

Date of Publication  
February 12, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

5 to 11 FEBRUARY 2024

# Table Of Contents

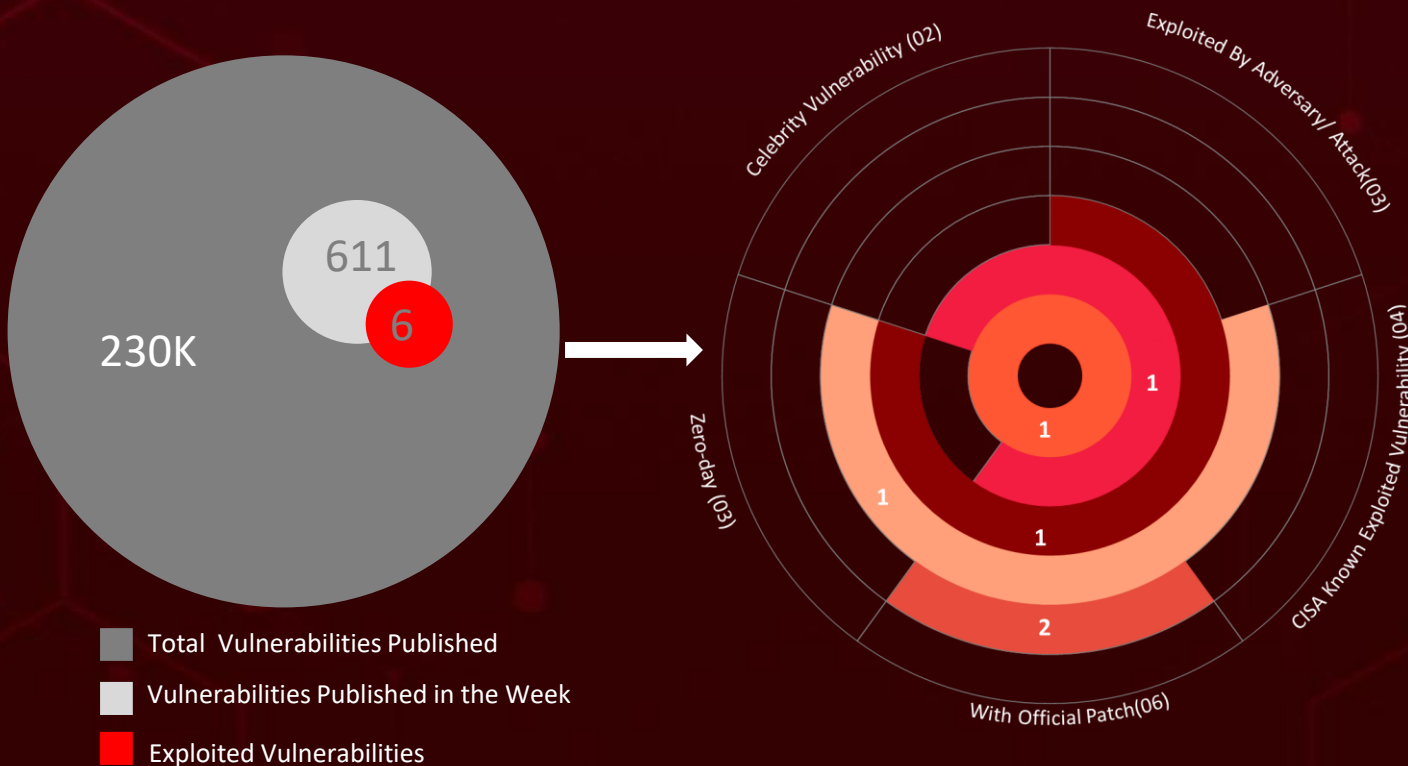
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	20

# Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **five** attacks were executed, **six** vulnerabilities were uncovered, and **two** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs revealed **three zero-day** vulnerabilities in **Apache**, **Microsoft** Windows SmartScreen, and **Fortinet** FortiOS SSL-VPN. The entity identified as the **UAC-0027** group executed a sophisticated cyber attack against Ukrainian organizations.

The **Mispadu** info stealer, a malware known for targeting Spanish and Portuguese speakers, specifically targets Mexican regions and leverages the **CVE-2023-36025** vulnerability to gain access. **Volt Typhoon** is actively targeting critical infrastructure in the United States, employing sophisticated tactics. These attacks are on the rise, posing a significant threat to users worldwide.



# High Level Statistics

5

Attacks  
Executed

- [DIRTYMOE](#)
- [FritzFrog](#)
- [Mispadu](#)
- [Xphase](#)
- [Albatat](#)

6

Vulnerabilities  
Exploited

- [CVE-2021-4034](#)
- [CVE-2021-44228](#)
- [CVE-2023-36025](#)
- [CVE-2024-23917](#)
- [CVE-2024-22024](#)
- [CVE-2024-21762](#)

2

Adversaries in  
Action

- [UAC-0027](#)
- [Volt Typhoon](#)



# Insights

## CVE-Less

### Chaos:

**EventLogCrasher** Raises Concerns; Microsoft Yet to Tackle Threat

## Volt Typhoon's Precision Strike:

State-sponsored cyber actors from China execute a precision strike on critical US infrastructure, showcasing their expertise in sophisticated tactics that go beyond traditional cyber threats.

## Half a Decade of Threat:

**UAC-0027's** Long-standing Cyber Arsenal - **DIRTYMOE**

## Rust-Powered Threat:

Victims affected by **Albatat ransomware** face a straightforward demand to contact the perpetrator and pay a ransom of **0.0015 Bitcoin**, underscoring the attack's uncomplicated yet menacing nature.

## Expanded Data Theft Arsenal:

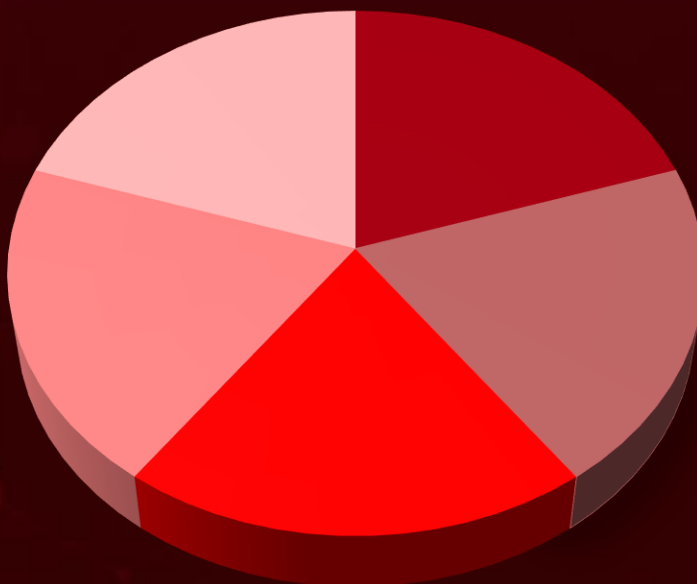
The **Mispadu** variant underscores the significance of the **CVE-2023-36025** vulnerability. Mispadu's enhanced capabilities now pose a direct threat to cryptocurrency wallets and other financial assets.

## Log4Shell

### Reimagined:

**FritzFrog's** Frog4Shell Revolutionizes Cyber Attacks

## Threat Distribution



■ Modular ■ Botnet ■ Infostealer ■ Clipper ■ Ransomware

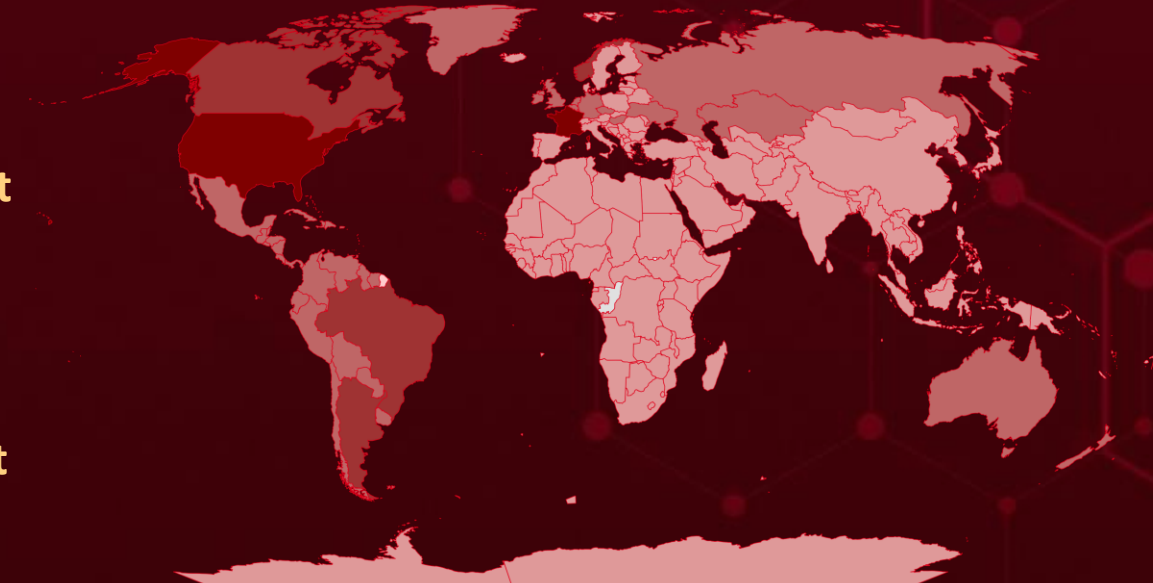


# Targeted Countries

Most



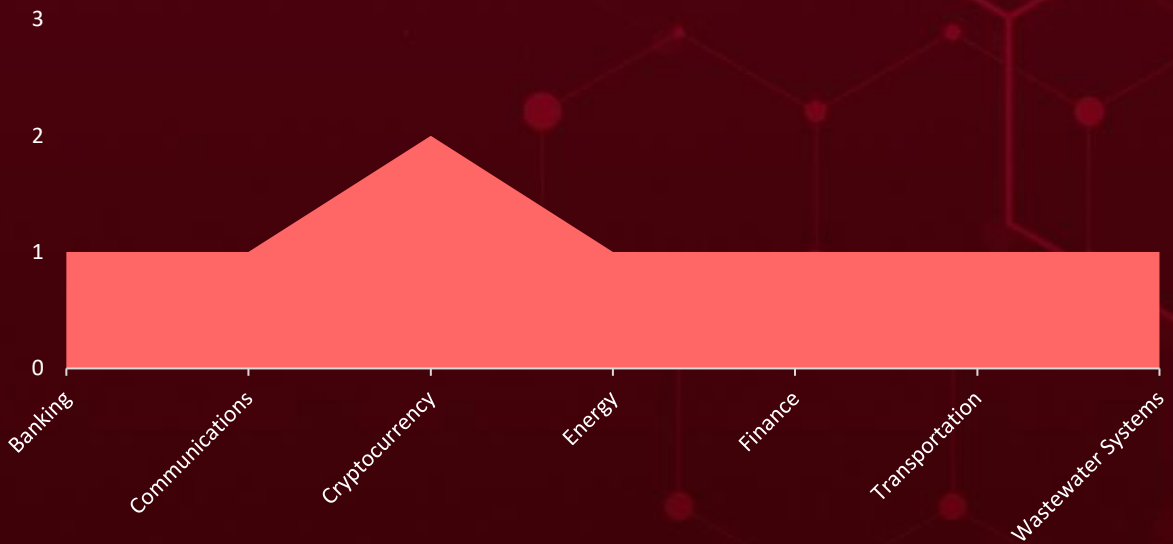
Least



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

Countries	Countries	Countries	Countries
USA	Trinidad and Tobago	Sint Maarten	Equatorial Guinea
France	Colombia	Germany	South Sudan
Canada	Ukraine	Suriname	Eritrea
Brazil	Costa Rica	Greenland	Tonga
Argentina	Honduras	Turks and Caicos Islands	Estonia
Norway	Cuba	Grenada	Uzbekistan
Jamaica	Ireland	UK	Eswatini
South Georgia and South Sandwich Islands	Curaçao	Guatemala	Niue
Bahamas	Kazakhstan	Uruguay	Ethiopia
Barbados	Czech Republic	Guyana	Pakistan
Anguilla	Mexico	Haiti	Benin
Belgium	Dominica	Venezuela	Pitcairn Islands
Monaco	Montserrat	Austria	Faroe Islands
Belize	Nicaragua	Albania	Saba
Saint Kitts and Nevis	New Zealand	Switzerland	Fiji
Bermuda	Panama	Belarus	Samoa
U.S. Virgin Islands	Peru	Papua New Guinea	Finland
Bolivia	Dominican Republic	East Timor	Singapore
Hungary	Paraguay	Slovenia	Antarctica
Aruba	Ecuador	Easter Island	South Africa
Luxembourg	Puerto Rico	U.S. Minor Outlying Islands	French Polynesia
British Virgin Islands	El Salvador	Angola	Sudan
Netherlands	Saint Barthélemy	Northern Cyprus	French Southern Territories
Australia	Falkland Islands	Egypt	Tanzania
Russia	Saint Lucia	Qatar	Gabon
Cayman Islands	Saint Pierre and Miquelon	Afghanistan	Turkey
Saint Martin	Antigua and Barbuda	Senegal	Gambia
Chile	Saint Vincent and the Grenadines		Bangladesh

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1190

Exploit Public-Facing Application

### T1588.006

Vulnerabilities

### T1027

Obfuscated Files or Information

### T1588

Obtain Capabilities

### T1218

System Binary Proxy Execution

### T1566

Phishing

### T1083

File and Directory Discovery

### T1055

Process Injection

### T1082

System Information Discovery

### T1105

Ingress Tool Transfer

### T1587.004

Exploits

### T1211

Exploitation for Defense Evasion

### T1204

User Execution

### T1068

Exploitation for Privilege Escalation

### T1584.005

Botnet

### T1078

Valid Accounts

### T1010

Application Window Discovery

### T1588.005

Exploits

### T1569

System Services

# 🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">DIRTYMOE (aka PURPLEFOX)</a></u>	The DIRTYMOE malware, also known as PURPLEFOX, is modular and has been a prominent player in the cyber threat landscape for over half a decade. It utilizes a rootkit to hinder removal and self-propagates by exploiting vulnerabilities and using authentication data.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Modular malware			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UAC-0027		Data Theft, and DDoS	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	6d817e8cd54c3a21f6d4aa437b16663a2a40b726014a8de1cbf9343101a0ab62, 43eef76fa966395bde56b4e3812831ca75ad010e3b8216103358deb09bdc14d1, 937e0068356e42654c9ab76cc34cf74dfa4c17b29e9439ebaa15d587757b14b0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">FritzFrog</a></u>	The FritzFrog Golang-based botnet reveals in its iterations, the employment of an exploit called 'Frog4Shell,' capitalizing on the Log4Shell vulnerability.	Log4Shell vulnerability	CVE-2021-4034 CVE-2021-44228
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Botnet			Polkit pkexec utility, Apache Log4j
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Data theft and Financial Loss	<a href="https://access.redhat.com/security/vulnerabilities/RHSB-2022-001">https://access.redhat.com/security/vulnerabilities/RHSB-2022-001</a> <a href="https://logging.apache.org/log4j/2.x/security.html">https://logging.apache.org/log4j/2.x/security.html</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d, fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291		

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>Mispadu</u>	The Mispadu Stealer, an infostealer that emerged in 2019. The malware employs sophisticated techniques to evade detection, including bypassing SmartScreen warnings by utilizing crafted .url files pointing to malicious binaries on a threat actor's network share.	Leverages the CVE-2023-36025 vulnerability	CVE-2023-36025
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Infostealer			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Data Theft	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	8e1d354dccc3c689899dc4e75fbd00ab076ac457de7fb83645fb735a46ad4ea, bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743eddfc53cf68789, fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4, 46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0da467eaf52		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Xphase</u>	The XPhase Clipper malware replaces cryptocurrency wallet addresses copied by users with addresses under the control of the attacker. Enabling attackers to reroute funds to their wallets instead of the intended recipients.	Social Engineering, Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Clipper			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Harvest credentials, Financial Loss	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	3bd57de116ae8a4f7dc69ac6fa73358e2063ea2b9c90fcb5886c3ccd35f5c524		




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><a href="#">Albabat (aka White Bat)</a></u>	<p>Albabat ransomware, made its debut in November 2023, emerging as a financially motivated threat crafted in Rust. Victims are then directed to a ransom note, instructing them to initiate contact with the perpetrator, with demands for a ransom of 0.0015 Bitcoin.</p>	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR		Data Theft, Financial Loss	AWS, Office365, PayPal, Sendgrid, and Twilio.
-			PATCH LINK
	-		
IOC TYPE	VALUE		
SHA256	e1c399c29b9379f9d1d3f17822d4496fce8a5123f57b33f00150f287740049e9, ce5c3ec17ce277b50771d0604f562fd491582a5a8b05bb35089fe466c67eef54, 483e0e32d3be3d2e585463aa7475c8b8ce254900bacfb9a546a5318fff024b74		
File Path	%USERPROFILE%\Albabat\Albabat.ekey, %USERPROFILE%\Albabat\Albabat_Logs.log, %USERPROFILE%\Albabat\personal_id.txt		




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-2021-4034</a>		Polkit pkexec utility	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*	FritzFrog Botnet
PwnKit (Polkit's Privilege Escalation Vulnerability)			
	CWE ID	T1068: Exploitation for Privilege Escalation	<a href="https://access.redhat.com/security/vulnerabilities/RHSB-2022-001">https://access.redhat.com/security/vulnerabilities/RHSB-2022-001</a>
	CWE-125 CWE-787		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2021-44228</a>		Apache Log4j: 2.0 - 2.14.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*	FritzFrog Botnet
Log4Shell (Apache Remote Code Execution Vulnerabilities)			
	CWE ID	T1059: Command and Scripting Interpreter	<a href="https://logging.apache.org/log4j/2.x/security.html">https://logging.apache.org/log4j/2.x/security.html</a>
	CWE-917 CWE-502 CWE-20 CWE-400		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-36025</u></a>		Windows: 10 - 11 23H2 & Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	Mispadu infostealer
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-23917</u></a>		TeamCity: 2017.1 - 2023.11.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*	-
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-288 CWE-306	T1190: Exploit Public-Facing Application, T1588: Obtain Capabilities	<a href="https://www.jetbrains.com/teamcity/download/other.html">https://www.jetbrains.com/teamcity/download/other.html</a> <a href="https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917.zip">https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917.zip</a> <a href="https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917_pre2018">https://download.jetbrains.com/teamcity/plugins/internal/fix_CVE_2024_23917_pre2018</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-22024</u></a>		Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1), Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability		cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1588: Obtain Capabilities, T1190: Exploit Public-Facing Application, T1005: Data from Local System, T1046: Network Service Discovery	<a href="https://forums.ivanti.com/s/product-downloads/">https://forums.ivanti.com/s/product-downloads/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21762</u></a>		Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*	-
Fortinet FortiOS SSL-VPN Out-of-Bounds Write Vulnerability		ASSOCIATED TTPs	
	CWE-787	T1203: Exploitation for Client Execution, T1588.005: Exploits	<a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-015">https://fortiguard.fortinet.com/psirt/FG-IR-24-015</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b><u>UAC-0027</u></b>	-	-	Ukraine
	<b>MOTIVE</b>		
	Financial gain, Information Theft and Espionage	-	
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	DIRTYMOE (also known as PURPLEFOX)	Windows
<b>TTPs</b>			
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1569.002: Service Execution; T1569: System Services; T1218.007: Msiexec; T1218: System Binary Proxy Execution; T1014: Rootkit; T1027: Obfuscated Files or Information; T1055: Process Injection; T1071.004: DNS; T1071: Application Layer Protocol; T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Volt Typhoon (aka Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, Insidious Taurus)</u></p>	China	Communications, Energy, Transportation Systems, and Water and Wastewater Systems	United States, Canada, Australia, and New Zealand
	<b>MOTIVE</b>		
	Information theft and espionage	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	<b>TARGETED CVEs</b>		
-	-	-	

### TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; T1592: Gather Victim Host Information; T1589: Gather Victim Identity Information; T1589.002: Email Addresses; T1590: Gather Victim Network Information; T1591: Gather Victim Org Information; T1593: Search Open Websites/Domains; T1594: Search Victim-Owned Websites; T1583.003: Botnet; T1584.005: Botnet; T1584.004: Server; T1587.004: Exploits; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.004: Unix Shell; T1047: Windows Management Instrumentation; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1006: Direct Volume Access; T1070.009: Clear Persistence; T1070.001: Clear Windows Event Logs; T1070.004: File Deletion; T1036.005: Match Legitimate Name or Location; T1112: Modify Registry; T1027.002: Software Packing; T1218: System Binary Proxy Execution; T1110.002: Password Cracking; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1003.001: LSASS Memory; T1003.003: NTDS; T1552: Unsecured Credentials; T1552.004: Private Keys; T1087.001: Local Account; T1010: Application Window Discovery; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1654: Log Enumeration; T1046: Network Service Discovery; T1120: Peripheral Device Discovery; T1069: Permission Groups Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1082: System Information Discovery; T1614: System Location Discovery; T1016.001: Internet Connection Discovery; T1033: System Owner/User Discovery; T1007: System Service Discovery; T1124: System Time Discovery; T1563: Remote Service Session Hijacking; T1021.007: Cloud Services; T1021.001: Remote Desktop Protocol; T1550: Use Alternate Authentication Material; T1078.004: Cloud Accounts; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1074: Data Staged; T1113: Screen Capture; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1090: Proxy; T1090.001: Internal Proxy; T1090.003: Multi-hop Proxy; T1048: Exfiltration Over Alternative Protocol

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actors **UAC-0027, Volt Typhoon**, and malware **DIRTYMOE, FritzFrog, Mispadu, Xphase, Albatat**.

## 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 **six exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UAC-0027, Volt Typhoon**, and malware **DIRTYMOE, FritzFrog, Mispadu, Xphase, Albatat** in Breach and Attack Simulation(BAS).



# Threat Advisories

[EventLogCrasher Flaw: Not Serviced by Microsoft](#)

[Ukraine Hit by Cyber Attack 2,000+ Computers Infected by DIRTYMOE](#)

[FritzFrog Expanding Its Lethal Reach with Frog4Shell](#)

[Mispadu Leverages CVE-2023-36025 Vulnerability in Latest Attack](#)

[Deceptive Crypto Sites A Breeding Ground for XPhase Clipper](#)

[JetBrains TeamCity Authentication Bypass Flaw, Paving the Way for Server Takeover](#)

[Volt Typhoon: A Cyber Threat to U.S. Critical Infrastructure](#)

[Ivanti Addresses Yet Another VPN Flaw Within a Month](#)

[Albatat Ransomware Infiltrates via Counter-Strike Cheat Utility](#)

[Critical Vulnerability in FortiOS SSL VPN Exploited in the Wild](#)

# 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)

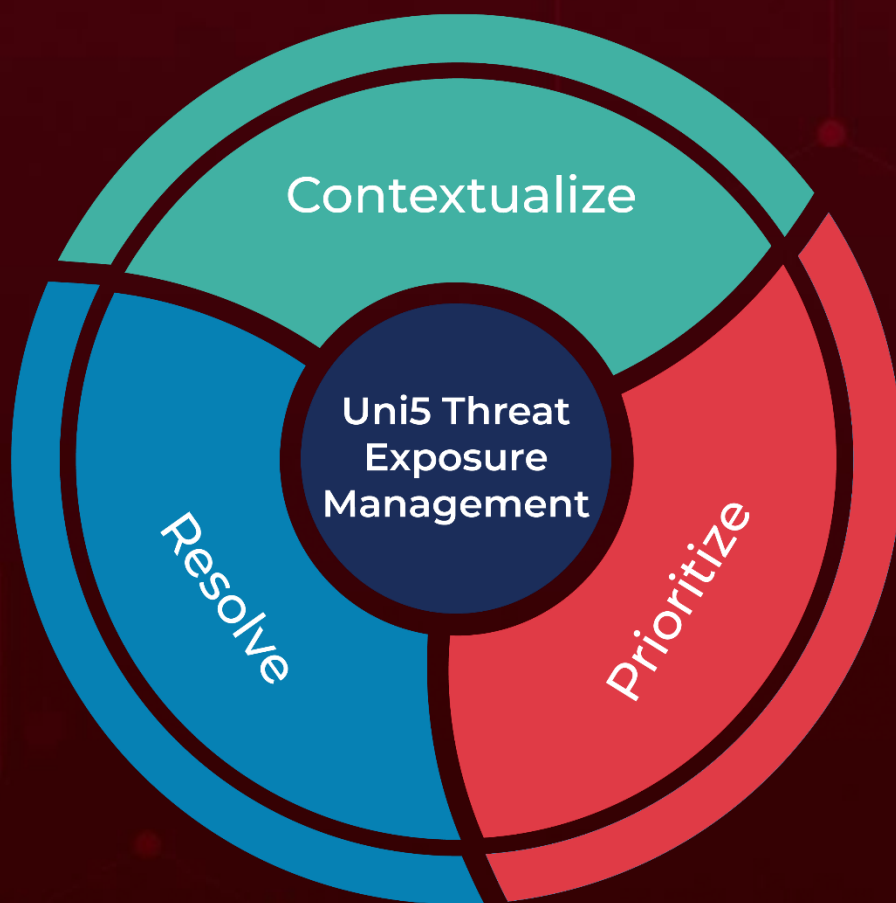
Attack Name	TYPE	VALUE
<a href="#"><u>DIRTYMOE</u></a>	SHA256	6d817e8cd54c3a21f6d4aa437b16663a2a40b726014a8de1cbf9343101a0ab62, 43eef76fa966395bde56b4e3812831ca75ad010e3b8216103358deb09bdc14d1, 937e0068356e42654c9ab76cc34cf74dfa4c17b29e9439ebaa15d587757b14b0
<a href="#"><u>FritzFrog</u></a>	SHA256	f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d, fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291
<a href="#"><u>Mispadu</u></a>	SHA256	8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea, bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743eddfc53cf68789, fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4, 46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0da467eaf52, 03bdae4d40d3eb2db3c12d27b76ee170c4813f616fec5257cf25a068c46ba15f, 1b7dc569508387401f1c5d40eb448dc20d6fb794e97ae3d1da43b571ed0486a0, e136717630164116c2b68de31a439231dc468ddcbee9f74cca511df1036a22ea

Attack Name	TYPE	VALUE
<u>Xphase</u>	SHA256	3bd57de116ae8a4f7dc69ac6fa73358e2063ea2b9c90fcb5886c3ccd35f5c524
<u>Albatat</u>	SHA256	e1c399c29b9379f9d1d3f17822d4496fce8a5123f57b33f00150f287740049e9, ce5c3ec17ce277b50771d0604f562fd491582a5a8b05bb35089fe466c67eef54, 483e0e32d3be3d2e585463aa7475c8b8ce254900bacfb9a546a5318fff024b74, 614a7f4e0044ed93208cbd4a5ab6916695e92ace392bc352415b24fe5b2d535c, bfb8247e97f5fd8f9d3ee33832fe29f934a09f91266f01a5fed27a3cc96f8fbb
	File Path	%USERPROFILE%\Albatat\Albatat.ekey, %USERPROFILE%\Albatat\Albatat_Logs.log, %USERPROFILE%\Albatat\personal_id.txt, %USERPROFILE%\Albatat\readme\README.html, %USERPROFILE%\Albatat\readme\assets\banner.jpg, %USERPROFILE%\Albatat\readme\assets\script.js, %USERPROFILE%\Albatat\readme\assets\style.css, %USERPROFILE%\Albatat\readme\pages\faq.html, %USERPROFILE%\Albatat\wallpaper_albatat.jpg

# 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

**February 12, 2024 • 5:00 AM**

© 2024 All Rights are Reserved by Hive Pro®



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