

Date of Publication
November 6, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

30 OCTOBER to 5 NOVEMBER 2023

Table Of Contents

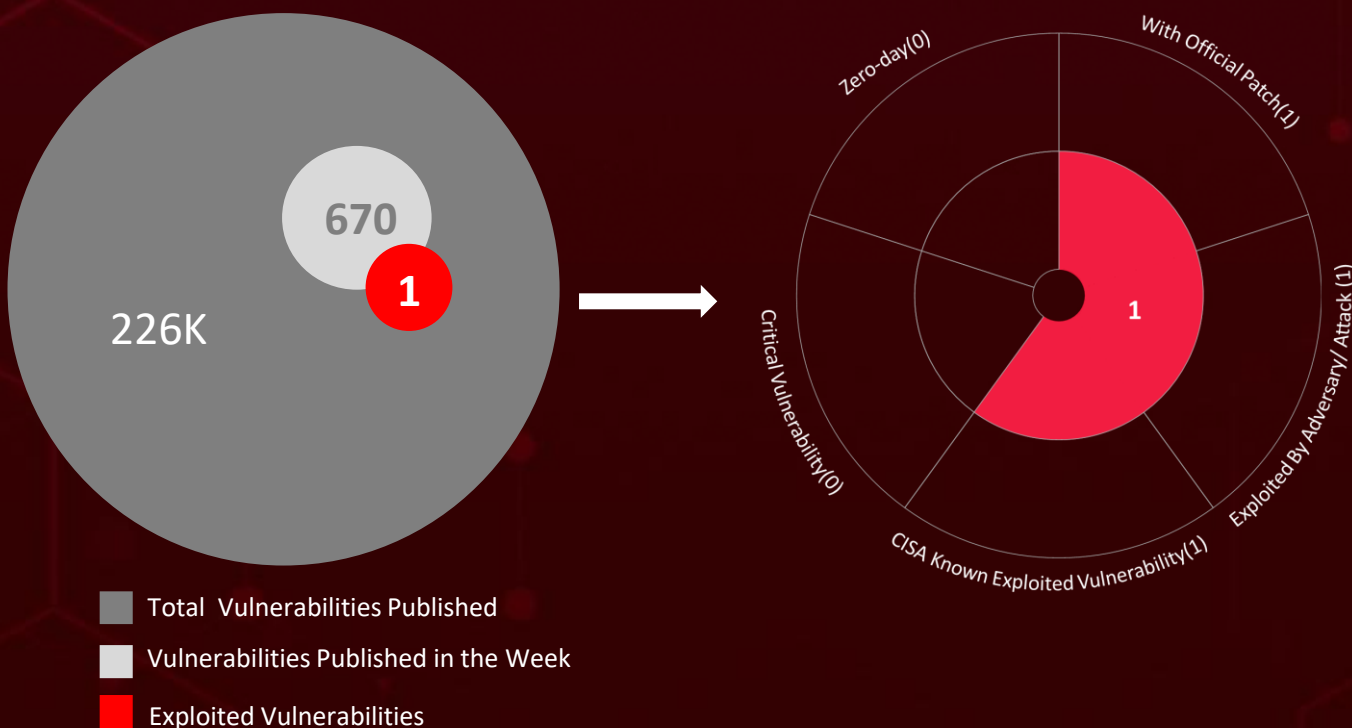
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	12
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	20

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **six** executed attacks, **three** instances of adversary activity, and **one** exploited vulnerability, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a malware framework named **LIONTAIL**, utilized by the **Scarred Manticore** threat group in their latest campaign, mainly targeting the Middle East region.

Meanwhile, a critical vulnerability (**CVE-2023-46604**) in Apache ActiveMQ is being exploited by the **HelloKitty ransomware** in various attacks. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

6

Attacks
Executed

1

Vulnerabilities
Exploited

3

Adversaries in
Action

- SIGNBT
- LPEClient
- BiBi-Linux
- GHOSTPULSE
- LIONTAIL
- HelloKitty

- CVE-2023-46604

- Lazarus Group
- Scarred
- Manticore
- MuddyWater

MuddyWater

Launches new spearphishing campaign targeting two Israeli entities

Lazarus Group

Exploiting software vulnerabilities and introducing the SIGNBT malware to gain control over their victims in latest campaign

HelloKitty

ransomware exploiting a critical vulnerability (CVE-2023-46604) in Apache ActiveMQ

Israeli-Hamas conflict

Going digital now by using a sophisticated Linux-based wiper malware known as BiBi-Linux Wiper, launching cyberattacks with the aim of sowing chaos and fear

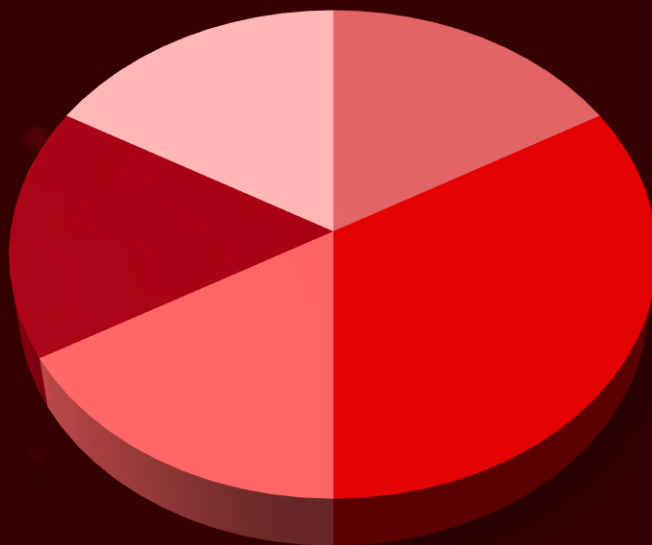
Scarred Manticore

Group conducting a highly sophisticated cyber espionage campaign targeting Middle East by using LIONTAIL malware framework

GHOSTPULSE

A new cyber attack campaign uses fake MSIX Windows apps posing as real applications

Threat Distribution



■ Downloader ■ Loader ■ Wiper ■ Passive loader ■ Ransomware

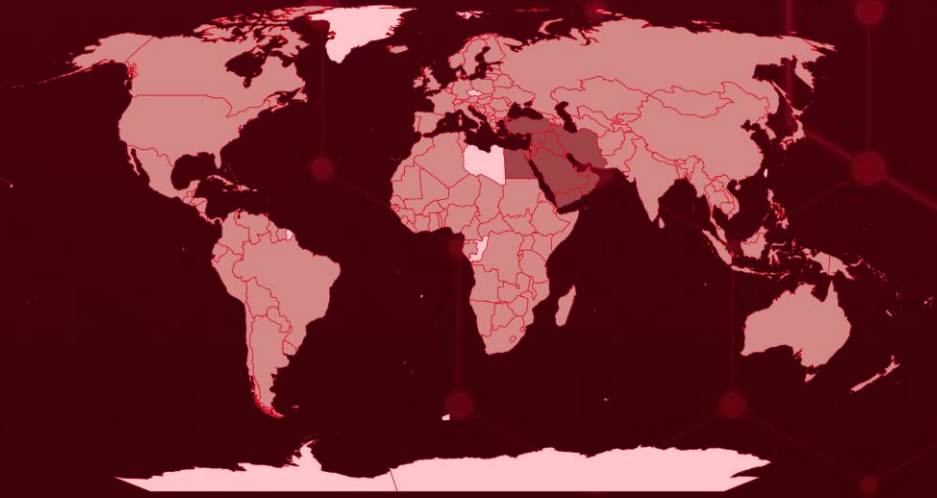


Targeted Countries

Most



Least



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

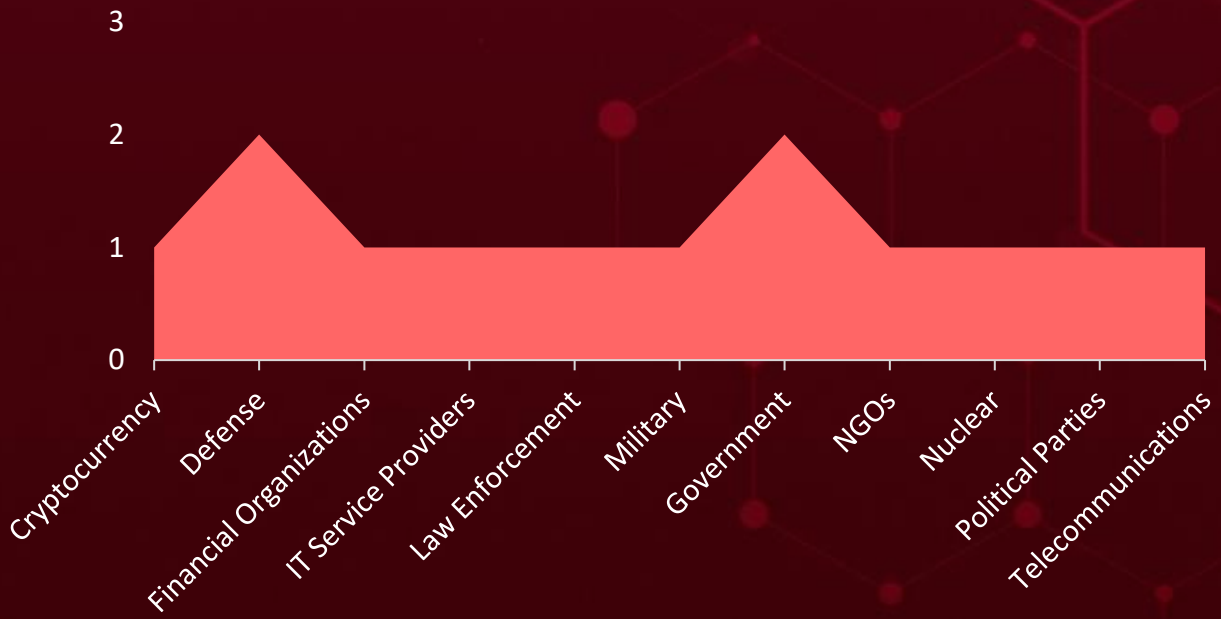
Countries
Israel
Kuwait
Saudi Arabia
Oman
Cyprus
Bahrain
Egypt
Yemen
Iran
Qatar
Iraq
Syria
Turkey
United Arab Emirates
Jordan
Lebanon
Russia
Micronesia
Timor-Leste
Belize
North Korea

Countries
Benin
Somalia
Bhutan
Malaysia
Bolivia
Namibia
Bosnia and Herzegovina
Papua New Guinea
Botswana
Senegal
Brazil
Sudan
Brunei
Uganda
Bulgaria
Marshall Islands
Burkina Faso
Montenegro
Burundi
New Zealand
Cabo Verde

Countries
Pakistan
Cambodia
Poland
Cameroon
Samoa
Canada
Singapore
Central African Republic
Congo
Monaco
Costa Rica
Mozambique
Côte d'Ivoire
Nepal
Croatia
Niger
Cuba
Norway
Algeria
Palestine
Czech Republic (Czechia)
Peru
Eswatini

Countries
Denmark
Bahamas
Djibouti
Saint Kitts & Nevis
Dominica
Sao Tome & Principe
Dominican Republic
Seychelles
DR Congo
Slovenia
Ecuador
South Korea
Andorra
St. Vincent & Grenadines
El Salvador
Sweden
Equatorial Guinea
Tanzania
Eritrea
Tonga
Estonia
Turkmenistan

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1082

System Information Discovery

T1083

File and Directory Discovery

T1190

Exploit Public-Facing Application

T1059.001

PowerShell

T1204

User Execution

T1071.001

Web Protocols

T1140

Deobfuscate/Decode Files or Information

T1574

Hijack Execution Flow

T1071

Application Layer Protocol

T1056

Input Capture

T1204.002

Malicious File

T1203

Exploitation for Client Execution

T1547.001

Registry Run Keys / Startup Folder

T1005

Data from Local System

T1041

Exfiltration Over C2 Channel

T1105

Ingress Tool Transfer

T1027

Obfuscated Files or Information

T1518.001

Security Software Discovery

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>SIGNBT</u>	SIGNBT malware is a loader, which means that it is used to load other malware onto a victim's system. It can load a variety of different types of malware, such as backdoors, ransomware, and data stealers. It has been attributed to the North Korean Lazarus Group.	-	-
		IMPACT	AFFECTED PRODUCTS
		Inject Shellcode	-
			PATCH LINK
			-
TYPE			
Loader			
ASSOCIATED ACTOR			
Lazarus			
IOC TYPE	VALUE		
MD5	9cd90dff2d9d56654dbecdc409e1ef3, 88a96f8730b35c7406d57f23bbba734d, 54df2984e833ba2854de670cce43b823, Ae00b0f490b122ebab614d98bb2361f7, e6fa116ef2705ecf9677021e5e2f691e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>LPEClient</u>	LPEClient malware is an HTTP(S) downloader that is used to download and execute other malware on a victim's system. It is often used to download and execute backdoors, ransomware, and other types of malware that can be used to steal data, disrupt operations, or gain control of systems.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Executes other malware, stealing data	-
			PATCH LINK
			-
TYPE			
Downloader			
ASSOCIATED ACTOR			
Lazarus			
IOC TYPE	VALUE		
MD5	3a77b5054c36e6812f07366fb70b007d, e89fa6345d06da32f9c8786b65111928		
File Path	%systeme%\wbem\wbemcomn.dll, %ProgramData%\Microsoft\Windows\ServiceSetting\ESENT.dll		

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>BiBi-Linux</u>	BiBi-Linux malware is a new Linux wiper malware that has been used to target Israeli organizations. It was first discovered in October 2023, and it is believed to be used by a pro-Hamas hacktivist group.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data loss	-
			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad		
SHA1	0dbabdc1ae8c3c8a48224ee3c3e8b6a17f41d6e7		
MD5	de9da4fcfb8320b9d34239effce1871a		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>GHOSTPULSE</u>	GHOSTPULSE malware is a new type of malware that was discovered in October 2023. It operates as a multi-stage loader, decrypting its payload and deploying various types of malware while employing advanced defense evasion techniques.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Executes other malware	-
			PATCH LINK
ASSOCIATED ACTOR			
-			-

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
LIONTAIL	LIONTAIL is a passive loader that uses undocumented functionalities of the HTTP.sys driver to load incoming payloads. It is highly customizable and allows attackers to evade detection.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Passive loader			
ASSOCIATED ACTOR		Data theft and Financial Losses	PATCH LINK
Scarred Manticore			-
IOC TYPE	VALUE		
SHA256	daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33, f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b66122596, 2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da838, 67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde9542, 4f6351b8fb3f49ff0061ee6f338cd1af88893ed20e71e211e8adb6b90e50a3b8		


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HelloKitty	HelloKitty emerged as a ransomware variant in late 2020, focusing mainly on Windows systems and gaining a reputation for its agility in adopting new Tactics, Techniques, and Procedures (TTPs). It utilized a Golang-based packer to enhance its ability to evade detection. By early 2021, a Linux version of HelloKitty had been spotted operating in the wild.	-	CVE-2023-46604
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR		Data theft and Financial Losses	PATCH LINK
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604
IOC TYPE	VALUE		
SHA256	c3c0cf25d682e981c7ce1cc0a00fa2b8b46cce2fa49abe38bb412da21da99cb7, 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a0, 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4		
Email	service@helloworldcat[.]online		
IPv4	172.245.16[.]125		


Vulnerabilities Exploited


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46604</u>		Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:* :* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*	HelloKitty ransomware
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories/data/CVE-2023-46604



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</u></p>	North Korea	Satellite, Software, Media, Defense, Manufacturing, ICT, And Financial Sectors.	Korea
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-42793	Volgmer, Scout, ForestTiger, FeedLoad, RollSling, and HazyLoad	TeamCity
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing;T1195: Supply Chain Compromise;T1204: User Execution;T1047: Windows Management Instrumentation;T1543: Create or Modify System Process;T1574.002: DLL Side-Loading;T1070: Indicator Removal;T1573: Encrypted Channel;T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Scarred Manticore</u></p>	Iran	Government, Military, IT Service Providers, Financial Organizations, NGOs, and Telecommunications Sectors	Middle East
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LIONTAIL	Windows
TTPs			
<p>TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1574: Hijack Execution Flow, T1078: Valid Accounts, T1543: Create or Modify System Process, T1003: OS Credential Dumping, T1082: System Information Discovery, T1005: Data from Local System, T1041: Exfiltration Over C2 Channel, T1490: Inhibit System Recovery, T1036: Masquerading, T1083: File and Directory Discovery, T1105: Ingress Tool Transfer</p>			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)</u></p>	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Aerospace	Middle East, Asia, Africa, Europe, and North America
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	-	-	
TTPs			
TA0043: Reconnaissance, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0010: Exfiltration, TA0011: Command and Control, T1566: Phishing, T1566.002: Spearphishing Link, T1547: Boot or Logon Autostart: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1105: Ingress Tool Transfer, T1204: User Execution, T1204.002: Malicious File			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **Lazarus Group , Scarred Manticore , MuddyWater** and malware **SIGNBT, LPEClient, BiBi-Linux, GHOSTPULSE, LIONTAIL, HelloKitty**.

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 **one exploited vulnerability**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Lazarus Group , Scarred Manticore , MuddyWater** and malware **SIGNBT, LPEClient, BiBi-Linux, GHOSTPULSE, LIONTAIL, HelloKitty** in Breach and Attack Simulation(BAS).

Threat Advisories

[Lazarus Unleash SIGNBT Malware in Latest Campaign](#)

[From Bullets to Bytes: The Hamas-Israel Conflict Goes Digital](#)

[Hackers Utilize MSIX App Packages to Disseminate GHOSTPULSE Malware](#)

[Atlassian's Latest Critical Confluence Flaw Poses Risk of Data Loss](#)

[Scarred Manticore's Middle Eastern Gambit](#)

[Apache ActiveMQ RCE Vulnerability Exploited by HelloKitty Ransomware](#)

[MuddyWater Returns with a New Spear-Phishing Campaign](#)

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>SIGNBT</u>	MD5	9cd90dff2d9d56654dbecdc409e1ef3, 88a96f8730b35c7406d57f23bbba734d, 54df2984e833ba2854de670cce43b823, Ae00b0f490b122ebab614d98bb2361f7, e6fa116ef2705ecf9677021e5e2f691e, 31af3e7fff79bc48a99b8679ea74b589, 9b62352851c9f82157d1d7fcafeb49d3
	File Path	%system%\ualapi.dll, %system%\ualapi.dll, %system%\ualapi.dll, %system%\ualapi.dll, C:\GoogleD\Coding\JS\Node\winhttp.dll
<u>LPEClient</u>	MD5	3a77b5054c36e6812f07366fb70b007d, e89fa6345d06da32f9c8786b65111928
	File Path	%system%\wbem\wbemcomn.dll, %ProgramData%\Microsoft\Windows\ServiceSetting\ESENT.d ll
<u>BiBi-Linux</u>	SHA256	23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edc b16d7d558efad
	SHA1	0dbabdc1ae8c3c8a48224ee3c3e8b6a17f41d6e7
	MD5	de9da4fcfb8320b9d34239effce1871a

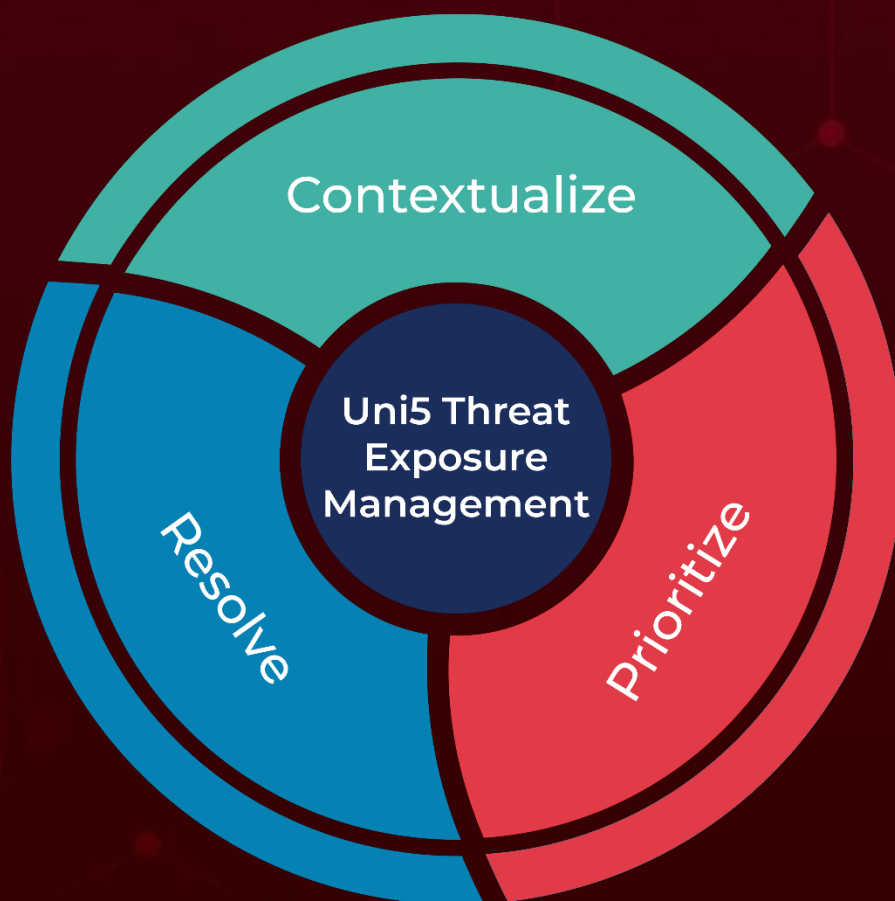
Attack Name	TYPE	VALUE
<u>LIONTAIL</u>	SHA256	daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33, f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b6612259, 2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da88, 67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde954, 4f6351b8fb3f49ff0061ee6f338cd1af88893ed20e71e211e8adb6b90e50a3b8, f6c316e2385f2694d47e936b0ac4bc9b55e279d530dd5e805f0d963cb47c3c0d, 1485c0ed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1c00c780419a4, 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d033, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0cb, e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, a2598161e1efff623de6128ad8aafba9da0300b6f86e8c951e616bd19f0a572b, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 6f0a38c9eb9171cd323b0f599b74ee571620bc3f34aa07435e7c5822663de60, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, b71aa5f27611a2089a5bbe34fd1aafb45bd71824b4f8c2465cf4754db746aa79, da450c639c9a50377233c0f195c3f6162beb253f320ed57d5c9bb9c7f0e83999

Attack Name	TYPE	VALUE
<u>HelloKitty</u>	SHA256	c3c0cf25d682e981c7ce1cc0a00fa2b8b46cce2fa49abe38bb412da21da99cb7, 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a, 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4
	Email	service@hellokittycat[.]online
	IPv4	172.245.16[.]125
	URLs	hxxp://172.245.16[.]125/m4.png, hxxp://172.245.16[.]125/m2.png

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 6, 2023 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com