

Date of Publication
July 7, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

30 JUNE to 6 JULY 2025

Table Of Contents

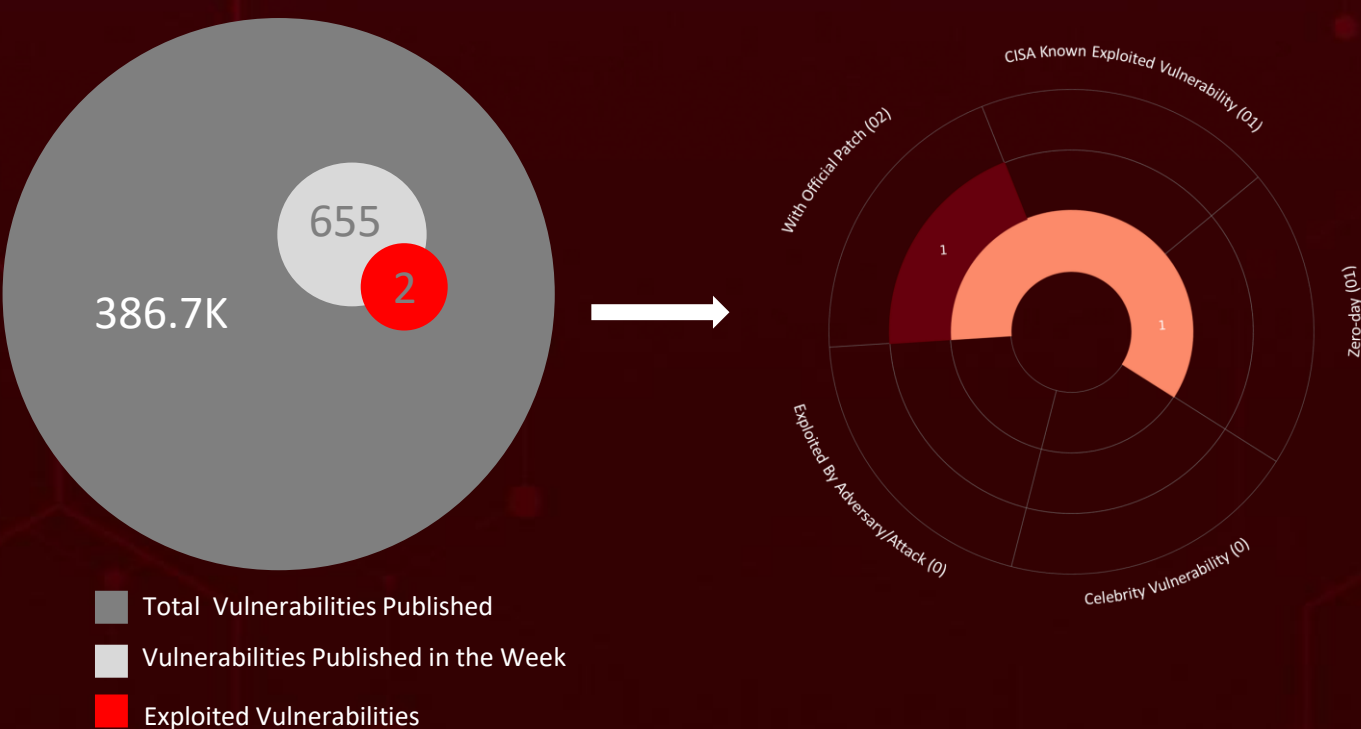
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	19

Summary

HiveForce Labs has identified a surge in cyber threats, with **five** attacks executed, **two** vulnerabilities uncovered, and **one** active adversary exposed in the past week alone highlighting the relentless nature of cyberattacks.

One of the critical vulnerabilities, **CVE-2025-6554**, is a zero-day flaw in Google Chrome’s V8 JavaScript engine that enables attackers to corrupt memory and potentially execute arbitrary code. Google has confirmed that this bug is being actively exploited in the wild. Another high-severity flaw, **CVE-2025-6463**, affects the Forminator Forms WordPress plugin (used by over 600,000 websites), allowing unauthenticated attackers to delete arbitrary files from the server due to unsafe file path handling. Users are urged to update or disable the plugin until it’s secured.

On the threat actor front, Latin America is currently being targeted by **Blind Eagle**, a cybercriminal group deploying banking-themed phishing emails laced with remote access tools like **Remcos** and **AsyncRAT**. Simultaneously, a new ransomware variant called **DEVMAN**, derived from the DragonForce codebase, has surfaced with unique traits and a leak site called Devman’s Place. DEVMAN reflects the evolving complexity of ransomware-as-a-service (RaaS) ecosystems, where operators blur lines between independence and collaboration. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

5

Attacks
Executed

- Remcos
- AsyncRAT
- NimDoor
- DEVMAN
- Hpingbot

2

Vulnerabilities
Exploited

- CVE-2025-6554
- CVE-2025-6463

1

Adversaries in
Action

- Blind Eagle



Insights

NimDoor Unleashed

North Korea-linked hackers breached macOS via a fake Zoom update, dropping stealthy Nim-based malware to steal sensitive data..

Chrome Under Fire: Google confirms in-the-wild exploitation of **CVE-2025-6554**, a critical V8 type confusion zero-day - update now!

Hpingbot on the Rise

This stealthy, Go-based botnet is infecting Linux, Windows, and IoT devices, using hping3 and Pastebin to launch DDoS attacks and sustain long-term control.

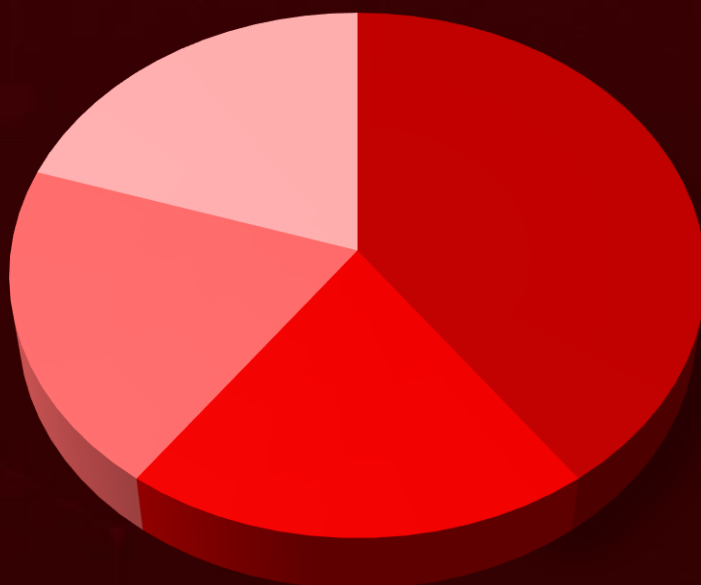
CVE-2025-6463: A critical flaw in Forminator Forms lets attackers delete server files - 600K+ sites at risk.

Blind Eagle is targeting Latin America with crafty bank-themed phishing emails that deploy remote access tools like **Remcos** and **AsyncRAT**, giving attackers full control of victims.

DEVMAN Ransomware

Emerges: Spawned from DragonForce code, this new variant is hitting Asia and Africa, with its own leak site, Devman's Place.

Threat Distribution



■ RAT

■ Backdoor

■ Ransomware

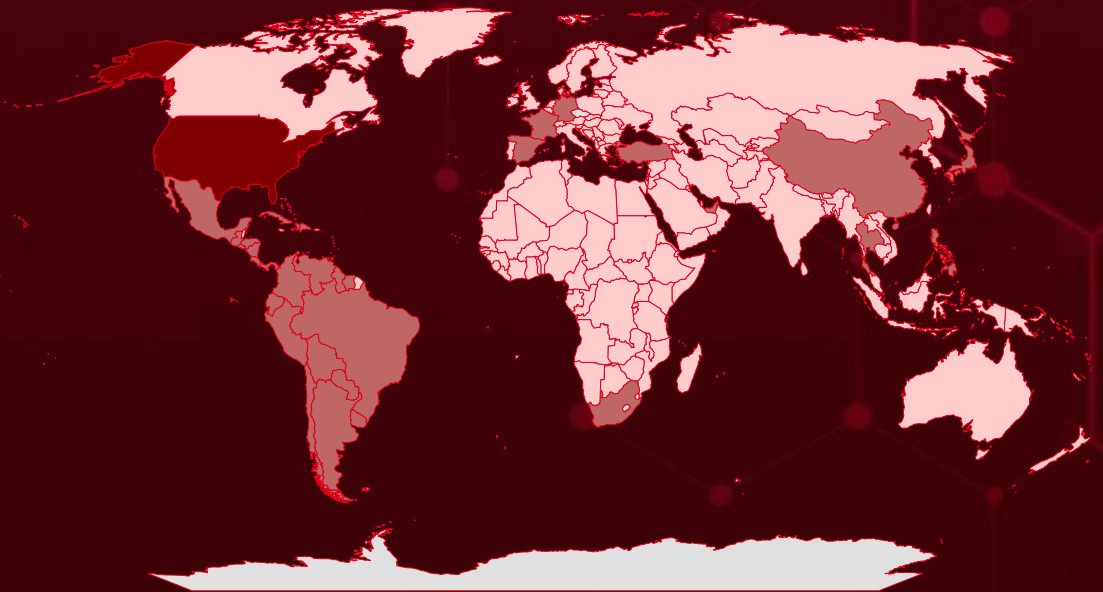
■ Botnet



Targeted Countries

Most

Least



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

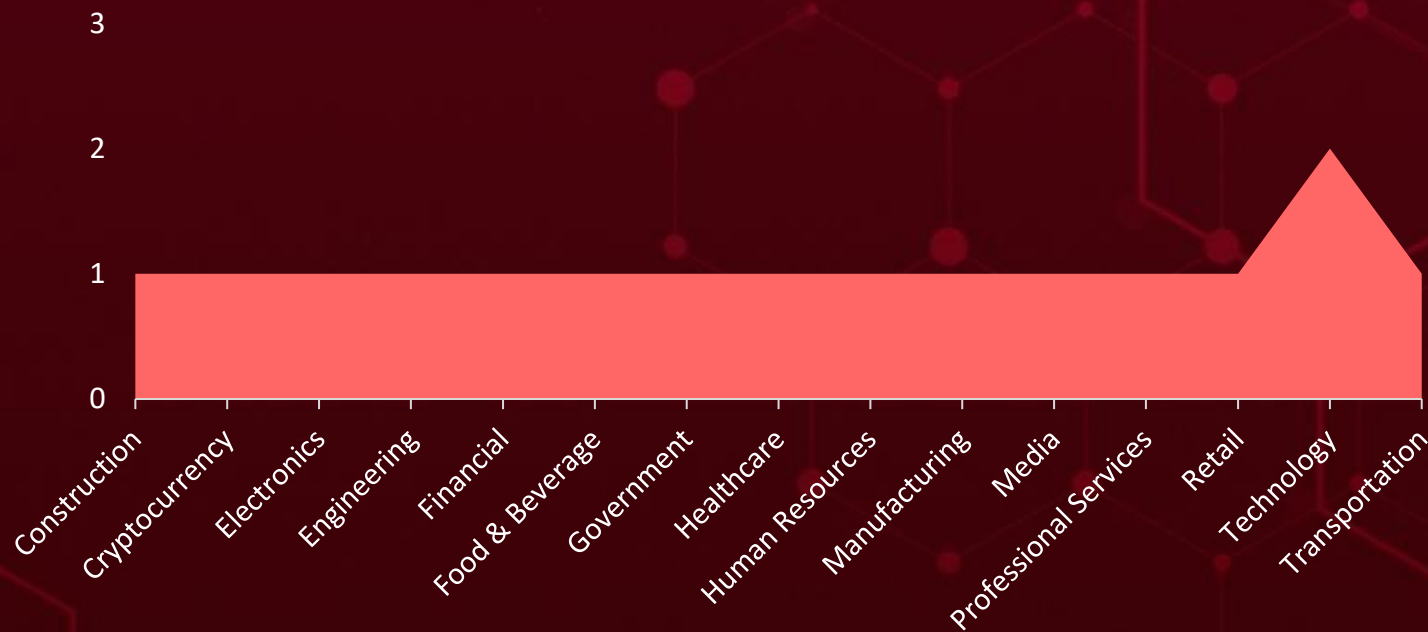
Countries
United States
Panama
Thailand
Argentina
Singapore
Bolivia
Honduras
Brazil
Mexico
Chile
Peru
China
Spain
Colombia
United Arab Emirates
Costa Rica
Japan
Cuba
Venezuela
Dominican Republic
Nicaragua

Countries
Ecuador
Paraguay
El Salvador
Philippines
France
South Africa
Germany
Suriname
Guatemala
Turkey
Guyana
Haiti
Uruguay
Slovakia
Nigeria
Angola
Antigua and Barbuda
Barbuda
Romania
Albania
Taiwan
Comoros

Countries
India
Niger
Indonesia
North Korea
Iran
Norway
Iraq
Pakistan
Ireland
Andorra
Israel
Brunei
Italy
Burkina Faso
Jamaica
Portugal
Benin
Qatar
Jordan
Russia
Kazakhstan

Countries
Malaysia
Canada
Maldives
Togo
Mali
Trinidad and Tobago
Malta
Central African Republic
Marshall Islands
Tuvalu
Martinique
Ukraine
Mauritania
United Kingdom
Mauritius
Bosnia and Herzegovina
Lebanon
Vanuatu
Lesotho
Vietnam
Liberia

Targeted Industries



TOP MITRE ATT&CK TTPs

<u>T1059</u> Command and Scripting Interpreter	<u>T1053</u> Scheduled Task/Job	<u>T1588</u> Obtain Capabilities	<u>T1027</u> Obfuscated Files or Information	<u>T1070</u> Indicator Removal
<u>T1140</u> Deobfuscate/Decode Files or Information	<u>T1566</u> Phishing	<u>T1204</u> User Execution	<u>T1656</u> Impersonation	<u>T1132.001</u> Standard Encoding
<u>T1588.006</u> Vulnerabilities	<u>T1070.004</u> File Deletion	<u>T1082</u> System Information Discovery	<u>T1486</u> Data Encrypted for Impact	<u>T1583.006</u> Web Services
<u>T1555.001</u> Keychain	<u>T1012</u> Query Registry	<u>T1041</u> Exfiltration Over C2 Channel	<u>T1059.001</u> PowerShell	<u>T1543.002</u> Systemd Service

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos, is often employed by attackers to gain complete control over systems. It operates stealthily, elevates privileges, and persists through reboots. Common methods of delivery include phishing emails, exploit kits, and watering hole attacks.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Information Theft, Remote Control	-
Blind Eagle			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	5cf4a8c83f8591950c24c8b5d79c5464e4cb1b608fc61775f605d6a3503c73c3, 1728133a5a75adc097d2b5dee5693c5b1b72d25832435213bada40be433b2f75		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a publicly available remote access trojan (RAT) on GitHub. A modified version ensures persistence by creating a scheduled task that triggers at startup. Upon activation, a complex sequence initiates AsyncRAT within Windows Sandbox, which must be manually enabled and requires a reboot.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Remote Control, Information Theft	-
Blind Eagle			PATCH LINK
	-		
IOC TYPE	VALUE		
SHA256	394908cbe5ba04a3b772ef11ea6a2c6a0c8d3d9689c89ccd1410aaa583bb07d7, 48ee878fefc7d5d9df66fc978dfaafcfc61129acf92b1143e1b865ab292be9f0, 2e432426a7a0a10a0068c035368f749c298e1ef1add61e31a8b25da74676fcaa		

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>NimDoor</u>	<p>NimDoor is a sophisticated macOS backdoor malware, primarily attributed to North Korean threat actors, that specifically targets Web3 and cryptocurrency businesses. It distinguishes itself by utilizing the relatively uncommon Nim programming language for its binaries, making it harder to detect and analyze. The infection typically begins with social engineering tactics, that initiates a multi-stage infection process, including process injection and the deployment of persistent components. Once established, NimDoor is capable of exfiltrating sensitive data like browser information, Keychain credentials, and Telegram chat histories, all communicated securely to its command-and-control servers using encrypted channels.</p>	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise, Data Theft	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	469fd8a280e89a6edd0d704d0be4c7e0e0d8d753e314e9ce205d7006b573865f		

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>DEVMAN</u>	DEVMAN ransomware is a new and evolving variant belonging to the DragonForce malware family, which has emerged as a significant threat in 2025. This ransomware encrypts victim data and appends a ".DEVMAN" extension to the locked files, dropping a ransom note. DEVMAN first exfiltrates sensitive data and then encrypts the systems. While seemingly still under development due to some peculiar behaviors, DEVMAN has already shown capabilities for rapid lateral movement, and is actively engaging in collaborations with established Ransomware-as-a-Service (RaaS) groups, expanding its reach across various industries globally.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403		
Filename	e47qfsnz2trbkhnt.devman		

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
Hpingbot	<p>Hpingbot is a newly discovered, rapidly spreading botnet family that emerged in June 2025. Written in the Go programming language, it's a cross-platform threat, infecting both Windows and Linux/IoT devices across various processor architectures. Hpingbot is notable for its innovative use of Pastebin for payload delivery and leveraging the legitimate network testing tool hping3 to launch powerful DDoS attacks. While its primary purpose appears to be DDoS, it also exhibits sophisticated persistence mechanisms, including modifying system services and scheduled tasks, and the ability to download and execute arbitrary payloads, indicating potential for broader malicious activities beyond just DDoS.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		System Persistence, Launch DDoS attacks	Windows, Linux, IoT
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	3359037b5a331ecf79ab9aa114f673e96a227a038fdb377badfbe16b5eaa4e7f		

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-2025-6554</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 LINK
	CWE-843	T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1189: Drive-by Compromise; T1068: Exploitation for Privilege Escalation	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6463</u>		WordPress Forminator Forms plugin versions prior to 1.44.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wpmudev:forminator_forms:*:*:*:*:wordpress:*:*	-
WordPress Forminator Plugin Unauthenticated Arbitrary File Deletion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1485: Data Destruction; T1070: Indicator Removal	https://wordpress.org/plugins/forminator/advanced/ , https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/forminator/forminator-forms-contact-form-payment-form-custom-form-builder-1442-unauthenticated-arbitrary-file-deletion-triggered-via-administrator-form-submission-deletion

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)</u>	Colombia	Financial institutions	Latin America
	MOTIVE		
	Information theft and espionage, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	Remcos, AsyncRAT	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1656: Impersonation; T1027: Obfuscated Files or Information; T1011: Exfiltration Over Other Network Medium; T1140: Deobfuscate/Decode Files or Information; T1053: Scheduled Task/Job; T1078: Valid Accounts; T1588: Obtain Capabilities; T1588.004: Digital Certificates; T1552: Unsecured Credentials; T1132: Data Encoding; T1132.001: Standard Encoding			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actor **Blind Eagle** and malware **Remcos, AsyncRAT, NimDoor, DEVMAN Ransomware, Hpingbot**.

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 **two exploited vulnerabilities**.
- Testing the efficacy of their security controls **AsyncRAT, NimDoor, DEVMAN Ransomware** and **Hpingbot** in Breach and Attack Simulation(BAS).

Threat Advisories

[CVE-2025-6554: Google Chrome's Zero-Day Flaw Exploited in the Wild](#)

[Blind Eagle's Banking Trap: Phishing Colombia's Financial Sector](#)

[Scripted Deception: NimDoor Malware Unfolds in Fake Zoom Update](#)

[Critical Forminator Plugin Flaw Can Delete Your Site's Core Files](#)

[DEVMAN Ransomware Is a New Derivative of the DragonForce Family](#)

[Hpingbot Rising: The Botnet That Thinks Outside the Payload](#)

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>Remcos</u>	SHA256	5cf4a8c83f8591950c24c8b5d79c5464e4cb1b608fc61775f605d6a3503c73c3, 1728133a5a75adc097d2b5dee5693c5b1b72d25832435213bada40be433b2f75
<u>AsyncRAT</u>	SHA256	394908cbe5ba04a3b772ef11ea6a2c6a0c8d3d9689c89ccd1410aaa583bb07d7, 48ee878fetc7d5d9df66fc978dfaafcfc61129acf92b1143e1b865ab292be9f0, 2e432426a7a0a10a0068c035368f749c298e1ef1add61e31a8b25da74676fcaa, 2a84f9440f120edd032eddb4b61339ee184743d47805e2ed50572ca4905c1fdd, 66663cf3596b0e6fd2721d81f91cda058ca61feb46f9943ef1a91fec7a68590d, 666f0c305b0a6cc558192918bc144c3119d898c33656101395140d93e9e10e69, fa32ea24d1a6041be009ad0c59ce61f3d00e0588700c709c0222ecd8c8c3753, 81ffcabc8db8db4f42ee4d53f35d47e5cca9aba8fadf972a97596b79492cb03
<u>NimDoor</u>	SHA256	469fd8a280e89a6edd0d704d0be4c7e0e0d8d753e314e9ce205d7006b573865f
<u>DEVMAN</u>	SHA256	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403

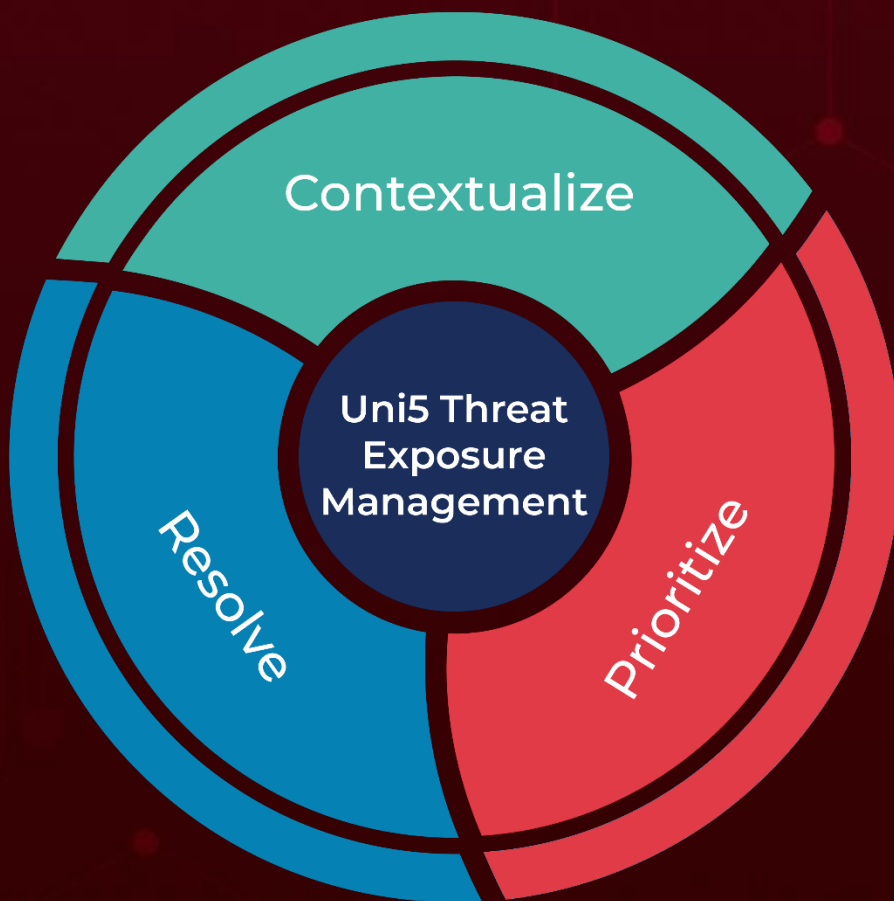
Attack Name	TYPE	VALUE
<u>DEVMAN</u>	SHA1	4a34bbad85312ef34b60818a47f7b5bb8e9a7e26
	MD5	e84270afa3030b48dc9e0c53a35c65aa
	Filename	e47qfsnz2trbkhnt.devman
	Mutex	hsfjuukjzloqu28oajh727190
	Tox ID	9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
	TOR Address	qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd[.]onion
<u>Hpingbot</u>	SHA256	3359037b5a331ecf79ab9aa114f673e96a227a038fdb377badfbe16b5eaa4e7f

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

July 7, 2025 • 11:30 PM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com