

Date of Publication  
August 19, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

12 to 18 August 2024

# Table Of Contents

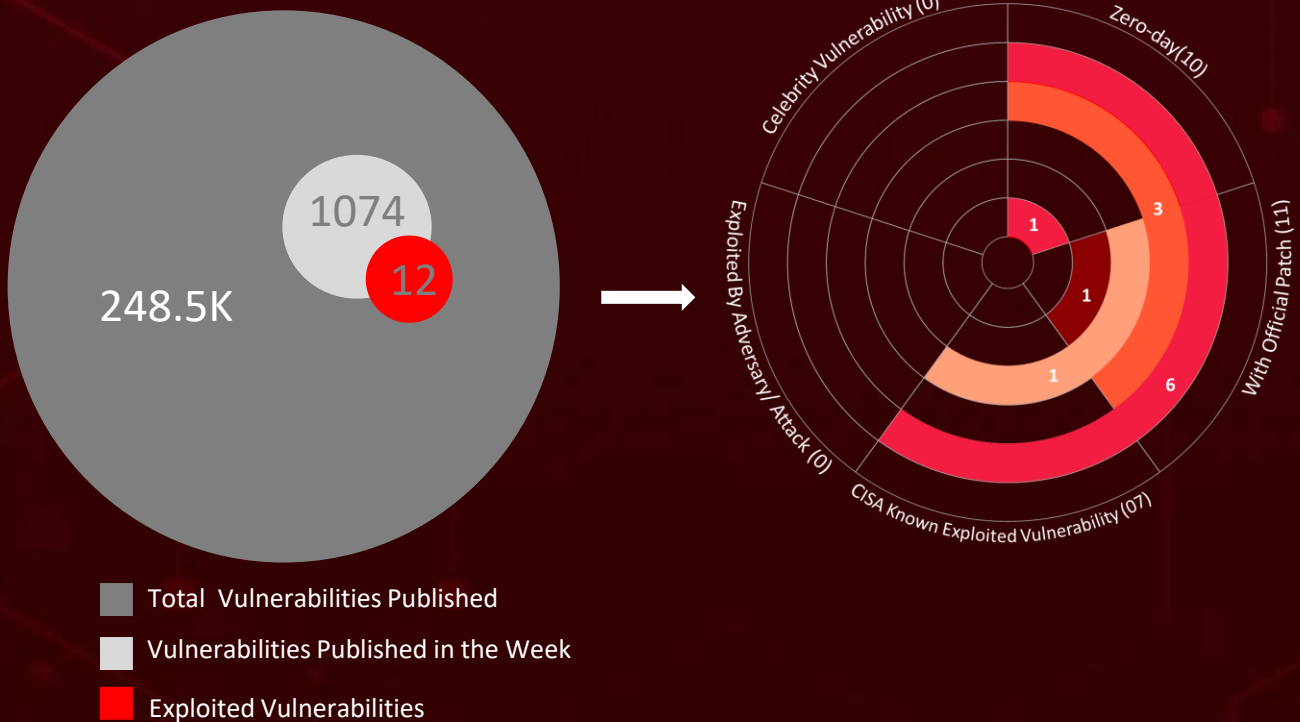
<a href="#"><u>Summary</u></a>	03
<a href="#"><u>High Level Statistics</u></a>	04
<a href="#"><u>Insights</u></a>	05
<a href="#"><u>Targeted Countries</u></a>	06
<a href="#"><u>Targeted Industries</u></a>	07
<a href="#"><u>Top MITRE ATT&amp;CK TTPs</u></a>	07
<a href="#"><u>Attacks Executed</u></a>	08
<a href="#"><u>Vulnerabilities Exploited</u></a>	12
<a href="#"><u>Adversaries in Action</u></a>	18
<a href="#"><u>Recommendations</u></a>	20
<a href="#"><u>Threat Advisories</u></a>	21
<a href="#"><u>Appendix</u></a>	22
<a href="#"><u>What Next?</u></a>	24

# Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week alone, HiveForce Labs has detected **eight** attacks, reported **twelve** vulnerabilities, and identified **two** active adversaries. These findings highlight the relentless and escalating danger of cyber intrusions.

Additionally, Ivanti's Virtual Traffic Manager (vTM) appliances have a critical authentication bypass vulnerability (**CVE-2024-7593**). This flaw allows attackers to create unauthorized admin accounts, risking system control. While, Microsoft's August 2024 Patch Tuesday addressed 89 vulnerabilities, **six** of which were actively exploited in wild.

Furthermore, **Earth Baku**, an APT group, has expanded its attacks from the Indo-Pacific to Europe, the Middle East, and Africa, using new tools against public-facing applications. These rising threats pose significant and immediate danger to users worldwide.



# High Level Statistics

8

Attacks  
Executed

12

Vulnerabilities  
Exploited

2

Adversaries in  
Action

- [StealthVector](#)
- [StealthReacher](#)
- [SneakCross](#)
- [GrewApache](#)
- [PlugY](#)
- [CloudSorcerer](#)
- [ABCloader](#)
- [ABCsync](#)

- [CVE-2024-7593](#)
- [CVE-2024-28986](#)
- [CVE-2024-38106](#)
- [CVE-2024-38107](#)
- [CVE-2024-38178](#)
- [CVE-2024-38189](#)
- [CVE-2024-38193](#)
- [CVE-2024-38213](#)
- [CVE-2024-21302](#)
- [CVE-2024-38202](#)
- [CVE-2024-38199](#)
- [CVE-2024-38200](#)

- [Earth Baku](#)
- [Actor240524](#)



# Insights

## OpenVPN

flaws chained together to achieve remote code execution (RCE) and local privilege escalation (LPE).

## SolarWinds Web Help Desk

critical deserialization flaw allows remote code execution.

## Earth Baku

, an advanced persistent threat (APT) actor, has expanded its operations to Europe, the Middle East, and Africa, using new tools to attack public-facing applications.

## Microsoft Patch Tuesday

Addresses 89 vulnerabilities, including 10 zero-days, out of which 6 actively exploited.

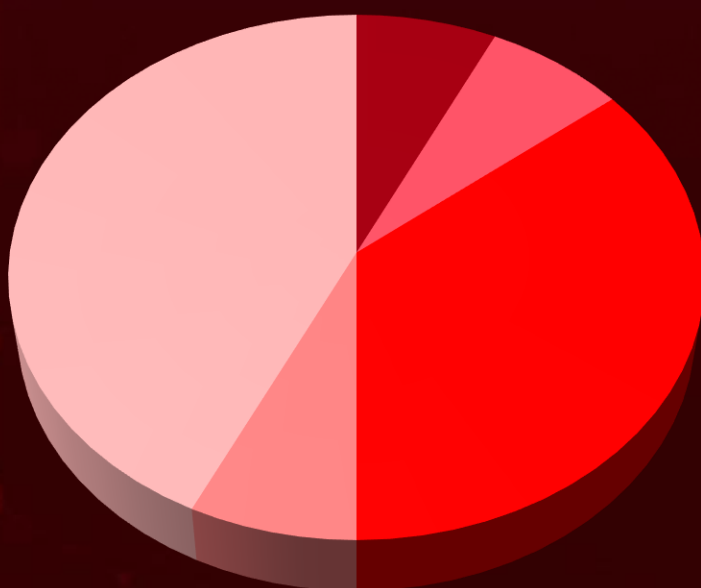
## EastWind Campaign

Sophisticated cyberattack targets Russian government, IT sectors. Chinese-speaking APTs' uses Dropbox, GitHub for covert operations.

## Widespread malware campaign

targeting web browser extensions, affected over 300,000 users globally.

## Threat Distribution



■ Backdoor ■ Trojan ■ Ransomware ■ Downloader ■ Stealer

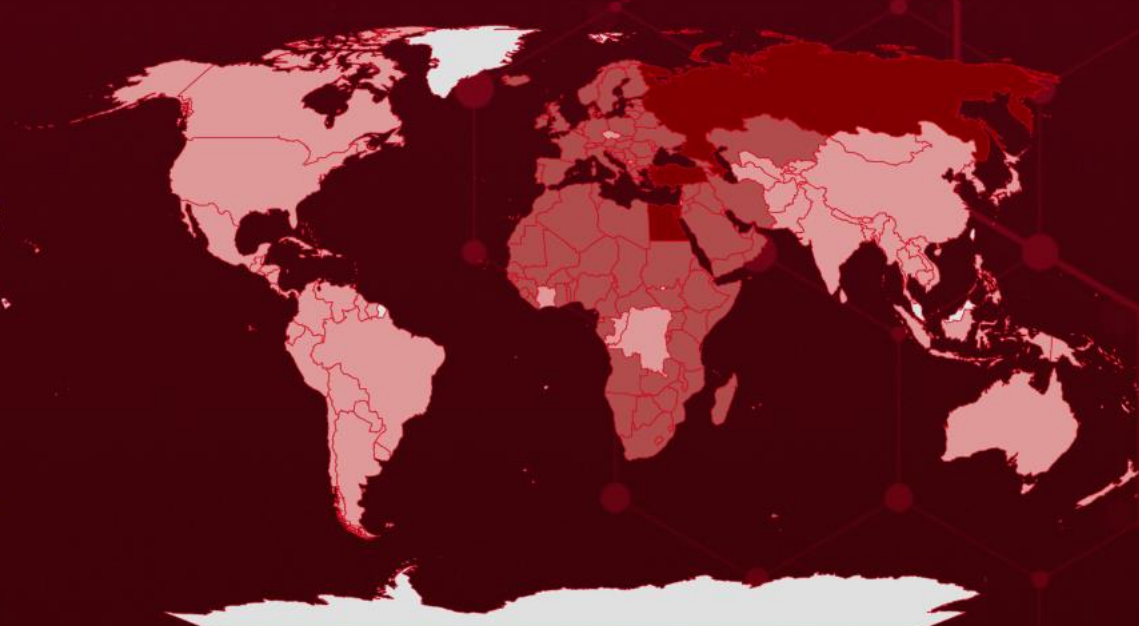


# Targeted Countries

Most



Least

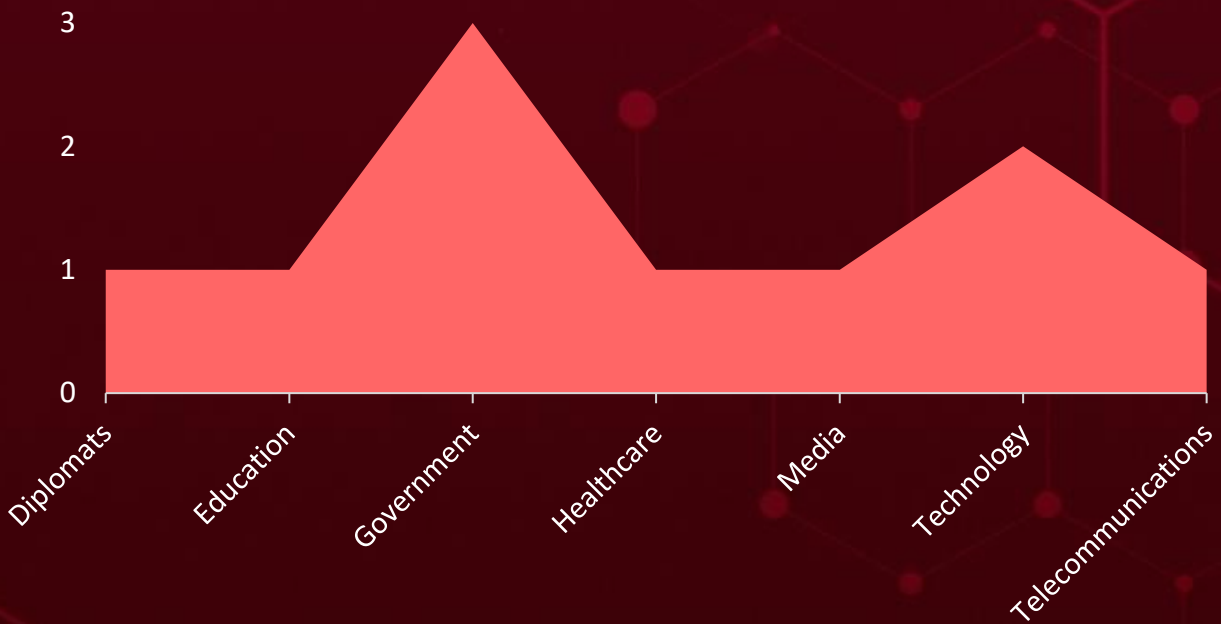


Powered by Bing

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

Countries	Countries	Countries	Countries
Egypt	Cabo Verde	Burundi	Romania
Russia	Libya	Switzerland	Iceland
Israel	Cameroon	Eswatini	Rwanda
Azerbaijan	Madagascar	Liechtenstein	Iran
Cyprus	Central African Republic	Ethiopia	Saudi Arabia
Turkey	Mauritania	Luxembourg	Iraq
Mozambique	Chad	Finland	Serbia
Austria	Montenegro	Malawi	Ireland
Senegal	Comoros	France	Sierra Leone
Albania	Netherlands	Malta	Angola
Mali	Croatia	Gabon	Slovenia
Belarus	Norway	Mauritius	Italy
Poland	Algeria	Gambia	South Africa
Belgium	Qatar	Monaco	Jordan
South Sudan	Denmark	Georgia	Spain
Benin	San Marino	Morocco	Kazakhstan
Lithuania	Djibouti	Germany	Sweden
Bosnia and Herzegovina	Seychelles	Namibia	United Kingdom
Moldova	Andorra	Ghana	Syria
Botswana	Somalia	Niger	Uganda
Nigeria	Equatorial Guinea	Greece	Togo
Bulgaria	Sudan	North Macedonia	United Arab Emirates
Armenia	Eritrea	Guinea	Yemen
Burkina Faso	Tanzania	Oman	Kenya
Slovakia	Estonia	Guinea-Bissau	Ukraine
	Zimbabwe	Portugal	Kuwait
		Hungary	

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1190

Exploit Public-Facing Application

### T1027

Obfuscated Files or Information

### T1566

Phishing

### T1068

Exploitation for Privilege Escalation

### T1204

User Execution

### T1055

Process Injection

### T1204.002

Malicious File

### T1588.006

Vulnerabilities

### T1588.005

Exploits

### T1041

Exfiltration Over C2 Channel

### T1133

External Remote Services

### T1547

Boot or Logon Autostart Execution

### T1588

Obtain Capabilities

### T1083

File and Directory Discovery

### T1036

Masquerading

### T1082

System Information Discovery

### T1057

Process Discovery

### T1498

Network Denial of Service

### T1587.001

Malware

# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>StealthVector</u></a>	StealthVector is a malicious software designed to download and execute harmful code (shellcode) on infected computers. It's written in C/C++, making it efficient and hard to detect. This malware is often used by Earth Baku to gain control over compromised systems.	-	-
		IMPACT	AFFECTED PRODUCTS
		Deploy Malware	-
			PATCH LINK
			-
TYPE			
Loader			
ASSOCIATED ACTOR			
Earth Baku			

IOC TYPE	VALUE
SHA256	7e63c6b9ab3b32beffbc1eb23d6ca7cc59616b0722f0dd4f0d893c0a1724f5d7, 8405d742405d3a6d3bda6bc49630dd5f3604a3d6ae27cbd533e425f8abbaafdc, a50f85c71b69563ba42bf04c937e1063244ca4957231d3adac76f1c96ab42d3c, ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf, ec10a9396dca694fe64366e0dab82d046cf92457f97efd50a68ceb85adef6b74

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>StealthReacher</u></a>	StealthReacher is a sophisticated loader developed by the cyberespionage group Earth Baku. As an integral part of their toolkit, it serves as a crucial component in their attack chain. This malicious software is designed to download and execute additional payloads onto compromised systems, allowing Earth Baku to establish persistent control and conduct their espionage operations.	-	-
		IMPACT	AFFECTED PRODUCTS
		Deploy Malware	-
			PATCH LINK
			-
TYPE			
Loader			
ASSOCIATED ACTOR			
Earth Baku			

IOC TYPE	VALUE
SHA1	7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a, 22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86, c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db, 073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75

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>SneakCross</u></a>	SneakCross is a malicious backdoor developed by the cyberespionage group Earth Baku. As part of their toolkit, it provides a covert channel for attackers to maintain persistent access to compromised systems. Once installed, SneakCross allows remote control, data exfiltration, and potentially further malicious activities.	-	-
<b>TYPE</b>		Remote control, data exfiltration	<b>AFFECTED PRODUCTS</b>
Modular Backdoor			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Baku		-	
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	c02acc26a389397fb172f83258baa8a974986ffd706ba708a3b0a679f61be56		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>GrewApacha</u></a>	GrewApacha is a remote access trojan (RAT) that has been linked to the Chinese state-sponsored hacking group APT31. It was first identified in 2021 and has been used in multiple campaigns targeting government and private sector organizations.	Phishing	-
<b>TYPE</b>		Data theft, Financial loss	<b>AFFECTED PRODUCTS</b>
RAT			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		-	
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	e2f87428a855ebc0cda614c6b97e5e0d65d9ddcd3708fd869c073943ecdde1c0		

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>PlugY</u></a>	PlugY is a recently discovered backdoor malware that has been linked to the Chinese hacking group APT27. It offers a wide range of capabilities, including executing commands, capturing screenshots, keylogging, and clipboard monitoring. Uses TCP, UDP, or named pipes to communicate with command-and-control servers.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Data Theft	-
<b>IOC TYPE</b>	<b>VALUE</b>		
MD5	Faf1f7a32e3f7b08017a9150dccb511d, 67cfecf2d777f3a3ff1a09752f06a7f5		
SHA256	141efc5eb38437b876fd1c82231fe80b836290b5fbe48a5dd57a85e2ce25e12b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>CloudSorcerer</u></a>	CloudSorcerer is a backdoor targeting Russian government entities. It uses legitimate cloud platforms for covert operations. By exfiltrating sensitive data and maintaining persistent access, it poses a significant threat. Its dynamic behavior and complex communication methods make detection challenging.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Data Theft and Persistent	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	5071022aaa19d243c9d659e78ff149fe0398cf7d9319fd33f718d8e46658e41c		
SHA1	e1cf6334610e0afc01e5de689e33190d0c17ccd4		
MD5	bed245d61b4928f6d6533900484cafc5		




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>ABCloader</u></a>	ABCloader is a component of the malware arsenal used by the APT group Actor240524, which has targeted diplomats in Azerbaijan and Israel. Primarily functioning as a decryption and loading mechanism, it prepares the system for the subsequent deployment of the ABCsync malware. To evade detection, ABCloader incorporates anti-analysis techniques.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Trojan			
<b>ASSOCIATED ACTOR</b>			
Actor240524	Data Theft	<b>PATCH LINK</b>	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	a250740948aba579462397ac95ff10e6b0ee952c2af7d9d726cbfde9da1eaaff		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>ABCsync</u></a>	ABCsync is a malicious payload delivered by the ABCloader component of the Actor240524 APT group. Once installed, it can execute remote shells, modify user data, and steal sensitive files. This malware poses a significant threat to targeted individuals and organizations, potentially leading to data breaches, espionage, and operational disruption.	ABCloader	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Trojan			
<b>ASSOCIATED ACTOR</b>			
Actor240524	Data breaches, Espionage, and Operational disruption	<b>PATCH LINK</b>	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	6fa56ab1ce0d4fc9db6422bff8caa38bea1bdb9abbe4a48ecfb364eb20c7ac1a		




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-2024-7593</a>		Ivanti Virtual Traffic Manager Versions: 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:vtm:*:*:*:*:* *:*:*	-
Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability			
	CWE ID		
	CWE-287, CWE-303	T1068 : Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-28986</a>		SolarWinds Web Help Desk 12.8.3 and all previous versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:solarwinds:web_help_desk:*:*:*:*:*	-
SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability			
	CWE ID		
	CWE-502	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1">https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-38106</u></a>		Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Kernel Privilege Escalation Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-591	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-38107</u></a>		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-38178</u></a>		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Scripting Engine Memory Corruption Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1204.001: User Execution: Malicious Link, T1562.010: Impair Defenses: Downgrade Attack	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-38189</u></a>		Microsoft Office LTSC 2021, Microsoft Project, Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:office:*:*:*:*:*:*	
Microsoft Project Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:project:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1204.002: User Execution: Malicious File	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38193</a>		Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38213</a>		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204.002: User Execution: Malicious File, T1562 : Impair Defenses	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-21302</a>		Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Windows Secure Kernel Mode Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38202</a>		Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Windows Update Stack Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38199</a>		Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1021 : Remote Services	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38200</a>		Microsoft 365 Apps for Enterprise, Microsoft Office	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:office:*:*:*:*:*	
Microsoft Office Spoofing Vulnerability		cpe:2.3:a:microsoft:365_apps:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1036 : Masquerading, T1204 : User Execution	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>Earth Baku</b>	-	Government, Media and Communications, Telecommunications, Technology, Healthcare, and Education	Europe, the Middle East, Africa, Italy, Germany, United Arab Emirates, Qatar, Georgia, and Romania
	<b>MOTIVE</b>		
	Espionage and Information theft		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	StealthVector, StealthReacher (aka DodgeBox), SneakCross (aka MoonWalk)	-	
<b>TTPs</b>			
TA0001: Initial Access; TA0003: Persistence; TA0002: Execution; TA0010: Exfiltration; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; TA0040: Impact; T1055.012: Process Hollowing; TA0008: Lateral Movement; TA0007: Discovery; T1027: Obfuscated Files or Information; T1055: Process Injection; T1565: Data Manipulation; T1082: System Information Discovery; T1056.001: Keylogging; T1056: Input Capture; T1071: Application Layer Protocol; T1021.001: Remote Desktop Protocol; T1133: External Remote Services; T1021: Remote Services; T1071.004: DNS; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>Actor240524</b>	-	Government, Diplomats	Azerbaijan, Israel
	<b>MOTIVE</b>		
	Espionage and Information theft		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	ABCloader, ABCsync	-

**TTPs**

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1059.005: Visual Basic; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1574: Hijack Execution Flow; T1036: Masquerading; T1070: Indicator Removal; T1082: System Information Discovery; T1497: Virtualization/Sandbox Evasion; T1041: Exfiltration Over C2 Channel

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **twelve exploited vulnerabilities** and block the indicators related to the threat actors **Earth Baku, Actor240524** and malware **StealthVector, StealthReacher, SneakCross, GrewApache, PlugY, CloudSorcerer, ABCloader, ABCsync**.

## 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 **twelve exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Earth Baku, Actor240524** and malware **StealthVector, StealthReacher, SneakCross, GrewApache, PlugY, ABCloader, ABCsync** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Widespread Malware Campaign Targets Over 300,000 Users via Fake Downloads](#)

[Chained Exploits: OpenVPN Vulnerabilities Lead to RCE and LPE](#)

[Unmasking Earth Baku: New Tactics and Targets in Cyber Espionage](#)

[Hackers Exploit Ivanti vTM Flaw to Create Rogue Admin Accounts](#)

[EastWind Campaign: Chinese APTs' Master Plan Against Russian Entities](#)

[Actor240524 the New Face of Geopolitical Cyber Espionage](#)

[Critical Flaw in SolarWinds Web Help Desk Leads to Remote Code Execution](#)

[Microsoft's August Patch Tuesday Addresses Active Zero-Day Exploits](#)

# 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)

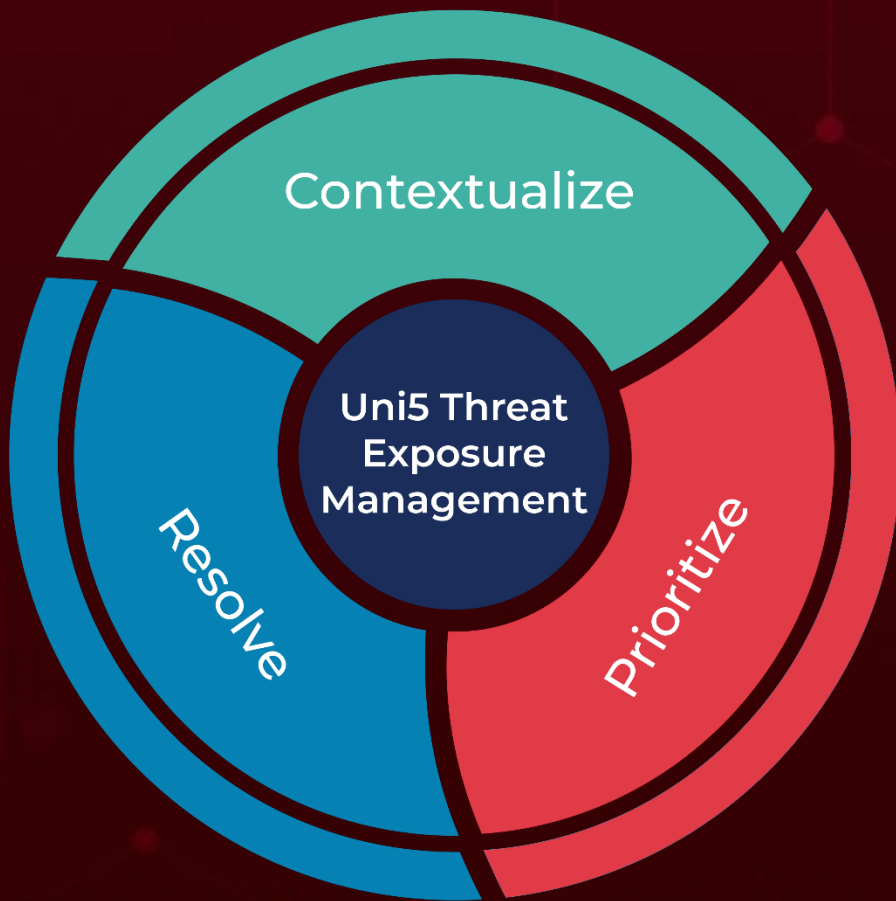
Attack Name	TYPE	VALUE
<a href="#"><u>StealthVector</u></a>	SHA256	7e63c6b9ab3b32beffbc1eb23d6ca7cc59616b0722f0dd4f0d893c0a1724f5d7, 8405d742405d3a6d3bda6bc49630dd5f3604a3d6ae27cbd533e425f8abbaafdc, a50f85c71b69563ba42bf04c937e1063244ca4957231d3adac76f1c96ab42d3c, ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf, ec10a9396dca694fe64366e0dab82d046cf92457f97efd50a68ceb85a def6b74, 73eaba82ef1c502448e533007e92b1afa879b09f85f28b71648668ea62839ff5, 0faddbe1713455e3fc9777ec45adf07b28e24f4c3ddca37586c2aa6b539898c0, 1c88150ec85a07c3db5f18c5eedcb0b653467b897af01d690ed996e5e07ba8e3, 3e52c310c6556367ff9e18448bc41719e603d1cbbdafdcba736c6565529617b6, 07aa971f0791b06dd442d4c7a49c1d3d27a1cbb16602f731e870b5ef50edf69e, 166b6dcdac31f4bf51e4b20a7c3f7d4f7017ca0c30fa123d5591e25c3fa66107, 21fc0f50d545c0a373380934dc61c423c8a31d8c3e6eae4f8a35149ad9962d88, 7463700ec5768d4af6549028465f978059611555aa8e22e2b7c664b1c dbfa9ae, cdcbd9c25e06ac6da5497fa19459d0007449ec1a3e6bc591334db6fb3598aecb, 7f24bc080281d250ec88493e5803e488721a17c9382cd54ba8dfbcb785f23a88

Attack Name	TYPE	VALUE
<u>StealthReacher</u>	SHA256	7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a, 22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86, c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5fb1a6db, 073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75
<u>SneakCross</u>	SHA256	e4360c0aa995e6e896b22bb7725a6c9b189be8606e7cbbc8b6e80c606358649d, 83de8917bf0ac1d670acf27431015215db872b7291979312dd65e30d99806abb, ec5a96f42aeccdf9a3ae4c3650689606c8539fd65c0b47f30887afecb901be43, e5f1360d4c299bb32e33e081115f2b520251a983af2ebc649b4b9b70308246fe
<u>GrewApache</u>	SHA256	e2f87428a855ebc0cda614c6b97e5e0d65d9ddcd3708fd869c073943ecdde1c0
<u>PlugY</u>	MD5	Faf1f7a32e3f7b08017a9150dccb511d, 67cfecf2d777f3a3ff1a09752f06a7f5
	SHA256	141efc5eb38437b876fd1c82231fe80b836290b5f5be48a5dd57a85e2ce25e12b
<u>CloudSorcerer</u>	SHA256	5071022aaa19d243c9d659e78ff149fe0398cf7d9319fd33f718d8e46658e41c
	SHA1	e1cf6334610e0afc01e5de689e33190d0c17ccd4
	MD5	bed245d61b4928f6d6533900484cafc5
<u>ABCloader</u>	SHA256	a250740948aba579462397ac95ff10e6b0ee952c2af7d9d726cbfde9da1eaaff
<u>ABCsync</u>	SHA256	6fa56ab1ce0d4fc9db6422bff8caa38bea1bdb9abbe4a48ecfb364eb20c7ac1a

# 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

**August 19, 2024 • 11:30 PM**

© 2024 All Rights are Reserved by Hive Pro



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