Date of Publication
December 29, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

22 to 28 DECEMBER 2025

Table Of Contents

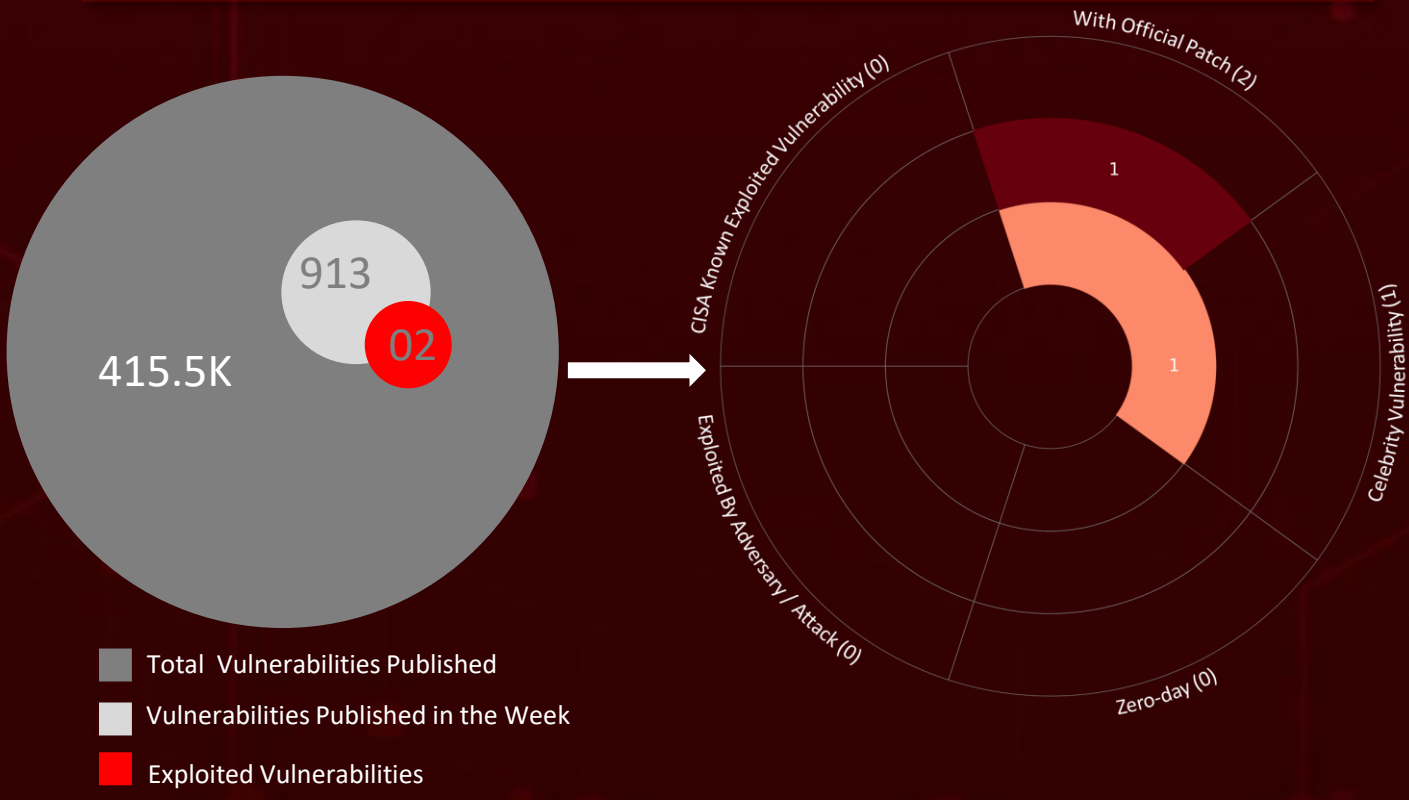
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **three** major attacks were detected, **two** critical vulnerabilities were publicly disclosed, and **one** active threat actor group was monitored, signaling a concerning escalation in malicious activity.

CVE-2025-68613 is a critical remote code execution vulnerability in the **n8n** workflow automation platform. It stems from weak sandbox isolation in the expression evaluation engine. This flaw enables full system compromise, unauthorized data access, and manipulation of automated workflows.

Prince of Persia, also referred to as Infy, is an Iranian state-linked advanced persistent threat that has been active since 2007. The group is known for long-term cyber-espionage operations targeting strategic entities in support of national intelligence objectives.

CVE-2025-14847 is a high-severity vulnerability dubbed **MongoBleed** in the MongoDB Server that requires no authentication. It allows remote attackers to read sensitive heap memory by exploiting an error in Zlib packet decompression, potentially exposing confidential data and internal memory contents. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

3
Attacks Executed

2
Vulnerabilities Exploited

1
Adversaries in Action

- Foudre
- Tonnerre
- MacSync

- CVE-2025-68613
- CVE-2025-14847

- Prince of Persia

Insights

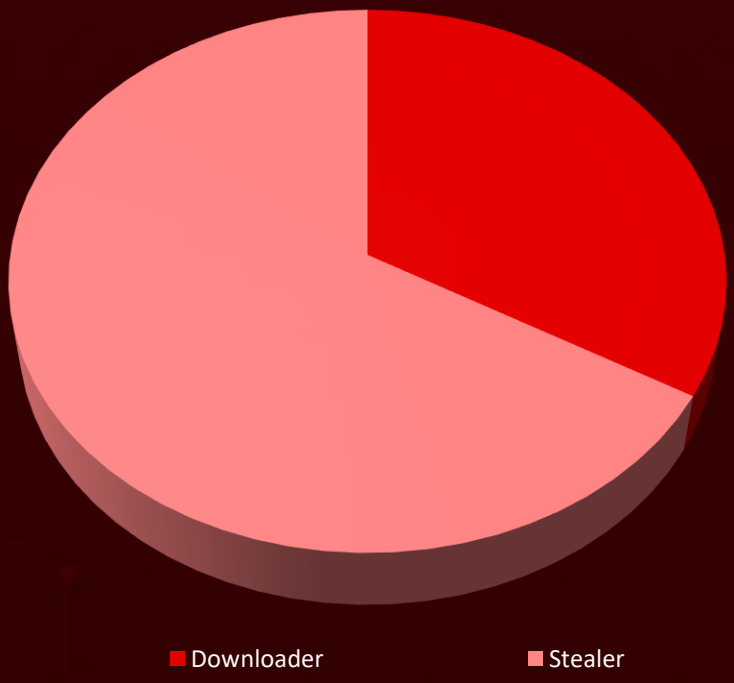
MacSync Stealer: Gatekeeper Bypass Without Warnings

CVE-2025-68613 n8n Under Fire: Data Exposure and Workflow Manipulation

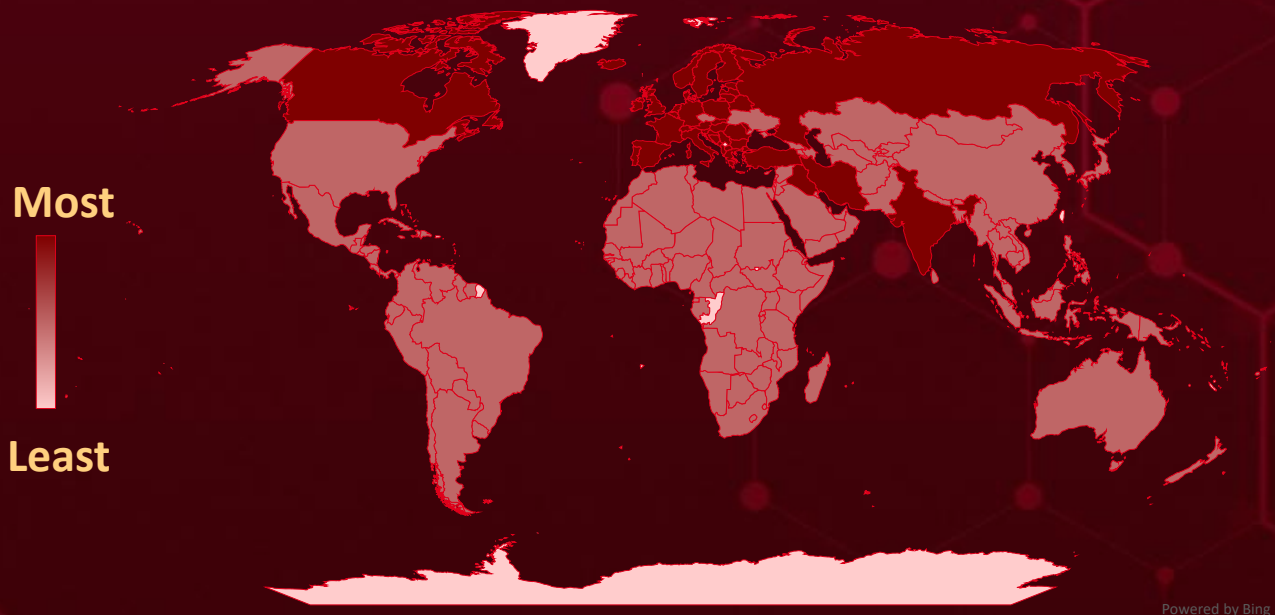
CVE-2025-14847 MongoBleed Vulnerability: When Compression Becomes an Attack Vector

Prince of Persia's Cyber Campaigns: A Mature Espionage Ecosystem

Threat Distribution

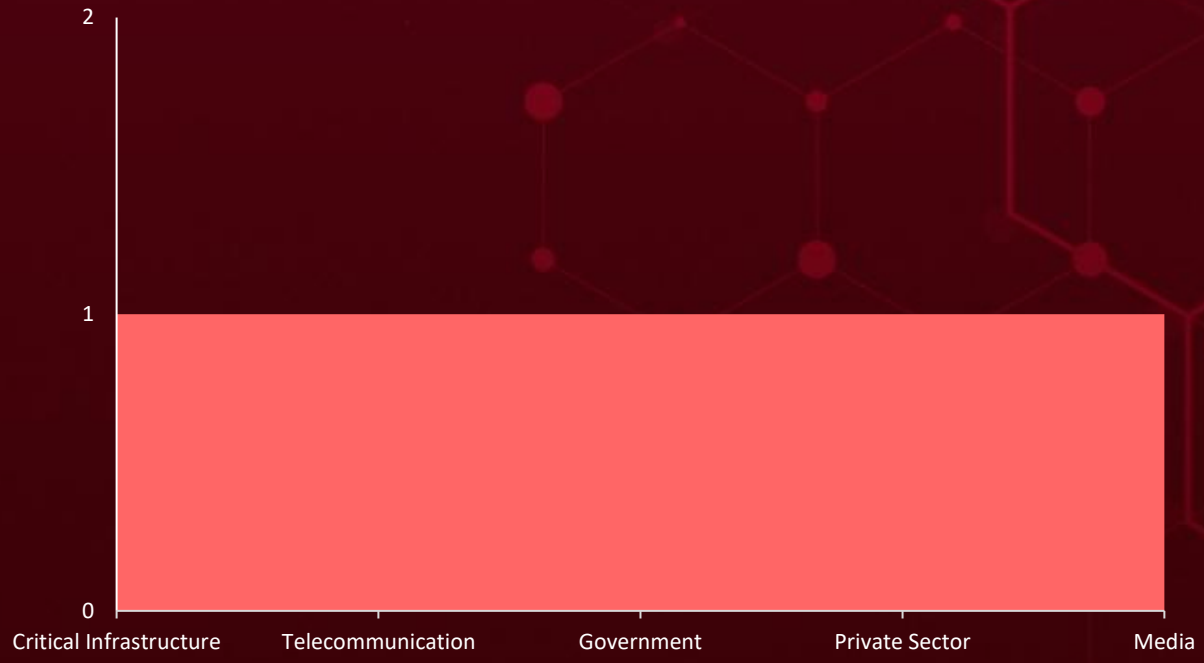


Targeted Countries



Countries	Countries	Countries	Countries
India	Monaco	Ecuador	New Zealand
United Kingdom	France	Saudi Arabia	Barbados
Denmark	Netherlands	Egypt	North Korea
Canada	Germany	State of Palestine	Ghana
Spain	Norway	El Salvador	Pakistan
North Macedonia	Greece	Tuvalu	Angola
Liechtenstein	Portugal	Equatorial Guinea	Paraguay
Slovakia	Hungary	Nepal	Grenada
Albania	Russia	Eritrea	Chile
Moldova	Iceland	Central African Republic	Guatemala
Andorra	Serbia		Rwanda
Romania	Slovenia	Bahamas	Guinea
Austria	Iran	Philippines	Comoros
Switzerland	Sweden	Eswatini	Guinea-Bissau
Belarus	Iraq	Saint Lucia	Congo
Luxembourg	Turkey	Ethiopia	Guyana
Belgium	Ireland	Sierra Leone	Costa Rica
Montenegro	Italy	Fiji	Haiti
Bosnia and Herzegovina	Latvia	South Sudan	South Africa
	Thailand	Bahrain	Holy See
Poland	China	Cyprus	Sri Lanka
Bulgaria	Niger	Bangladesh	Honduras
San Marino	Dominica	Trinidad and Tobago	Suriname
Croatia	Solomon Islands	Gabon	Antigua and Barbuda
Lithuania	Dominican Republic	Azerbaijan	
Estonia	Mozambique	Gambia	Tajikistan
Malta	DR Congo	Namibia	Belize
Finland	Panama	Georgia	Togo

Targeted Industries



TOP MITRE ATT&CK TTPs

T1005 Data from Local System	**T1059** Command and Scripting Interpreter	**T1543** Create or Modify System Process	**T1140** Deobfuscate/ Decode Files or Information	**T1082** System Information Discovery
T1041 Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information	**T1555** Credentials from Password Stores	**T1036** Masquerading	**T1071** Application Layer Protocol
T1588 Obtain Capabilities	**T1555.003** Credentials from Web Browsers	**T1546** Event Triggered Execution	**T1574** Hijack Execution Flow	**T1068** Exploitation for Privilege Escalation
T1553 Subvert Trust Controls	**T1070** Indicator Removal	**T1566** Phishing	**T1070.004** File Deletion	**T1587** Develop Capabilities

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Foudre	Foudre is a downloader and victim profiler that targets high-value systems, delivering a secondary malware implant known as Tonnerre.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Additional payload deployment	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
Prince of Persia			
IOC TYPE	VALUE		
SHA256	43ccc2620229d88d5a6ca2b064da0554ec3c3cc29a097e7a2d97283257cfae69, 0bfc11c6ba57fdaa8b865555d80d8f7d7b1d0f41a23a277885198b3113c945d9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Tonnerre	Tonnerre extracts sensitive data from compromised machines, making it a potent tool for cybercriminals. Additionally, Tonnerre includes a mechanism to contact a Telegram group through the C2 server.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data theft	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
Prince of Persia			
IOC TYPE	VALUE		
SHA256	cb6ed0dd5dbc2e34ae36dd22b9522f7eec94bbfda2dcda7425736656279f8cdf, 30c20ada243b7e476e006dec94876bdeece4f8aca12a4cb6cf962c80f1a6ee3c		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">MacSync</td><td rowspan="6">MaxSync is an advanced macOS information-stealing malware that exploits Apple's code-signing and notarization mechanisms to bypass Gatekeeper protections without requiring user interaction. By leveraging trusted digital signatures, decoy files, and cleaning up execution chains, MaxSync operates stealthily to steal sensitive data while evading detection.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="3">Data theft</td><td>macOS</td></tr>
<tr><td>Stealer</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">06c74829d8eee3c47e17d01c41361d314f12277d899cc9dfa789fe767c03693e, be961ec5b9f4cc501ed5d5b8974b730dabcdf7e279ed4a8c037c67b5b935d51a</td></tr>
</table>

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 PRODUCT	ASSOCIATED ACTORS
CVE-2025-68613	✗	n8n all versions starting with 0.211.0 and prior to 1.120.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:n8n:n8n:*:*:*:*:*:node.js:*:*	-
n8n Remote Code Execution via Expression Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-913	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1565.001: Stored Data Manipulation	https://github.com/n8n-io/n8n/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-14847	MongoBleed	MongoDB 8.2.0 through 8.2.2 MongoDB 8.0.0 through 8.0.16 MongoDB 7.0.0 through 7.0.27 MongoDB 6.0.0 through 6.0.26 MongoDB 5.0.0 through 5.0.31 MongoDB 4.4.0 through 4.4.29 All MongoDB Server v4.2 versions All MongoDB Server v4.0 versions All MongoDB Server v3.6 versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mongodb:mongodb:*:*:*:*:*:*:*:*	-
MongoDB Server Heap Memory Leak Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-130	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials, T1082: System Information Discovery	https://www.mongodb.com/try/download/community, https://jira.mongodb.org/browse/SERVER-115508, https://www.mongodb.com/community/forums/t/important-mongodb-patch-available/332977

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Prince of Persia (alias Infy, Operation Mermaid, APT-C-07)</td><td>Iran</td><td rowspan="3">Critical Infrastructure, Telecommunication, Government, Private Sector, Media</td><td rowspan="3">Iran, Iraq, Turkey, India, Canada, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Vatican City</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Foudre, Tonnerre</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1598: Phishing for Information; T1583: Acquire Infrastructure; T1583.001: Domains; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1543.003: Windows Service; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1574: Hijack Execution Flow; T1574.001: DLL; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1082: System Information Discovery; T1057: Process Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1056: Input Capture; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1102: Web Service; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1048: Exfiltration Over Alternative Protocol; T1485: Data Destruction</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploitable vulnerabilities** and block the indicators related to the threat actor **Prince of Persia,** and malware **Foudre, Tonnerre, MacSync.**

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 **two exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Prince of Persia,** and malware **MacSync** in Breach and Attack Simulation(BAS).

Threat Advisories

Prince of Persia APT Campaigns Across Iran, Europe, and Beyond

Automation Gone Rogue: CVE-2025-68613 Puts n8n Instances at Risk

MacSync A Notarized macOS Malware That Slips Past Gatekeeper

CVE-2025-14847: Critical MongoDB Memory Leak Exposes Sensitive Data

December 2025 Linux Patch Roundup

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
Foudre	SHA256	43ccc2620229d88d5a6ca2b064da0554ec3c3cc29a097e7a2d97283257cfae69, 0bfc11c6ba57fdaa8b865555d80d8f7d7b1d0f41a23a277885198b3113c945d9, cf64bf78ce570f8085110defc8ec32ff4f01c7359723510b9d1923fd93d12240, fbb2ac0d07b84068aa35376cc994039f9fc1d2341643bc2bf268d65ab11ecbe3, 2c46406fb9111e0e4d982de54f335ae2900cdc39490d58f765cd5014153b3e12, 52abb57bf6f9db815b3ddf6241e21d4096f36eb998bb51e728bbe68c0f8e8e15, fa95a09e538b8c186a3239e3ff80ec9054b50aab80c624e75563ace4e60e31da, f54cfe296186644d0fed271c469af1ef9b6156affe9e030e7b83b8de097eb1e7, 6f976a685ae838a7062fb4f152c6c77c42168b78b9aadd4278ec1c19f9bc1055, 12847dc6dfd86603e8f0085ae561b4b2e3089e5414e49628f7c411483c7b5ce8, d3d8b79f86f152338aabeadfaf35ba2e43f82aa4bfa29ff70b59702b455fa6a6, 15dd41ec1bdaabb741e8cc6481e0a98831798ac4e93c2513cdbd00c51241ffb7, 52e3a856548825ec0a3d6630e881ff4f79d2a11bc3420a73d42e161fabed53d9

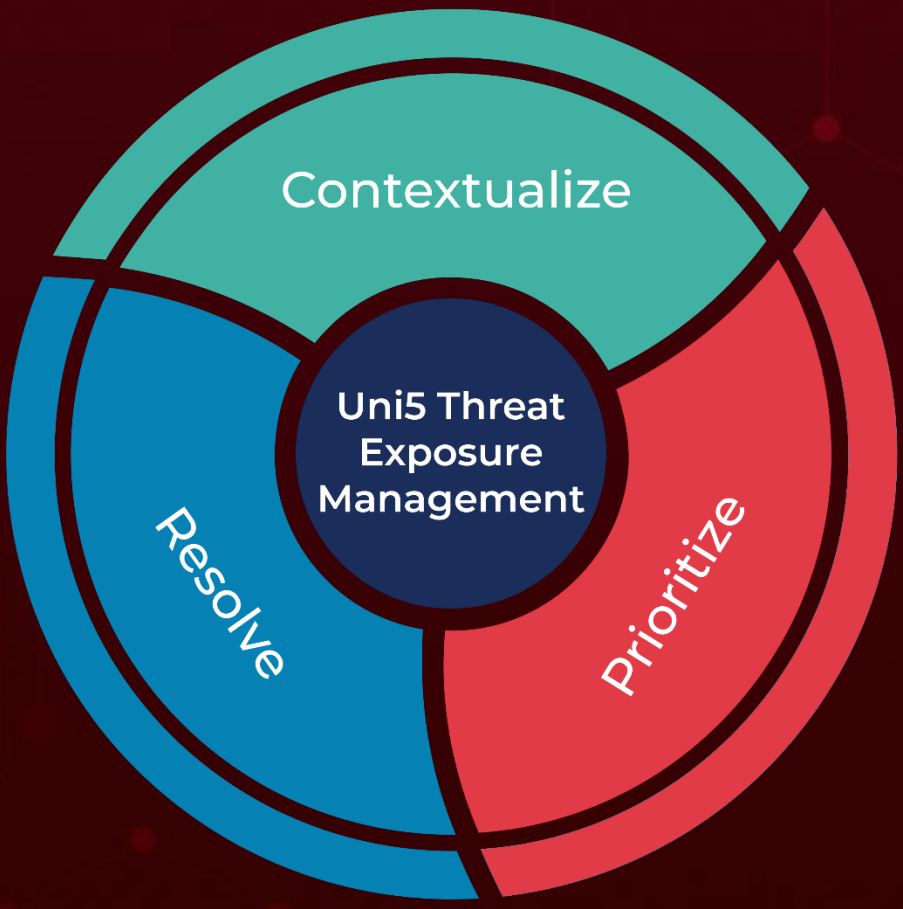
Attack Name	TYPE	VALUE
Tonnerre	SHA256	cb6ed0dd5dbc2e34ae36dd22b9522f7eec94bbfda2dcda7425736656279f8cdf, 30c20ada243b7e476e006dec94876bdeece4f8aca12a4cb6cf962c80f1a6ee3c, d9dfc8a8e3e259a517a91e2e91e3a1d6ef1d5b0886e6729bf897d6ef1b2de722, c8583fddf668808e31f993ff6bcfc6f8ba8b4c2c0c4ea51d4ccc6f5d311b6c90
MacSync	SHA256	06c74829d8eee3c47e17d01c41361d314f12277d899cc9dfa789fe767c03693e, be961ec5b9f4cc501ed5d5b8974b730dabcdf7e279ed4a8c037c67b5b935d51a, ecfaa20f25e11878686249c7094706bc3dcd2dc0ace0f2932a39d1bfdac85863, c4d3e5cdb264eded917cd61b8131c40715c0ee3f4d2c94c84d60fa295ca4ed97, 9990457feac0cd85f450e60c268ddf5789ed4ac81022b0d7c3021d7208ebccd3, 9d43e059111460c4f81351a062fb7eb7dbfd34988a06d756c7206f330c06cb42

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

December 29, 2025 . 9:00 AM

More at www.hivepro.com