Date of Publication
January 5, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 December 2025 to 4 January 2026

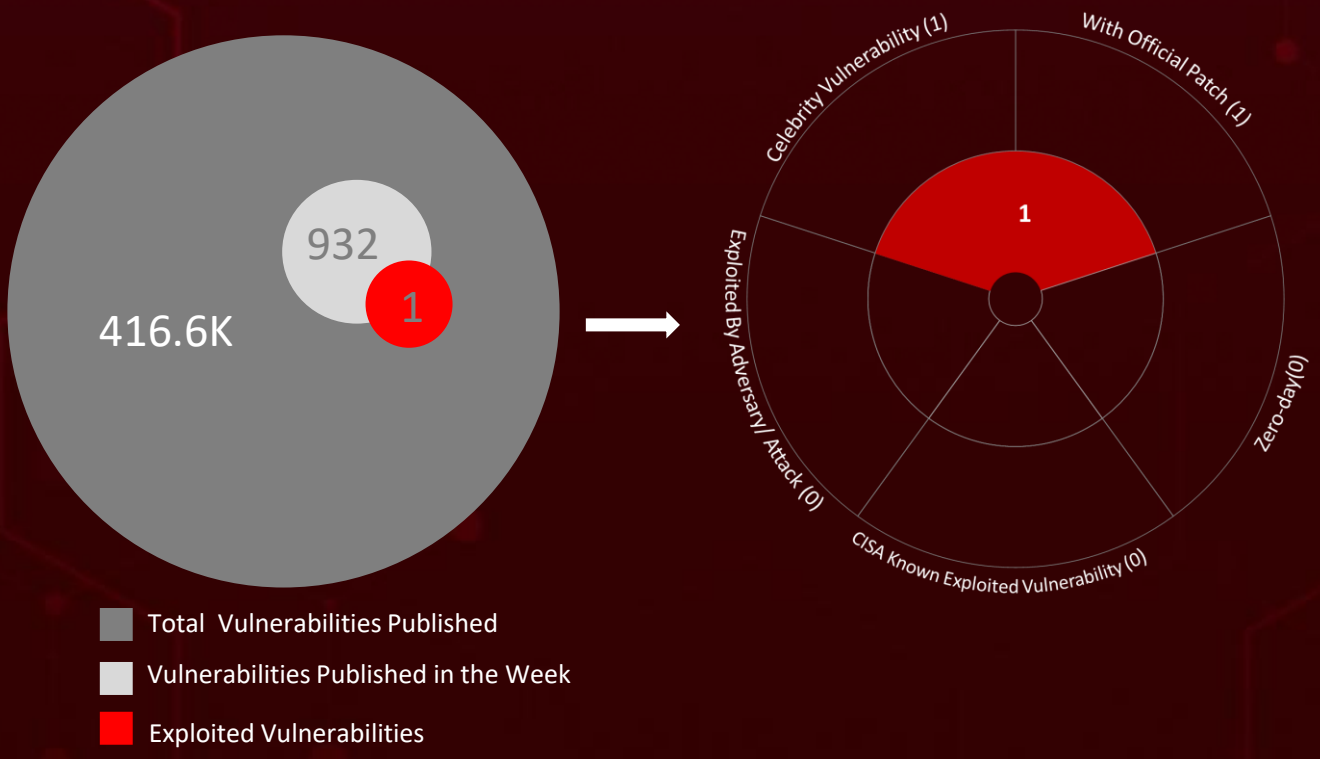
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **four** major attacks were detected, **one** critical celebrity vulnerability was actively exploited, and **two** threat actor were closely monitored, reflecting an alarming escalation in malicious activities.

GlassWorm has emerged as a self-propagating malware campaign abusing VS Code extensions to target developers. It hides malicious code using invisible Unicode characters and primarily affects macOS systems. The malware steals credentials and cryptocurrency wallets, with C2 traffic routed through the Solana blockchain. This campaign underscores growing risks to developer environments.

Meanwhile, China-aligned APT activity remains persistent and adaptive. **Silver Fox** exploited tax-season lures to deploy ValleyRAT via fake Indian tax notices, targeting enterprise and healthcare sectors. **Evasive Panda** sustained a multi-year AitM campaign delivering MgBot through DNS poisoning and fake updates. Additionally, the critical LangGrinch (CVE-2025-68664) flaw in **LangChain** exposes AI applications to data theft and potential RCE. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

4
Attacks Executed

1
Vulnerabilities Exploited

2
Adversaries in Action

- MgBot
- Donut
- Valley RAT
- GlassWorm

- CVE-2025-68664

- Evasive Panda
- Sliver Fox

Insights

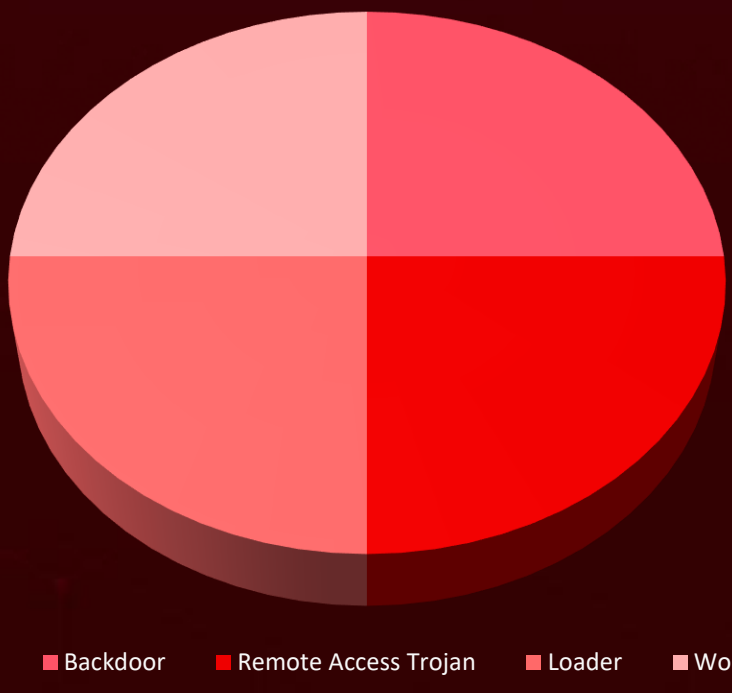
GlassWorm: macOS malware via malicious VS Code extensions with Solana C2.

Silver Fox Tax-themed phishing deploying ValleyRAT against India.

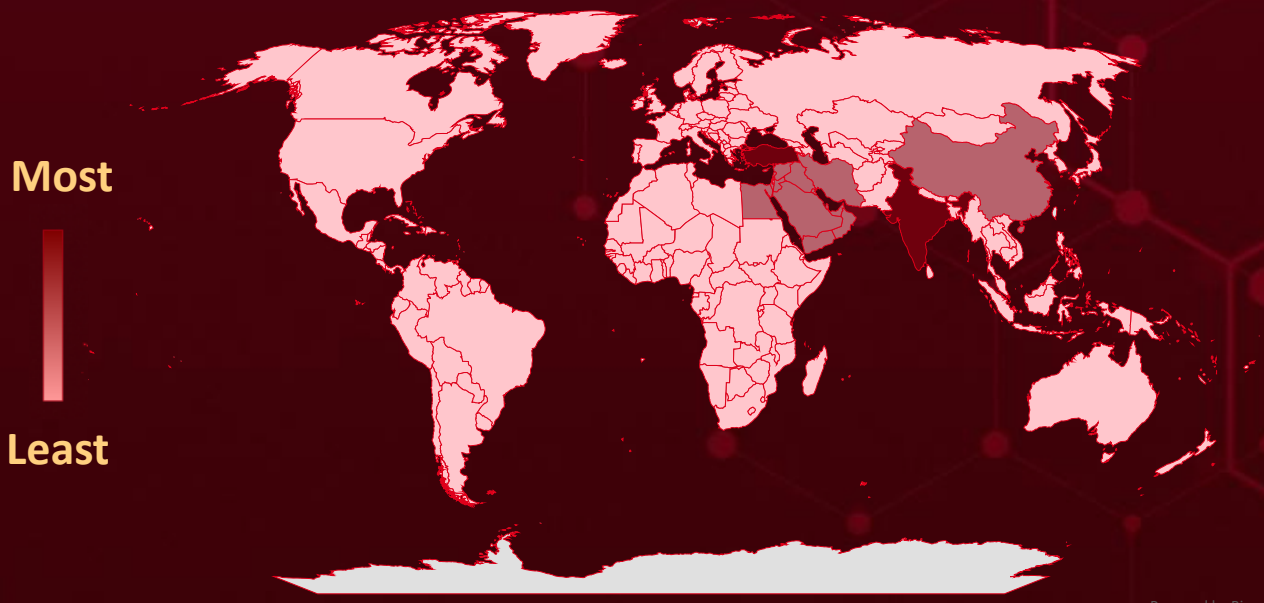
LangGrinch: CVE-2025-68664 (CVSS 9.3) in LangChain affecting 847M+ downloads.

Evasive Panda: 2-year DNS poisoning campaign delivering MgBot.

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
India	Bolivia	Chile	Canada
Turkey	Somalia	Spain	Portugal
Jordan	Bosnia and Herzegovina	Algeria	Central African Republic
Qatar	Maldives	Belarus	Samoa
Yemen	Botswana	Colombia	Chad
Cyprus	Nauru	Tunisia	Singapore
China	Brazil	Comoros	Djibouti
Egypt	Paraguay	United States	Philippines
Kuwait	Brunei	Congo	Dominica
Bahrain	Senegal	Malta	Republic of Congo
Oman	Bulgaria	Costa Rica	Dominican Republic
Iran	Sudan	Mexico	Saint Kitts & Nevis
Saudi Arabia	Burkina Faso	Côte d'Ivoire	DR Congo
Syria	Uganda	Mongolia	Sao Tome & Principe
United Arab Emirates	Burundi	Croatia	Ecuador
Iraq	Mauritania	Myanmar	Seychelles
Israel	Cabo Verde	Cuba	Angola
Lebanon	Morocco	Netherlands	Slovenia
Russia	Cambodia	Andorra	El Salvador
Moldova	Nicaragua	Nigeria	South Korea
Timor-Leste	Cameroon	Czech Republic	Equatorial Guinea
Bhutan	Palau	Albania	
North Macedonia		Denmark	
		Panama	

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1027 Obfuscated Files or Information

T1071.001 Web Protocols

T1071 Application Layer Protocol

T1190 Exploit Public-Facing Application

T1497 Virtualization/ Sandbox Evasion

T1059.001 PowerShell

T1555 Credentials from Password Stores

T1082 System Information Discovery

T1552 Unsecured Credentials

T1588 Obtain Capabilities

T1566 Phishing

T1078 Valid Accounts

T1195 Supply Chain Compromis

T1566.001 Spearphishing Attachment

T1068 Exploitation for Privilege Escalation

T1204.001 Malicious Link

T1027.013 Encrypted/Encoded File

T1041 Exfiltration Over C2 Channel

T1204 User Execution

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">MgBot</td><td rowspan="6">MgBot is a long-standing, modular malware closely tied to the Daggerfly threat group, with observed use dating back to at least 2012. Written in C++, the malware is built around a flexible, plugin-based architecture that allows operators to load and swap capabilities as needed during an intrusion. This design has enabled MgBot to evolve steadily over time, with new modules and enhancements continuing to surface through 2024, underscoring its role as a mature and actively maintained tool.</td><td>-</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="3">System Compromise, Data Theft</td><td rowspan="2">Windows</td></tr>
<tr><td>Backdoor</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Evasive Panda</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">7376FCB7D2BFDCD858CF0920F6B7611E263D779CDC419A246B2D3004CBA2C39F</td></tr>
<tr><td>IPv4</td><td colspan="3">60[.]28[.]124[.]21,
123[.]139[.]57[.]103,
140[.]205[.]220[.]98,
112[.]80[.]248[.]27</td></tr>
</table>

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">Donut</td><td rowspan="6">Donut is an open-source in-memory injector and loader designed for executing VBScript, JScript, EXE, DLL files, and .NET assemblies. As a shellcode generation tool, creates x86 or x64 shellcode payloads from .NET assemblies, which can then be injected into arbitrary Windows processes. This allows attackers to run the injected code directly in memory, bypassing disk-based detection mechanisms. Due to its ability to execute a variety of file formats and deliver payloads stealthily.</td><td>Phishing</td><td>-</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="4">Deploy Malware</td><td>-</td></tr>
<tr><td>TYPE</td><td>PATCH LINK</td></tr>
<tr><td>Loader</td><td rowspan="2">-</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>Silver Fox</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">7cfd50d3099b681c6739bd392700e5bf18a314ab7d554a2f39faf53d445dbce0,
cd1373851bc2dc1ac18743aa988fbefe9d32d0c21a0dbf65e3361cf455b3cc4f,
c971b537adc9851fcdd3ba4ce13693a2615021c478d384d0089603a6a13d69e0,
da23077aa0cd928f82b178ba9ad9e43d684ce40000998051799c28b0439a6c4d,
b37b346737c69ec3b32d468f3fb085a30d26b368b33b9442ca0687cb30c966f3</td></tr>
</table>

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
Valley RAT	Valley RAT is a sophisticated Remote Access Trojan (RAT) discovered in early 2023, primarily linked to the Chinese threat group "Silver Fox." It targets users via phishing emails and fake software installers to gain unauthorized control over systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote control, data theft, system compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Silver Fox			-
IOC TYPE	**VALUE**		
SHA256	068e49e734c2c7be4fb3f01a40bb8beb2d5f4677872fabbced7741245a7ea97c, 1c3501b4689c6072553f84fd7ea04c655a204f9d960825c09745fcbe38a33cdf		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GlassWorm	GlassWorm is a self-propagating supply chain malware discovered in late 2025 that targets Visual Studio Code extensions by injecting "invisible" Unicode characters to hide malicious code from human reviewers. It utilizes the Solana blockchain for an "unkillable" command-and-control (C2) infrastructure, ensuring it remains active even if servers are taken down.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Worm		Credential theft, remote control	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="5">CVE-2025-68664</td><td>  </td><td rowspan="2">Langchain-core versions before: 0.3.81 and 1.2.5</td><td rowspan="2">-</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="3">  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>cpe:2.3:a:langchain-ai:langchain:*:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td rowspan="2">LangGrinch (LangChain Serialization Injection Vulnerability)</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1059.006: Python, T1082: System Information Discovery, T1588.007: Artificial Intelligence</td><td>https://github.com/langchain-ai/langchain/releases</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Evasive Panda (aka Bronze Highland, Daggerfly, Storm Cloud, StormBamboo, TAG-102, TAG-112, Digging Taurus)</td><td>China</td><td rowspan="3">All</td><td rowspan="3">Turkey, China, India</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>MgBot</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059: Command and Scripting Interpreter; T1106: Native API; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1620: Reflective Code Loading; T1055: Process Injection; T1036: Masquerading; T1553: Subvert Trust Controls; T1555: Credentials from Password Stores; T1056: Input Capture; T1557: Adversary-in-the-Middle; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Silver Fox (alias Void Arachne)</td><td>China</td><td rowspan="2">Enterprise, Finance, Medical, Technology</td><td rowspan="2">India</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Donut loader, Valley RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1106: Native API; T1129: Shared Modules; T1620: Reflective Code Loading; T1547: Boot or Logon Autostart Execution; T1112: Modify Registry; T1574: Hijack Execution Flow; T1574.001: DLL; T1218: System Binary Proxy Execution; T1027: Obfuscated Files or Information; T1497: Virtualization/Sandbox Evasion; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1057: Process Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1573: Encrypted Channel; T1008: Fallback Channels; T1041: Exfiltration Over C2 Channel; T1056: Input Capture; T1056.001: Keylogging; T1547.001: Registry Run Keys / Startup Folder; T1489: Service Stop</td></tr>
</table>

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 **Evasive Panda, Sliver Fox** and malware **MgBot, Donut, Valley RAT, GlassWorm.**

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 **Evasive Panda** and malware **Valley RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Inside Evasive Panda’s Long-Running AitM Campaign

LangGrinch: Critical LangChain Serialization Flaws Enable Secret Exfiltration

Silver Fox Slips ValleyRAT Into India Through Fake Tax Notices

GlassWorm's Quiet Infiltration of Mac Systems

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
MgBot	MD5	9e72410d61eaa4f24e0719b34d7cad19
	SHA256	7376FCB7D2BFDCD858CF0920F6B7611E263D779CDC419A246B2D3004CBA2C39F
	IPv4	60[.]28[.]124[.]21, 123[.]139[.]57[.]103, 140[.]205[.]220[.]98, 112[.]80[.]248[.]27, 116[.]213[.]178[.]11, 60[.]29[.]226[.]181, 58[.]68[.]255[.]45, 61[.]135[.]185[.]29, 103[.]27[.]110[.]232, 117[.]121[.]133[.]33, 139[.]84[.]170[.]230
Donut	SHA256	7cfd50d3099b681c6739bd392700e5bf18a314ab7d554a2f39faf53d445dbce0, cd1373851bc2dc1ac18743aa988fbefe9d32d0c21a0dbf65e3361cf455b3cc4f, c971b537adc9851fcdd3ba4ce13693a2615021c478d384d0089603a6a13d69e0, da23077aa0cd928f82b178ba9ad9e43d684ce40000998051799c28b0439a6c4d, b37b346737c69ec3b32d468f3fb085a30d26b368b33b9442ca0687cb30c966f3

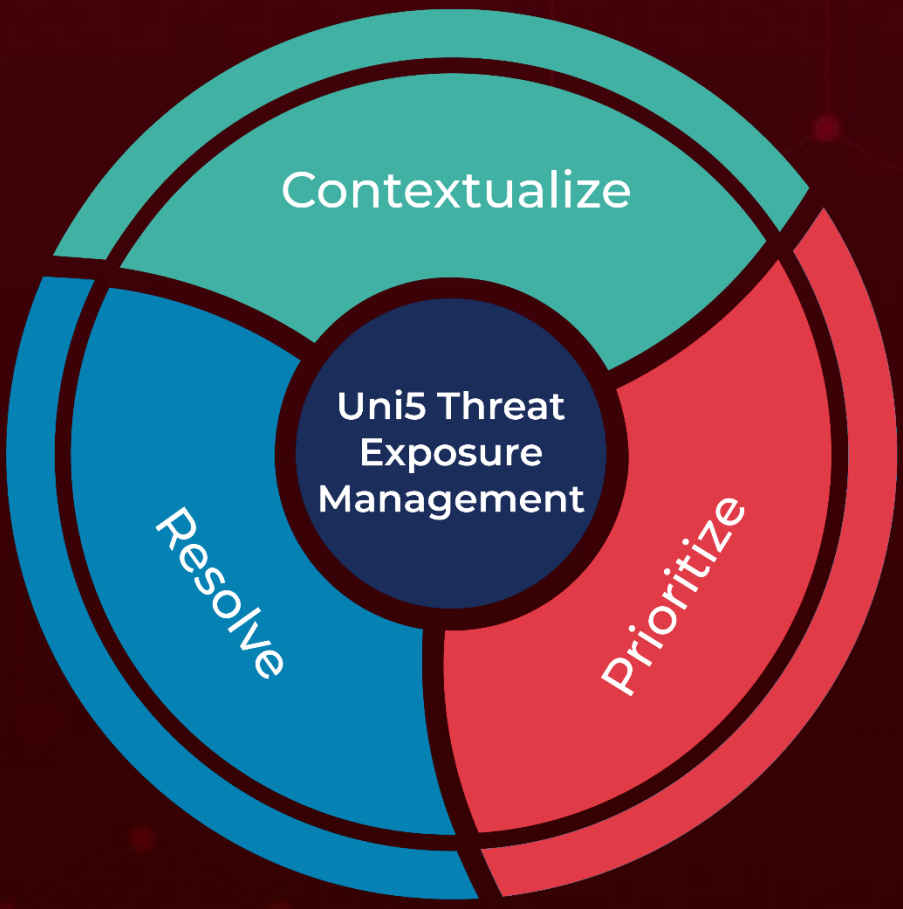
Attack Name	TYPE	VALUE
Valley RAT	SHA256	068e49e734c2c7be4fb3f01a40bb8beb2d5f4677872fabbced7741245a7ea97c, 1c3501b4689c6072553f84fd7ea04c655a204f9d960825c09745fcbe38a33cdf

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

January 5, 2026 . 8:30 AM

More at www.hivepro.com