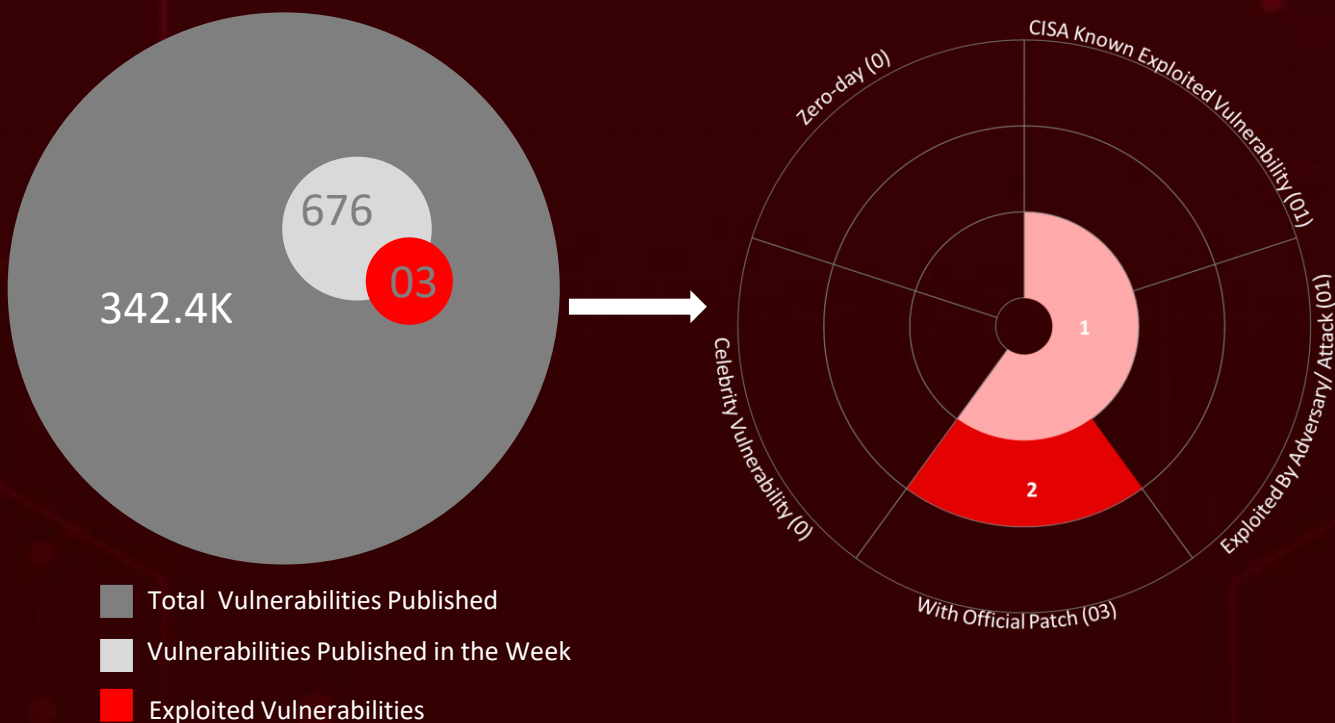
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	12
<u>Recommendations</u>	14
<u>Threat Advisories</u>	15
<u>Appendix</u>	16
<u>What Next?</u>	17

# Summary

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

Thai government officials are under siege by advanced cyberattacks utilizing DLL side-loading techniques to deploy **Yokai** malware. Concurrently, the threat actor **TA397** is focusing its efforts on organizations in the Turkish defense sector. This operation employs **WmRAT** and **MiyaRAT** in its attack chain, primarily for espionage purposes.

Adding to the urgency, Apache has disclosed a critical flaw (**CVE-2024-53677**) in its Apache Struts. This flaw allows remote attackers to execute arbitrary code, posing significant risks of critical data loss and full system compromise. 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

4

Attacks  
Executed

- [VIPKeyLogger](#)
- [Yokai](#)
- [WmRAT](#)
- [MiyaRAT](#)

3

Vulnerabilities  
Exploited

- [CVE-2017-11882](#)
- [CVE-2024-53677](#)
- [CVE-2023-34990](#)

2

Adversaries in  
Action

- [TA397](#)
- [Earth Koshchei](#)

# Insights

**VIPKeyLogger**  
Malware Poses  
New Risks to  
**Microsoft 365**  
Users

Full System Compromise Looms with  
**Apache Struts** Flaw **CVE-2024-53677**

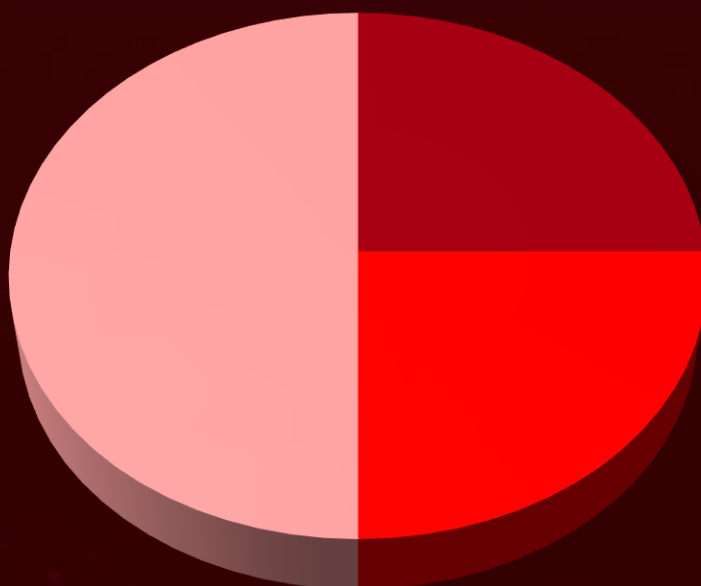
Decoy Docs to Data  
Theft Thai Officials  
Hit by **Yokai**  
**Malware**

**20,000** Users Targeted in  
**Microsoft Azure** Credential  
Harvesting Campaign

**TA397** Espionage Tactics  
Threaten **Turkish Defense**  
Organizations

**Over 200**  
Fraudulent  
Domains Fuel **Earth**  
**Koshchei's** RDP  
Attacks

### Threat Distribution



■ Infostealer    ■ Backdoor    ■ RAT

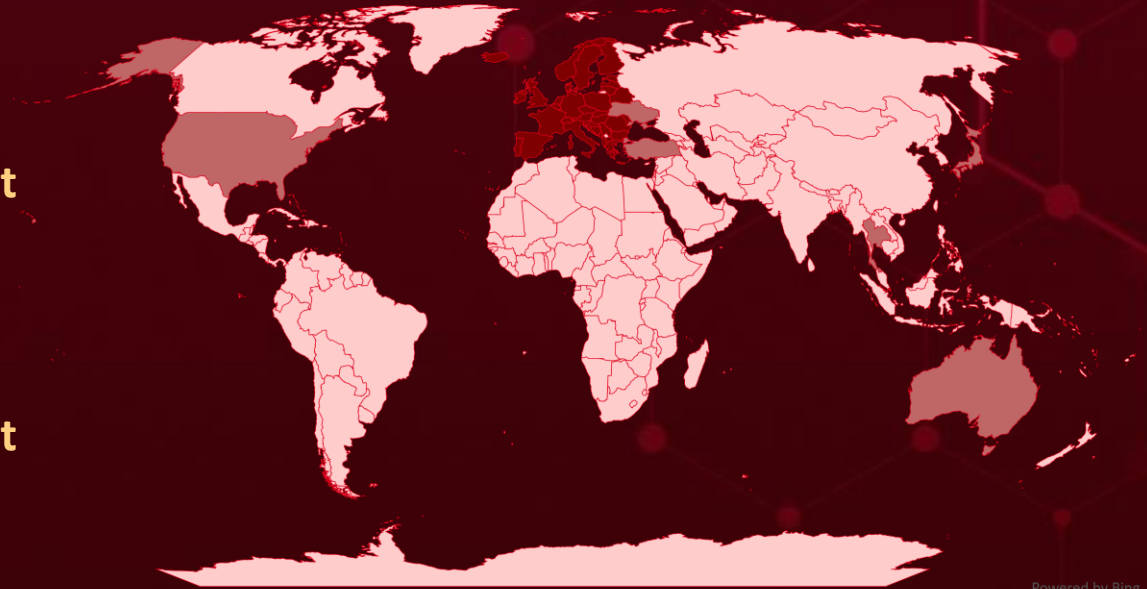


# Targeted Countries

Most



Least

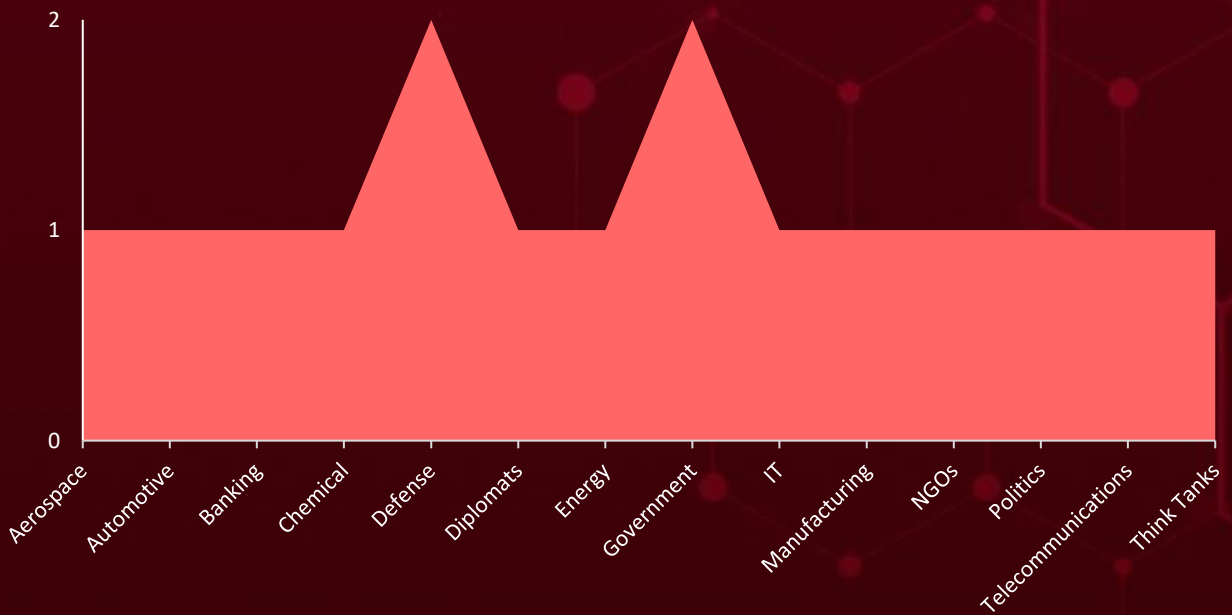


Powered by Bing

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

Countries	Countries	Countries	Countries
Poland	France	Egypt	Nepal
Luxembourg	Norway	Paraguay	Ghana
Sweden	Germany	El Salvador	Niger
Albania	Portugal	China	Angola
Montenegro	Greece	Equatorial Guinea	Cameroon
Andorra	San Marino	Suriname	Grenada
Serbia	Holy See	Eritrea	Panama
Austria	Slovakia	Dominica	Guatemala
Liechtenstein	Hungary	Bahamas	Philippines
Belarus	Spain	New Zealand	Guinea
Moldova	Iceland	Eswatini	Chad
Belgium	Switzerland	Pakistan	Guinea-Bissau
North Macedonia	Ireland	Ethiopia	Saint Lucia
Bosnia and Herzegovina	Italy	Central African Republic	Guyana
Romania	Latvia	Fiji	Saudi Arabia
Bulgaria	Thailand	Chile	Haiti
Slovenia	Ukraine	Bahrain	Sierra Leone
Croatia	Turkey	Colombia	Antigua and Barbuda
United Kingdom	Japan	Bangladesh	Solomon Islands
Czech Republic	Australia	Sri Lanka	Honduras
Lithuania	United States	Gabon	South Sudan
Denmark	Togo	Tajikistan	Belize
Malta	Rwanda	Gambia	State of Palestine
Estonia	North Korea	Djibouti	Benin
Monaco	DR Congo	Georgia	Côte d'Ivoire
Finland	South Africa	Mozambique	India
Netherlands	Ecuador	Barbados	Azerbaijan
	Namibia		

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1204

User Execution

### T1566

Phishing

### T1041

Exfiltration Over C2 Channel

### T1566.001

Spearphishing Attachment

### T1564

Hide Artifacts

### T1204.002

Malicious File

### T1027

Obfuscated Files or Information

### T1036

Masquerading

### T1588

Obtain Capabilities

### T1588.006

Vulnerabilities

### T1217

Browser Bookmark Discovery

### T1113

Screen Capture

### T1574

Hijack Execution Flow

### T1056.001

Keylogging

### T1056

Input Capture

### T1068

Exploitation for Privilege Escalation

### T1053

Scheduled Task/Job

### T1078

Valid Accounts

### T1090

Proxy

# ✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>VIPKeyLogger</u>	VIPKeyLogger is a newly identified infostealer malware resembling the notorious Snake Keylogger. This malware captures keystrokes, login credentials, and other sensitive system data. To avoid detection by conventional security software, VIPKeyLogger uses advanced obfuscation methods.	Phishing emails	CVE-2017-11882
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCT</b>
Infostealer			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Information Theft, Remote Control, System Compromise	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	b7d62d77cace855288bf6b463f8ad783316594f90dad78d97a7ea85be58b8bc3, d854f347061d9d7b8a9788ab8633c3f07619e29bd440924507a0147484c217c3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Yokai</u>	Yokai Backdoor, delivered via a RAR archive containing two Windows shortcut files. Yokai establishes persistence on the compromised system, enabling ongoing communication with a command-and-control (C2) server. In addition to executing commands, the backdoor gathers key system information, such as the hostname and username.	Unknown	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCT</b>
Backdoor			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		System Compromise, Data Exfiltration	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	eaae6d5dbf40239fb5abfa2918286f4039a3a0fcd28276a41281957f6d850456, 3e5cfe768817da9a78b63efad9e60d2d300727a97476edf87be088fb26f06500		

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
<a href="#"><u>WmRAT</u></a>	WmRAT is a remote access trojan (RAT) developed in C++ that utilizes sockets for communication and offers typical RAT capabilities. It can collect basic host information, upload and download files, capture screenshots, retrieve geolocation data of the target machine, enumerate directories and files, and execute arbitrary commands using cmd or PowerShell.	Spear-phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>  Remote System Control, Geolocation Tracking, Corporate Espionage	<b>AFFECTED PRODUCT</b>
RAT			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
TA397			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	10cec5a84943f9b0c635640fad93fd2a2469cc46aae5e43a4604c903d139970f		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#"><u>MiyaRAT</u></a>	MiyaRAT, written in C++, shares similar functionality with WmRAT. Upon execution, the malware decrypts its hardcoded command-and-control (C2) server and then collects basic system information, which is sent during its initial communication with the C2.	Spear-phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>  Remote Control Access, Data Exfiltration	<b>AFFECTED PRODUCT</b>
RAT			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
TA397			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	c7ab300df27ad41f8d9e52e2d732f95479f4212a3c3d62dbf0511b37b3e81317		

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="#">CVE-2017-11882</a>		Microsoft Office	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV		
Microsoft Office Memory Corruption Vulnerability		cpe:2.3:a:microsoft:office:- :*:*:*:*:*:*	VIPKeyLogger
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1005: Data from Local System; T1574: Hijack Execution Flow	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-53677</a>		Struts Version 2.0.0 - Struts 2.3.37 (EOL), Struts Version 2.5.0 - Struts 2.5.33, Struts Version 6.0.0 - Struts 6.3.0.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV		
Apache Struts Remote Code Execution Vulnerability		cpe:2.3:a:apache:struts:*:*:* :*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<a href="https://struts.apache.org/download.cgi">https://struts.apache.org/download.cgi</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-34990</u>		FortiWLM 8.5: Versions 8.5.0 through 8.5.4 FortiWLM 8.6: Versions 8.6.0 through 8.6.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiwlm:*:*:*:*:*:*	-
Fortinet FortiWLM Relative Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	<a href="https://www.fortiguard.com/psirt/FG-IR-23-144">https://www.fortiguard.com/psirt/FG-IR-23-144</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>TA397 (aka Bitter APT, T-APT-17, APT-C-08, Orange Yali)</u>	-	Defense	Turkey
	<b>MOTIVE</b> Information theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCTS</b>
	-	WmRAT and MiyaRAT	Windows
<b>TTPs</b>			
TA0005: Defense Evasion; TA0010: Exfiltration; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0003: Persistence; TA0009: Collection; TA0011: Command and Control; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1041: Exfiltration Over C2 Channel; T1027: Obfuscated Files or Information; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1053.005: Scheduled Task; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1564: Hide Artifacts; T1614: System Location Discovery; T1113: Screen Capture; T1204.002: Malicious File; T1217: Browser Information Discovery; T1056.001: Keylogging; T1056: Input Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u><a href="#">Earth Koshchei (aka APT29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, Midnight Blizzard, UNC3524, Cranefly, TEMP.Monkeys, Cloaked Ursa, Blue Dev 5, NobleBaron, Solar Phoenix)</a></u></p>	Russia	Diplomats, Energy, Telecommunications, IT, Government, Think Tanks, NGOs, Politics, Aerospace, Defense, Banking	Europe, US, Japan, Ukraine, and Australia
	<b>MOTIVE</b>		
	Information theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>	<b>AFFECTED PRODUCTS</b>
	-	-	-

### TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1204: User Execution; T1552.001: Credentials In Files; T1566.001: Spearphishing Attachment; T1078.003: Local Accounts; T1078: Valid Accounts; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1090: Proxy; T1552: Unsecured Credentials; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1560: Archive Collected Data; T1560.003: Archive via Custom Method; T1005: Data from Local System; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1046: Network Service Discovery; T1570: Lateral Tool Transfer; T1563.002: RDP Hijacking; T1563: Remote Service Session Hijacking; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1036: Masquerading

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **TA397, Earth Koshchei**, and malware **VIPKeyLogger, Yokai, WmRAT, MiyaRAT**.

## 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 **three exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **TA397, Earth Koshchei**, and malware **VIPKeyLogger, Yokai, WmRAT, MiyaRAT, HustleCon** in Breach and Attack Simulation(BAS).

# Threat Advisories

[VIPKeyLogger: A New Infostealer in Phishing Attacks](#)

[Apache Struts Flaw Exploited for Remote Code Execution in Active Attacks](#)

[Yokai A New Backdoor Stalks Thai Officials](#)

[December 2024 Linux Patch Roundup](#)

[European Firms Hit by Sophisticated Cloud Phishing Campaign](#)

[Uncovering TA397's Targeted Malware Campaign Against Turkish Defense](#)

[Critical Fortinet FortiWLM Vulnerability Exposes Admin Controls to Attackers](#)

[Earth Koshchei's Large-Scale Spear-Phishing Campaign Exposed](#)

# 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>VIPKeyLogger</u>	SHA256	b7d62d77cace855288bf6b463f8ad783316594f90dad78d97a7ea85be58b8bc3, d854f347061d9d7b8a9788ab8633c3f07619e29bd440924507a0147484c217c3
<u>Yokai</u>	SHA256	eaae6d5dbf40239fb5abfa2918286f4039a3a0fcd28276a41281957f6d850456, 3e5cfe768817da9a78b63efad9e60d2d300727a97476edf87be088fb26f06500, 1626ce79f2b96c126cbdb00195dd8509353e8754b1a0ce88d359fa890acd6676, 2852223eb40cf0dae4111be28ce37ce9af23e5332fb78b47c8f5568d497d2611
<u>WmRAT</u>	SHA256	10cec5a84943f9b0c635640fad93fd2a2469cc46aae5e43a4604c903d139970f
<u>MiyaRAT</u>	SHA256	c7ab300df27ad41f8d9e52e2d732f95479f4212a3c3d62dbf0511b37b3e81317

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

**December 23, 2024 • 3:00 AM**

© 2024 All Rights are Reserved by Hive Pro



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