

Date of Publication
July 14, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

7 to 13 JULY 2025

Table Of Contents

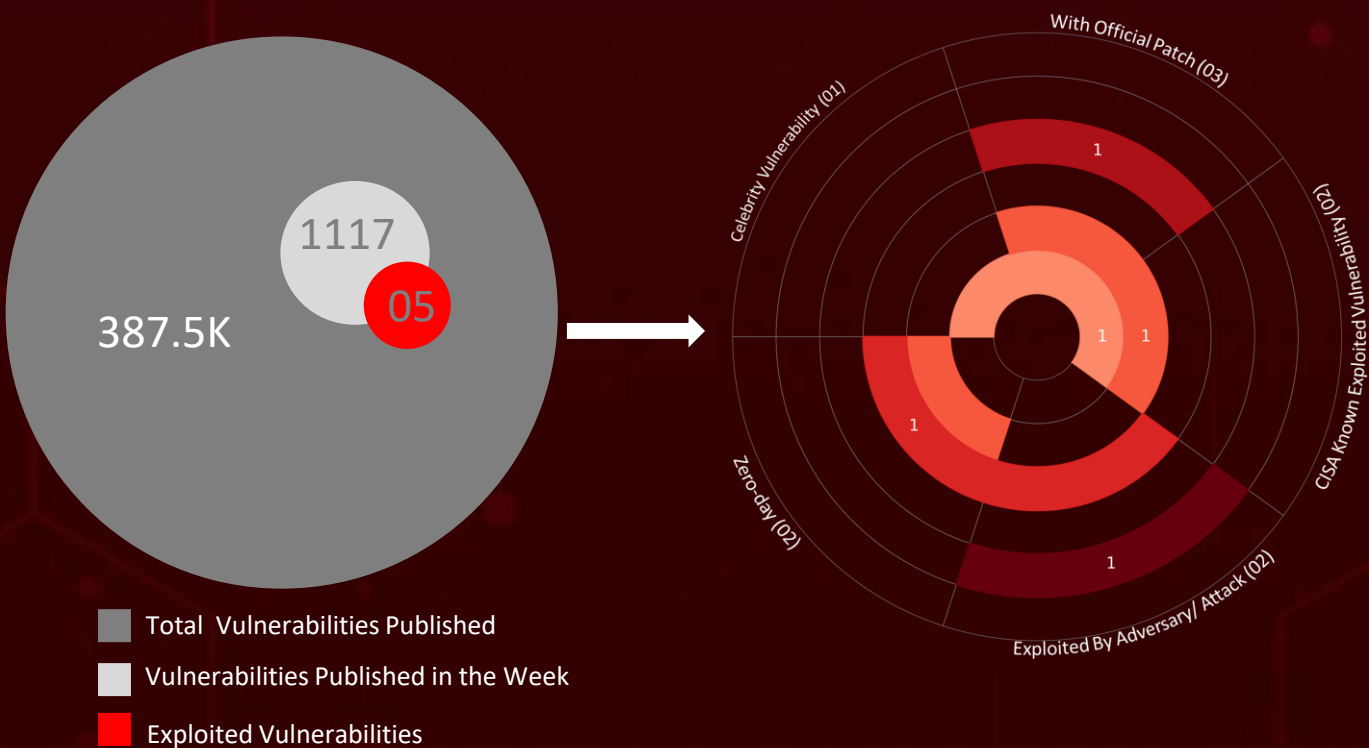
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	13
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	19

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **four** major attacks were detected, **five** critical vulnerabilities were actively exploited, and **two** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the key developments, **Dire Wolf**, a sophisticated ransomware group first identified in May 2025, is targeting sectors across 13 countries using double extortion tactics. A newly uncovered botnet campaign, **RondoDox**, is actively exploiting critical vulnerabilities in TBK DVRs and Four-Faith devices, allowing attackers to compromise systems and repurpose them for malicious operations covertly.

APT36, a Pakistan-based threat group, has resumed cyber-espionage activity against India's defense sector, this time focusing on Linux systems, particularly those running BOSS Linux. An Initial Access Broker group, **Gold Melody**, has been linked to a high-impact campaign targeting ASP.NET applications by exploiting leaked machine keys to gain unauthorized access and enable further exploitation. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



High Level Statistics

4

Attacks
Executed

- [Dire Wolf](#)
- [RondoDox](#)
- [Batavia](#)
- [Lumma](#)

5

Vulnerabilities
Exploited

- [CVE-2025-49719](#)
- [CVE-2025-6554](#)
- [CVE-2024-3721](#)
- [CVE-2024-12856](#)
- [CVE-2025-5777](#)

2

Adversaries in
Action

- [APT36](#)
- [Gold Melody](#)



Insights

Microsoft SQL
Server Info Leak Bug
Among **130**
Vulnerabilities
Patched in July

Batavia Spyware
Campaign Hits Over
100 Users Across
Dozens of Russian
Organizations

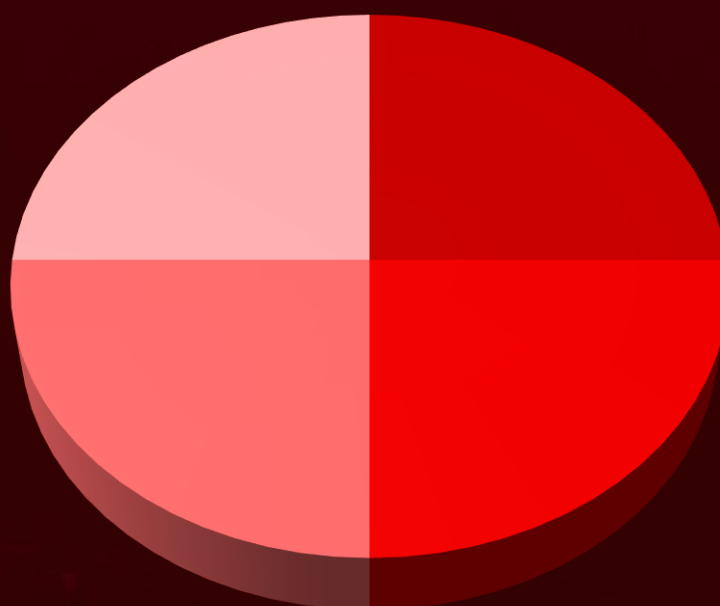
Golang-Powered Ransomware
'**Dire Wolf**' Disrupts
Manufacturing and Tech Sectors

APT36 Targets BOSS Linux
in Stealthy Cyber Attack Against
India's Defense Networks

CitrixBleed 2 Vulnerability
Now Weaponized in Active
Campaigns

'Free VPN' and
'Minecraft Skin'
Repositories
Spread **Lumma**
Stealer

Threat Distribution



■ Ransomware ■ Botnet ■ Stealer ■ Spyware

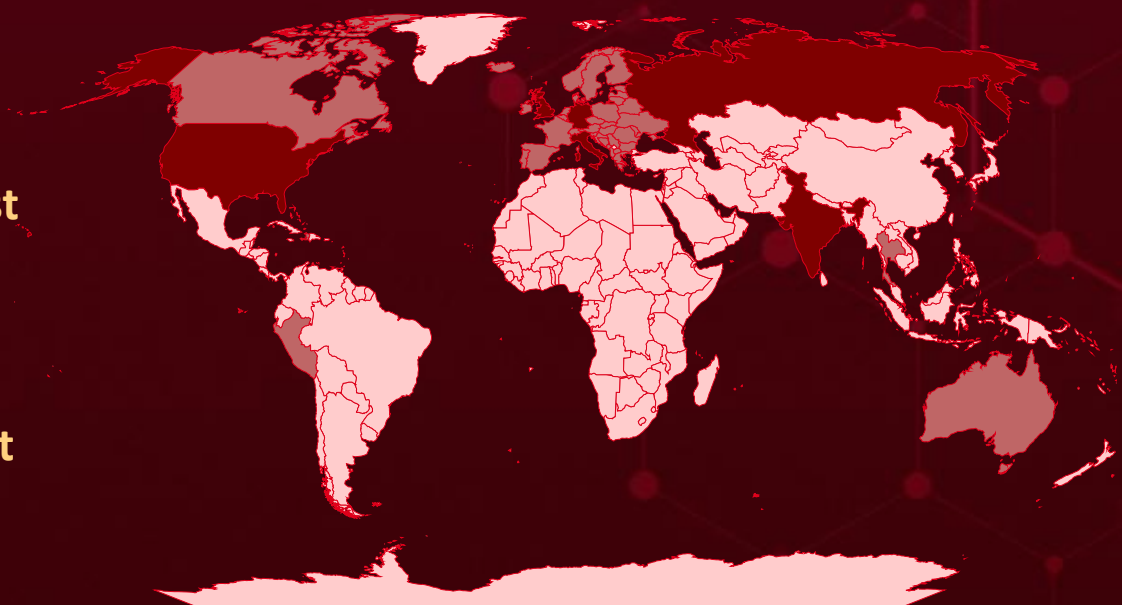


Targeted Countries

Most



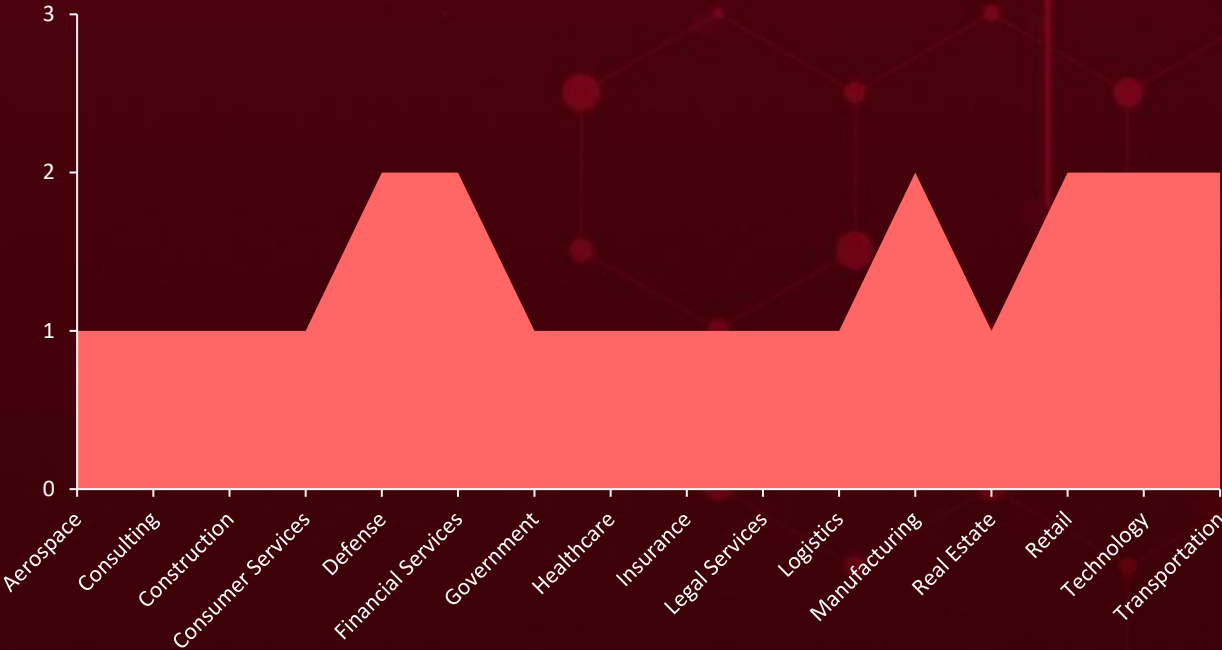
Least



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

Countries	Countries	Countries	Countries
United States	France	Palau	Grenada
United Kingdom	Moldova	Eritrea	Ecuador
Russia	Albania	Sri Lanka	Guatemala
Germany	Montenegro	Barbados	Vietnam
India	Greece	Equatorial Guinea	Guinea
Italy	North Macedonia	Eswatini	Nigeria
Poland	Haiti	Congo	Guinea-Bissau
Malta	Peru	Ethiopia	Oman
Slovenia	Holy See	Antigua and Barbuda	Guyana
Belgium	Portugal	Fiji	Panama
Netherlands	Hungary	Tajikistan	Bhutan
Bosnia and Herzegovina	Austria	Argentina	Philippines
San Marino	Iceland	Uruguay	Bolivia
Bulgaria	Serbia	Armenia	Costa Rica
Thailand	Andorra	Chile	Honduras
Canada	Slovakia	Gabon	Saint Lucia
Monaco	Ireland	Paraguay	Algeria
Croatia	Spain	Gambia	Saudi Arabia
Norway	Australia	Rwanda	Botswana
Czech Republic	Switzerland	Georgia	Sierra Leone
Romania	Latvia	Cuba	Brazil
Denmark	Ukraine	Belize	Solomon Islands
Singapore	Lithuania	South Africa	Indonesia
Estonia	Belarus	Ghana	South Sudan
Sweden	Luxembourg	Dominica	Iran
Finland	Liechtenstein	Benin	Sudan
Bahrain	Turkey	Togo	Iraq
	Bahamas		Syria

Targeted Industries



TOP MITRE ATT&CK TTPs

<u>T1059</u> Command and Scripting Interpreter	<u>T1071</u> Application Layer Protocol	<u>T1082</u> System Information Discovery	<u>T1027</u> Obfuscated Files or Information	<u>T1036</u> Masquerading
<u>T1105</u> Ingress Tool Transfer	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits	<u>T1070</u> Indicator Removal
<u>T1204</u> User Execution	<u>T1189</u> Drive-by Compromise	<u>T1543</u> Create or Modify System Process	<u>T1566.001</u> Spearphishing Attachment	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1562.001</u> Disable or Modify Tools	<u>T1083</u> File and Directory Discovery	<u>T1190</u> Exploit Public-Facing Application	<u>T1095</u> Non-Application Layer Protocol	<u>T1498</u> Network Denial of Service



Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Dire Wolf</u>	Dire Wolf is a ransomware written in Golang, compressed with UPX, and engineered to disable recovery options while employing robust encryption. Each attack is tailored, featuring distinctive ransom notes and dedicated negotiation portals, highlighting a targeted operation.	-	-
		IMPACT	AFFECTED PLATFORM
		Data Exfiltration, Data Integrity Risks, Financial Loss	Windows (cross-platform capability via Golang)
			PATCH LINK
TYPE			
Ransomware			
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3, 8fdee53152ec985ffeeda3d7a85852eb5c9902d2d480449421b4939b1904aad		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RondoDox</u>	RondoDox is designed for Linux-based systems. Its shell script downloader scans for writable directories with execution permissions to deploy its payload. Once established, it sets up multiple redundant mechanisms to retain control, such as modifying system startup scripts, creating hidden services, and renaming critical security utilities to evade detection and removal.	Exploiting Critical Vulnerabilities in TBK DVRs and Four-Faith devices	CVE-2024-3721 CVE-2024-12856
		IMPACT	AFFECTED PLATFORM
		Resource Drain, Disruption of Services	TBK DVR-4104 and DVR-4216 devices, Four-Faith F3x24 and F3x36
			PATCH LINK
TYPE			
Botnet			
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	0a9ebbecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9, 9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd		




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
<u>Batavia</u>	Batavia is a Windows-based spyware that steals the victim's documents and collects sensitive system information, including installed programs, drivers, and operating system components.	Multi-Stage Phishing Campaign	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Exfiltration of Sensitive Information	Windows
Spyware			PATCH LINK
ASSOCIATED ACTOR			
-			-





NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Lumma</u>	Lumma Stealer is a potent info-stealing malware that evades detection by injecting itself into memory, employing multiple layers of encryption and obfuscation. The payload, cleverly disguised as a Base64-encoded DLL concealed within a block of French text, is specifically crafted to bypass most antivirus defenses.	Social Engineering via Github	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Exfiltration, Evasion of Detection	Windows
Stealer			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	acbaa6041286f9e3c815cd1712771a490530f52c90ce64da20f28cfa0955a5ca		





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>CVE-2025-49719</u>		Microsoft SQL Server: 2016 - 2022	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:sql_server:*:*:*:*:*:*	-
Microsoft SQL Server Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1213: Data from Information Repositories, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49719

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6554</u>		Google Chrome prior to 138.0.7204.96	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-6554 , https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-3721</u>		TBK DVR-4104 and DVR-4216 up to 20240412	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tbk_vision:tbk_dvr_4104:*:*:*:*:*:*	RondoDox botnet
TBK DVR OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1071: Application Layer Protocol	


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-12856</u>		Four-Faith F3x24 and F3x36	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:four-faith:f3x24:*:*:*:*:*:*	RondoDox botnet
Four-Faith OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1499: Endpoint Denial of Service, T1078.001: Default Accounts	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-5777</u>	CitrixBleed 2	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1190: Exploit Public-Facing Application, T1059: Command and Scripting, T1068: Exploitation for Privilege Escalation	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
<div></div> <div><u>APT36 (aka Mythic Leopard, Transparent Tribe, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, C-Major)</u></div>	Pakistan	Defense, Government	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	BOSS (Bharat Operating System Solutions) Linux
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1543.003: Windows Service; T1036: Masquerading; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1571: Non-Standard Port; T1204: User Execution; T1592: Gather Victim Host Information; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1113: Screen Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Gold Melody (aka Prophet Spider, UNC961)</u>	-	Financial Services, Manufacturing, Retail, Technology, Transportation, Logistics	Europe and the U.S.
	MOTIVE		
	Financial Gain, Information theft, and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1036.005: Match Legitimate Resource Name or Location; T1036.010: Masquerade Account Name; T1046: Network Service Discovery; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1136: Create Account; T1136.001: Local Account; T1190: Exploit Public-Facing Application; T1217: Browser Information Discovery; T1505: Server Software Component; T1505.003: Web Shell; T1572: Protocol Tunneling; T1587: Develop Capabilities; T1587.001: Malware; T1036: Masquerading			

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 **APT36, Gold Melody**, and malware **Dire Wolf, RondoDox, Batavia, Lumma**.

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 **five exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT36, Gold Melody**, and malware **Dire Wolf, RondoDox, Lumma** in Breach and Attack Simulation(BAS).

Threat Advisories

[Dire Wolf Ransomware: A New Global Cyber Threat Emerges](#)

[Microsoft's July 2025 Patch Tuesday Addresses 130 Vulnerabilities](#)

[RondoDox Botnet Campaign Targets TBK DVRs and Four-Faith Routers](#)

[APT36's Covert Linux Attack on India's Defense Sector](#)

[Batavia Multi-Stage Spyware Campaign Targeting Russian Industrial Sector](#)

[Malware in Disguise: How GitHub Became a Dropper's Playground](#)

[Gold Melody Is Weaponizing Leaked ASP.NET Machine Keys](#)

[Multiple Flaws in Citrix NetScaler ADC and Gateway Pose Immediate Threat](#)

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)

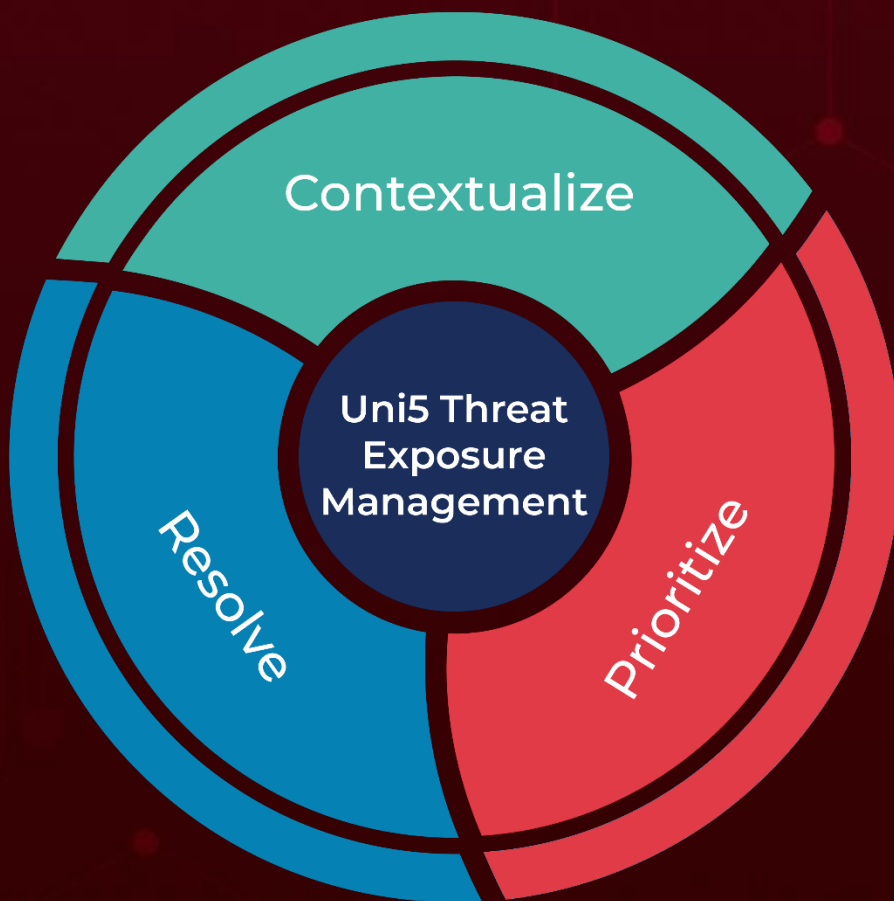
Attack Name	TYPE	VALUE
<u>Dire Wolf</u>	SHA256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3,8fdee53152ec985ffeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
	SHA1	ed7c9fbd42605c790660df86b7ec325490f6d827,4a5852e9f9e20b243d8430b229e41b92949e4d69
	MD5	a71dbf2e20c04da134f8be86ca93a619,aa62b3905be9b49551a07bc16eaad2ff
	TOX ID	B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2
	TOR Address	hxxp[:]//direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd[.]onion
	File Name	data345.exe
<u>RondoDox</u>	SHA256	0a9ebbcecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9,9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd,6c81fd73b4bef6fef379cbefdcce7f374ea7e6bf1bf0917cf4ca7b72d4cee788,a55a3859a203ca2bae7399295f92aeae61d845ffa173c1938f938f5c148eef99,57573779f9a62eecb80737d41d42165af8bb9884579c50736766abb63d2835ba,3daa53204978b7797bd53f5c964eed7a73d971517a764785ce3ab65a9423c2e7,

Attack Name	TYPE	VALUE
<u>RondoDox</u>	SHA256	8bf8928bc255e73e0b5b0ce13747c64d82d5f2647da129f189138773733ac21f, 20a24b179bdbbdcc0053838c0484ea25eff6976f2b8cb5630ab4efb28b0f06b5, 42aa715573c7d2fca01914504cb7336db715d73d1e20d23e4bd37f2e4f4fe389
<u>Lumma</u>	SHA256	acbaa6041286f9e3c815cd1712771a490530f52c90ce64da20f28cfa0955a5ca

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

July 14, 2025 • 9:30 PM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com