Date of Publication
June 24, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

16 to 22 JUNE 2025

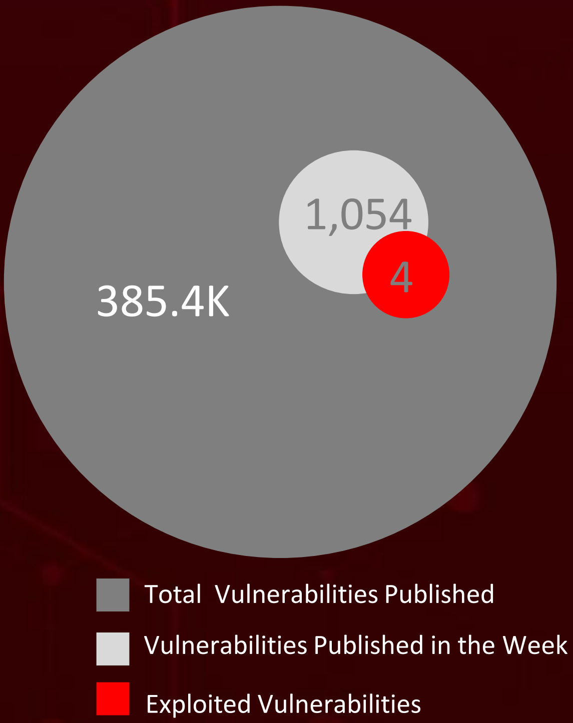
Table Of Contents

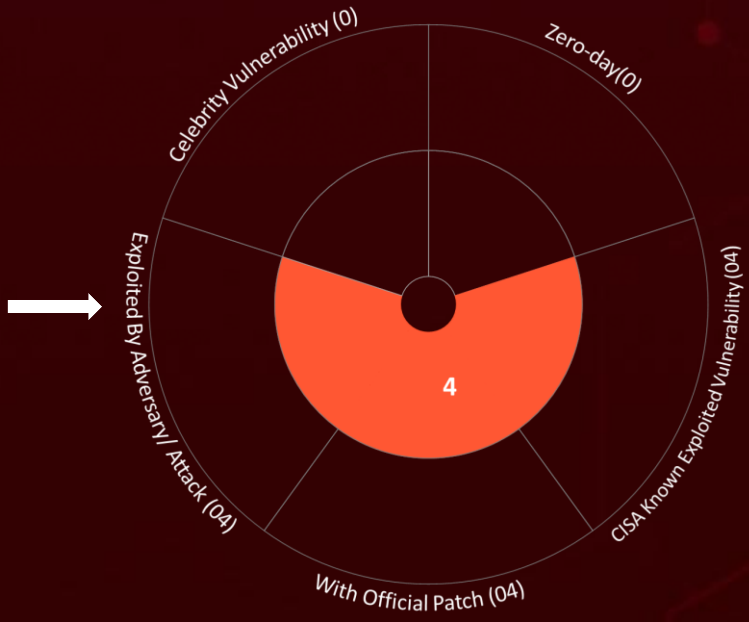
Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **eleven** attacks, reported **four** vulnerabilities, and identified **three** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Gunra ransomware, written in C/C++ and based on leaked Conti code, emerged in April 2025. It has since compromised 13 high-profile organizations using aggressive double-extortion tactics. **CVE-2025-3248** is a critical RCE flaw in Langflow due to unsafe use of Python's exec(), allowing unauthenticated code execution. It's actively exploited, including by the Flodrix botnet, targeting exposed instances.

Additionally, **PylangGhost**, a Python-based RAT used by the North Korea-linked group **Famous Chollima,** targets crypto job seekers. The campaign blends social engineering with technical skill to infiltrate the high-value crypto sector. **Katz Stealer**, a new malware-as-a-service, enables easy credential theft via phishing and fake software. It hides in images, abuses trusted tools, and steals data from browsers, crypto wallets, and apps like Discord. These rising threats pose significant and immediate dangers to users worldwide.





High Level Statistics

11
Attacks Executed

4
Vulnerabilities Exploited

3
Adversaries in Action

- Anubis
- Sakura RAT
- DULLRAT
- HoldingHands RAT
- Flodrix
- Gunra Ransomware
- PylangGhost
- DragonForce Ransomware
- AsyncRAT
- RevengeRAT
- Katz Stealer

- CVE-2025-3248
- CVE-2015-2291
- CVE-2021-35464
- CVE-2024-37085

- Water Curse
- Famous Chollima
- Scattered Spider

Insights

Anubis is a RaaS ransomware that emerged in Dec 2024, offering encryption and optional wiper mode, targeting sectors like healthcare and engineering.

Scattered Spider pivoted in June 2025 from UK retail to targeting US insurance firms, leveraging AI-driven phishing, ransomware, and advanced toolkits.

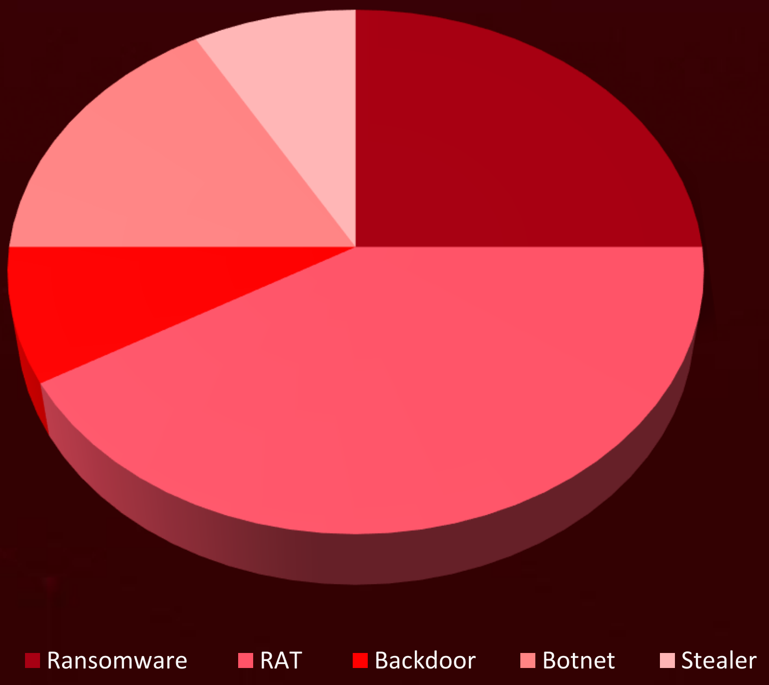
Katz Stealer is a new stealthy MaaS malware that steals credentials and crypto via phishing, hidden code, and abused system tools.

SERPENTINE#CLOUD is a stealthy campaign using Cloudflare Tunnel and multi-stage scripts to deliver fileless RATs like AsyncRAT via phishing and memory injection.

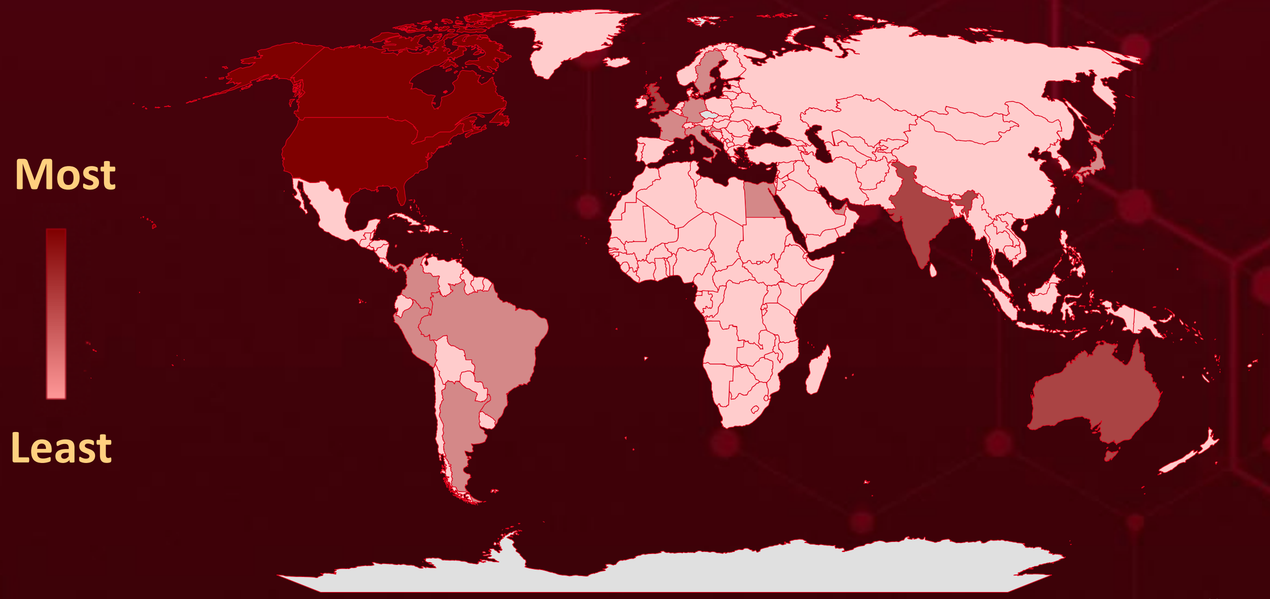
CVE-2025-3248 is a critical RCE vulnerability in Langflow <1.3.0 that allows unauthenticated code execution via unsafe use of exec(), with active Flodrix botnet attacks exploiting exposed instances.

Water Curse is a financially driven threat group abusing GitHub to deliver multi-stage malware via fake developer tools, targeting developers, security pros, & crypto users.

Threat Distribution



Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

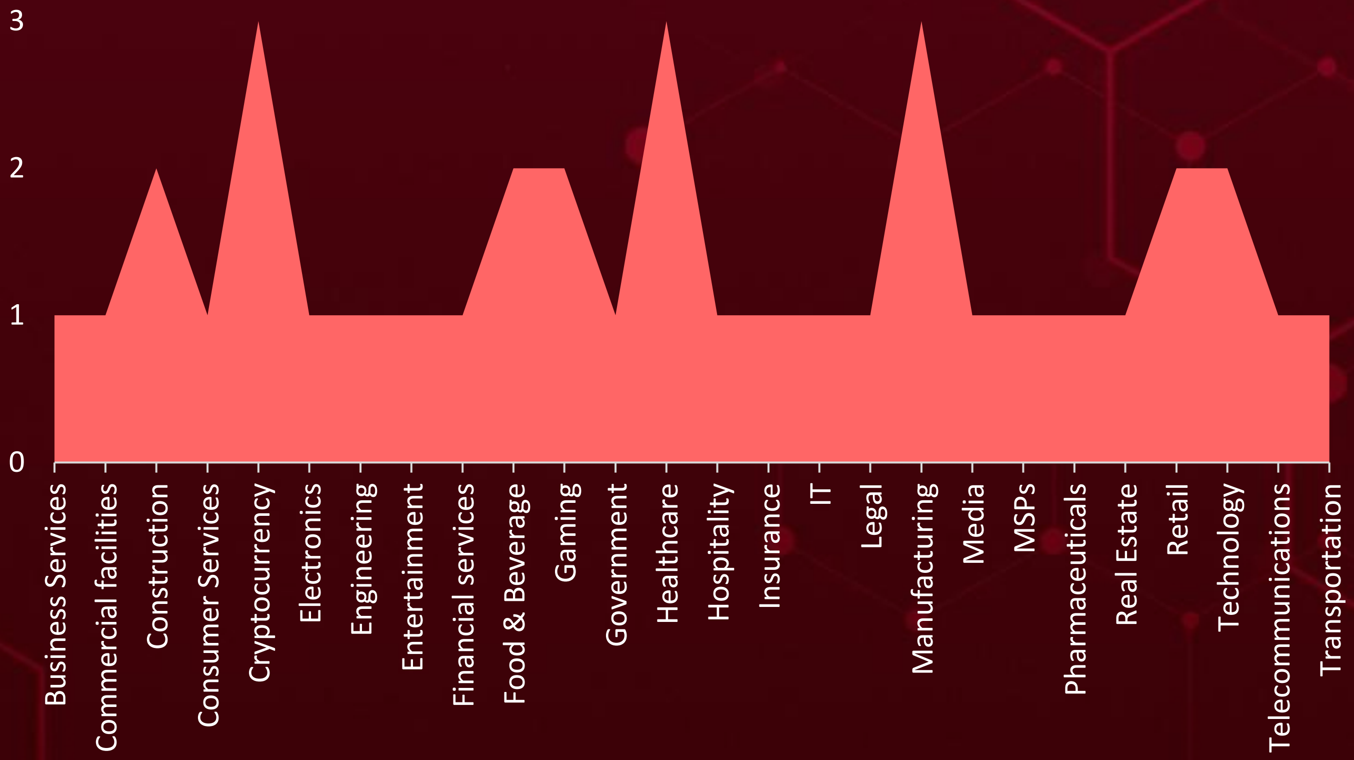
Countries
Canada
United States
Australia
India
United Kingdom
Germany
Peru
Japan
Argentina
Sweden
Brazil
Italy
Colombia
Panama
Croatia
Singapore
Egypt
France
United Arab Emirates
Saint Kitts & Nevis
Monaco
Tonga
Bolivia
Norway
Sao Tome & Principe

Countries
Bosnia and Herzegovina
South Korea
Botswana
Mali
Armenia
Nepal
Brunei
Philippines
Bulgaria
Seychelles
Burkina Faso
Benin
Burundi
Madagascar
Cabo Verde
Mauritius
Cambodia
Mozambique
Cameroon
Niger
Albania
Belarus
Central African Republic
Republic of Congo
Chad

Countries
Chile
Slovenia
China
St. Vincent & Grenadines
Andorra
Tanzania
Comoros
Turkmenistan
Congo
Malaysia
Costa Rica
Marshall Islands
Côte d'Ivoire
Micronesia
Austria
Montenegro
Cuba
Namibia
Cyprus
New Zealand
Czech Republic (Czechia)
North Korea
Denmark
Pakistan
Djibouti

Countries
Dominica
Portugal
Dominican Republic
Russia
DR Congo
Samoa
Ecuador
Senegal
Azerbaijan
Belize
El Salvador
Somalia
Equatorial Guinea
Spain
Eritrea
Sudan
Estonia
Syria
Eswatini
Timor-Leste
Ethiopia
Tunisia
Fiji
Luxembourg
Finland
Malawi
Bahamas

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1190
Exploit Public-Facing Application

T1566
Phishing

T1078
Valid Accounts

T1068
Exploitation for Privilege Escalation

T1588
Obtain Capabilities

T1588.005
Exploits

T1588.006
Vulnerabilities

T1203
Exploitation for Client Execution

T1204
User Execution

T1027
Obfuscated Files or Information

T1204.002
Malicious File

T1036
Masquerading

T1133
External Remote Services

T1566.001
Spearphishing Attachment

T1140
Deobfuscate/ Decode Files or Information

T1547
Boot or Logon Autostart Execution

T1105
Ingress Tool Transfer

T1041
Exfiltration Over C2 Channel

T1204.001
Malicious Link

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Anubis</td><td rowspan="5">Anubis is a destructive ransomware threat that emerged in December 2024, offering both file encryption and an optional wiper mode that renders data unrecoverable. Distributed via phishing, stolen credentials, and access brokers, it operates under a ransomware-as-a-service (RaaS) model.</td><td>Phishing</td><td>-</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Ransomware</td><td rowspan="3">Data theft and Data exfiltration</td><td>Windows, Linux, NAS, and ESXi (VMware) environments</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
</table>

IOC TYPE	VALUE
SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed

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
Sakura RAT	Sakura RAT is a lightweight remote access trojan used by the Water Curse group to maintain control over compromised systems. It supports basic functions like system reconnaissance, command execution, and credential theft. Often deployed in later stages, it acts as a modular payload for long-term access and data harvesting.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote control, Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Water Curse			-

IOC TYPE	VALUE
SHA1	5cd53d94caf0e811b82bad958b34322eb082567f

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DULLRAT	DULLRAT is a lightweight, JavaScript-based backdoor used in the Water Curse campaign, often embedded within malicious Electron applications. It enables remote access, command execution, and data theft, acting as part of a modular multi-stage infection chain.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System control, Data theft and Unauthorized access	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Water Curse			-

IOC TYPE	VALUE
SHA1	60bdf425bd22c34bad7d5663db31d2107153f729, 68911ad6696cfdb15c967a82c2d8aab1be634659, d94f476b2aceaf4e83197475280f89ecbe3b8d35
SHA256	af6e99f86899fe12907850ba365d75b57238300869795d5f998b7b2f57f11837

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
HoldingHands RAT	HoldingHands RAT, also known as Gh0stBins, is a variant of the notorious Gh0st RAT, commonly used by Chinese state-sponsored threat actors. It's delivered via sophisticated phishing campaigns, often mimicking official communications like tax or invoice lures. Once active, it establishes command-and-control, allowing attackers to collect user data, manage files, and conduct remote desktop operations on compromised systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
RAT		Remote control, Data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	50fbd7e4cfa193f009d80913efd1cd2b04a9007db2fb97d5b26c9786216db124, a19fdfc131e8fbe063289c83a3cdefb9fb9fb6f1f92c83b892d3519a381623db		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Gunra Ransomware	Gunra ransomware, a malware strain written in C/C++, is quickly making headlines for its aggressive double-extortion tactics. Built on the leaked Conti ransomware source code, it has compromised approximately 13 high-profile organizations worldwide since its emergence in April 2025.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd		
SHA1	77b294117cb818df701f03dc8be39ed9a361a038		
MD5	9a7c0adedc4c68760e49274700218507		

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
Flodrix	Flodrix is a botnet actively exploiting a critical vulnerability in Langflow, a framework for building AI applications. Once a system is compromised, Flodrix turns it into part of a botnet capable of launching high-volume Distributed Denial of Service (DDoS) attacks. It can also achieve full system compromise and potentially exfiltrate sensitive data, employing stealth techniques like self-deletion to evade detection.	Exploiting vulnerability	CVE-2025-3248
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Botnet		Network Overload, Compromise systems	Langflow
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	EC0F2960164CDCF265ED78E66476459337C03ACB469B6B302E1E8AE01C35D7EC, 52A034E732BCE0CB10FBFAE6F3C208FFB885D490FBCD70BAD62FB2E32A7C33F8, E4AEA6EE7005EE4B500E0B8673B69EA91D1A7532FACAD653E575BA29824845D9, 7BDBF2766AD55F9A67BFBB97A32D308530E4B5959BB68A9ACB22326DFEE8F282, E08E03091DEFB5006792934389AA350E8C48C37E59E282EF8FE3C3F126212E20

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an open-source Remote Access Trojan (RAT) commonly used by cybercriminals since 2019. It provides attackers with full remote control over compromised Windows systems, enabling actions like data theft (keylogging, screen recording, password recovery), file manipulation, and further payload execution.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Data theft, System control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a

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
RevengeRAT	RevengeRAT is a versatile Remote Access Trojan, often distributed via spear-phishing emails containing malicious attachments or links. It's known for its .NET origins and has been leveraged by various threat groups, including state-sponsored actors, in campaigns targeting diverse sectors.	Spear-phishing	CVE-2025-3248
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Data theft, Full system control	Langflow
ASSOCIATE D ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	7a8c864ed8b7ca908d3f317d7e63a30a85fb3e8c94070f23f2cf0bfa01c5e0b5, 837f60772b83b9aed7304d8e56f4aa8a49f7b79122e6d394447e9225105d6b6d, a30fa780cca1e7ab27f5802c749737ead187b8139e39cb736237087da1660024, 382593c547f7b0f4f9bebe0039ff7194ad8bf5969aae5f7d8267d48ece91bc96

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Katz Stealer	Katz Stealer is a newly discovered, sophisticated information-stealing malware-as-a-service (MaaS) that emerged in 2025. It targets a vast array of sensitive data including browser credentials, crypto wallets, and system information, employing stealthy evasion techniques like UAC bypass and in-memory execution.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Stealer		Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	6dc8e99da68b703e86fa90a8794add87614f254f804a8d5d65927e0676107a9d, e73f6e1f6c28469e14a88a633aef1bc502d2dbb1d4d2dfcaaef7409b8ce6dc99, 2798bf4fd8e2bc591f656fa107bd871451574d543882ddec3020417964d2faa9, e345d793477abbecc2c455c8c76a925c0dfe99ec4c65b7c353e8a8c8b14da2b6, c601721933d11254ae329b05882337db1069f81e4d04cd4550c4b4b4fe35f9cd,

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>PylangGhost</td><td rowspan="5">PylangGhost is a Python-based Remote Access Trojan (RAT) identified in May 2025, primarily targeting cryptocurrency and blockchain professionals in India. Linked to the North Korean threat group Famous Chollima, it's delivered via fake job offers on spoofed job sites, tricking victims into executing malicious commands to install fake video drivers.</td><td>Phishing through fake job offers</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td>RAT</td><td rowspan="3">Remote control, Data exfiltration</td><td>Windows</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Famous Chollima</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">267009d555f59e9bf5d82be8a046427f04a16d15c63d9c7ecca749b11d8c8fc3</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
DragonForce	DragonForce ransomware is a financially motivated extortion tool designed to encrypt victims' files and demand payment for their recovery. Once a system is compromised, the ransomware appends encrypted files with extensions such as .dragonforce_encrypted or .cyberbears, signaling successful infection. Victims receive a ransom note stating that their data has been both stolen and encrypted, with attackers emphasizing their monetary intent rather than any political agenda. The note directs victims to contact the group via a Tor website or TOX ID, where they are offered a list of exfiltrated files and a free decryption of one file as proof of the attackers' capabilities.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Scattered Spider			-

IOC TYPE	VALUE
SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9

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
CVE-2025-3248	✗	Langflow versions prior to 1.3.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:langflow-ai:langflow:*:*:*:*:*:*:*:*	Flodrix
Langflow Missing Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006: Python	https://github.com/langflowai/langflow/releases/tag/1.3.0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-2291	✗	IQVW32.sys before 1.3.1.0 and IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows	Scattered Spider
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw32.sys:1.03.0.7:*:*:*:*:*:*:* cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw64.sys:1.03.0.7:*:*:*:*:*:*:*	-
Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1068: Exploitation for Privilege Escalation; T1499: Endpoint Denial of Service	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2021-35464</td><td>✗</td><td rowspan="2">ForgeRock AM server before 7.0</td><td rowspan="2">Scattered Spider</td></tr>
<tr><th>ZERO-DAY</th></tr>
<tr><td>✗</td><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:a:forgerock:access_management:*:*:*:*:*:*:*:*
cpe:2.3:a:forgerock:openam:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability</td><td>✓</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application; T1505.003: Server Software Component: Web Shell</td><td>https://backstage.forgerock.com/knowledge/advisories/article/a47894244</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37085	✗	VMware ESXi VMware vCenter Server VMware Cloud Foundation	Scattered Spider
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:internet_explorer:*:*:*:*:*:*:*:*	-
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Water Curse	-	Cryptocurrency, Gaming, Information Technology	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Sakura RAT, DULLRAT	Windows

TTPs
TA0006: Credential Access; TA0010: Exfiltration; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; T1053.005: Scheduled Task; T1119: Automated Collection; T1560: Archive Collected Data; T1102.002: Bidirectional Communication; T1102: Web Service; T1557: Adversary-in-the-Middle; T1497: Virtualization/Sandbox Evasion; T1113: Screen Capture; T1555: Credentials from Password Stores; T1082: System Information Discovery; T1497.001: System Checks; T1213: Data from Information Repositories; T1555.003 Credentials from Web Browsers; T1005: Data from Local System; T1543: Create or Modify System Process; T1036 Masquerading; T1218: System Binary Proxy Execution; T1048: Exfiltration Over Alternative Protocol; T1548 Abuse Elevation Control Mechanism; T1112: Modify Registry; T1027: Obfuscated Files or Information; T1057: Process Discovery:; T1548.002: Bypass User Account Control; T1562.001: Disable or Modify Tools; T1562.004 Disable or Modify System Firewall; T1562: Impair Defenses; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1129: Shared Modules; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Famous Chollima (aka Wagemole, Contagious Interview, Nickel Tapestry, Storm-1877, UNC5267, Void Dokkaebi, PurpleBravo, TenaciousPungsan, WaterPlum, BadClone)	North Korea	Cryptocurrency	India
	MOTIVE		
	Financial gain, Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PylangGhost	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.003: Spearphishing via Service; T1189: Drive-by Compromise; T1059: Command and Scripting Interpreter; T1059.006: Python; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1083: File and Directory Discovery; T1012: Query Registry; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027: Obfuscated Files or Information; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1560.001: Archive via Utility; T1560: Archive Collected Data; T1543: Create or Modify System Process; T1656: Impersonation; T1041: Exfiltration Over C2 Channel			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)</td><td>Suspected UK and US</td><td rowspan="3">Commercial facilities, Telecommunications, Technology, Business-Process Outsourcing (BPO), Financial services, Hospitality, Media and entertainment, Healthcare, Retail, Insurance, Managed Service Providers (MSPs), Manufacturing, Cryptocurrency, and Food services</td><td rowspan="3">United States, Canada, United Kingdom, Singapore, India, France, Sweden, and Australia</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Financial gain</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>CVE-2015-2291
CVE-2021-35464
CVE-2024-37085</td><td>DragonForce Ransomware</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1585.001: Social Media Accounts; T1585: Establish Accounts; T1566: Phishing; T1660: Phishing; T1566.004: Spearphishing Voice; T1199: Trusted Relationship; T1078.002: Domain Accounts; T1078: Valid Accounts; T1648: Serverless Execution; T1204: User Execution; T1136: Create Account; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1484.002: Domain Trust Modification; T1484: Domain Policy Modification; T1578.002: Create Cloud Instance; T1578: Modify Cloud Compute Infrastructure; T1656: Impersonation; T1606: Forge Web Credentials; T1621: Multi-Factor Authentication Request Generation; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552: Unsecured Credentials; T1217: Browser Bookmark Discovery; T1538: Cloud Service Dashboard; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1539: Steal Web Session Cookie; T1021: Remote Services; T1021.007: Cloud Services; T1213.003: Code Repositories; T1213.002: Sharepoint; T1213: Data from Information Repositories; T1074: Data Staged; T1114:Email Collection; T1530: Data from Cloud Storage; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1567.002: Exfiltration to Cloud Storage; T1526: Cloud Service Discovery; T1218: System Binary Proxy Execution; T1562: Impair Defenses ; T1568: Dynamic Resolution; T1003: OS Credential Dumping; T1036: Masquerading; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **Water Curse, Famous Chollima, Scattered Spider,** and malware **Anubis, Sakura, DULLRAT, HoldingHands RAT, Flodrix, Gunra, PylangGhost, DragonForce Ransomware, AsyncRAT, RevengeRAT, Katz Stealer.**

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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Water Curse, Famous Chollima, Scattered Spider,** and malware **Anubis, DULLRAT, HoldingHands RAT, Gunra, PylangGhost, DragonForce Ransomware, Katz Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

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
Anubis	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
Sakura RAT	SHA1	5cd53d94caf0e811b82bad958b34322eb082567f
DULLRAT	SHA1	60bdf425bd22c34bad7d5663db31d2107153f729, 68911ad6696cfdb15c967a82c2d8aab1be634659, d94f476b2aceaf4e83197475280f89ecbe3b8d35
	SHA256	af6e99f86899fe12907850ba365d75b57238300869795d5f998b7b2f57f11837
HoldingHands RAT	SHA256	50fbd7e4cfa193f009d80913efd1cd2b04a9007db2fb97d5b26c9786216db124, a19fdfc131e8fbe063289c83a3cdefb9fb9fb6f1f92c83b892d3519a381623db
AsyncRAT	SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a

Attack Name	TYPE	VALUE
Flodrix	SHA256	EC0F2960164CDCF265ED78E66476459337C03ACB469B6B302E1E8AE01C35D7EC, 52A034E732BCE0CB10FBFAE6F3C208FFB885D490FBCD70BAD62FB2E32A7C33F8, E4AEA6EE7005EE4B500E0B8673B69EA91D1A7532FACAD653E575BA29824845D9, 7BDBF2766AD55F9A67BFBB97A32D308530E4B5959BB68A9ACB22326DFEE8F282, E08E03091DEFB5006792934389AA350E8C48C37E59E282EF8FE3C3F126212E20, 57CEDC81378F98E568539CC653349FF70EF851A6D51886FD2560F30DF5E31BBD, C97128A452FF24D9BA70A3A7674C1D7AD21BABC9C75E7C34330BADDAEEA3D4BD, 80C956C5F279A436E7CF81B3E47333144DA5EF39BD76BD8C4A65E4571125EA7A, DC9A484F4910EE08EB22AFAB8D328EEF5328C9A5A8ABC6A50062E2065262A81F, 4AA59DDE4C8DA2CFF1A3AFE02DB3AE6C00D99E698DB11838B791E1D6C582FFB6, 912573354E6ED5D744F490847B66CB63654D037EF595C147FC5A4369FEF3BFEE, 09EFD15FF0317424B9B964626DA5E42D68B3CE91F509B16DAD9892D156D3EABE, 1E5E9723C6B492C477471CCCB4D7B26AAE653B0C5491C29739F784C664699D36, AB0F9774CA88994091DB0AE328D98F45034F653BD34E4F5E85679A972D3A039C, C2BCDD6E3CC82C4C4DB6AAF8018B8484407A3E3FCE8F60828D2087B2568ECCA4, A6CF8124E9B4558AACC7DDFA24B440454B904B937929BE203ED088B1040D1B36, EC52F75268B2F04B84A85E08D56581316BD5CCFEB977E002EB43270FE713F307, CCB02DCE1BCA9C3869E1E1D1774764E82206026378D1250AED324F1B7F9B1F11, 9991C664C052EC407E53439AC6BB4DF3CBBE3E54AF243D007A39D8A3DAB935B9, F73B554E6AA7095CFC79CDB687204D99533AEDA73309106BA6CC9428FF57BD1E, EE84591092A971C965B4E88CC5D6E8C2F07773B3BEE1486F3A52483EE72A2B3B, 002F3B2C632E0BE6CBC3FDF8AFCD0432FFE36604BA1BA84923CADAA147418187,

Attack Name	TYPE	VALUE
Flodrix	SHA256	99B59E53010D58F47D332B683EB8A40DF0E0EACEF86390BCA249A708E47D9BAD, 78B430BFF7D797B020D06702659E26D8CA01C8FC968239390697AEFF472623A7, D8D5A32BBD747C92FA1BB55DCE4ABB20E8D09711AEBCBFE8E7EEC83173F9E627, 08CF20E54C634F21D8708573EEF7FDE4DBD5D3CD270D2CB8790E3FE1F42ECCEC, 6DD0464DD0ECDE4BB5A769C802D11AB4B36BBE0DD4F0F44144121762737A6BE0, C462A09DB1A74DC3D8ED199EDCA97DE87B6ED25C2273C4A3AFE811ED0C1C8B1D, C2DCEB14EB91802CD4F78E78634E7837F4B2F4D1329D3F5293C53798B4D0C30E, 9850EB26D8CBEF3358DA4DF154E054759A062116C2AA82DE9A69A8589F0DCE49, A42F8428AA75C180C2F89FBB8B1E44307C2390ED0EBF5AF10015131B5494F9E1, E1C830643DE2EC7BC7C032F7EC96C302CE54E703EAF576D3796D1BBD05D8A63F, 51085CD2DE0ED6A9A6738AC85A8CAF297FBD22DB4B049822A9802BB8140DCD3D, 64927195D388BF6A1042C4D689BCB2C218320E2FA93A2DCC065571ADE3BB3BD3, ABB0C4AD31F013DF5037593574BE3207A4C1E066A96E58CE243AAF2EF0FC0E4D, 47497B24AF6FF42DAE582998AEEEDBC7B9CA6B3E0D82E8E49E8AC4A0F453A659, DF9E9006A566A4FE30EAA48459EC236D90FD628F7587DA9E4A6A76D14F0E9C98
	MD5	Eaf854b9d232566e82a805e9be8b2bf2, 176f293dd15b9cf87ff1b8ba70d98bcf, 82d8bc51a89118e599189b759572459f
	SHA1	E367cee9e02690509b4acdf7060f1a4387d85ec7, 7823b91efceedaf0e81856c735f13ae45b494909, d703ec4c4d11c7a7fc2fcf4a4b8776862a3000b5

Attack Name	TYPE	VALUE
Katz Stealer	Domain	katz-stealer[.]com, katzstealer[.]com
	SHA256	6dc8e99da68b703e86fa90a8794add87614f254f804a8d5d65927e0676107a9d, e73f6e1f6c28469e14a88a633aef1bc502d2dbb1d4d2dfcaaef7409b8ce6dc99, 2798bf4fd8e2bc591f656fa107bd871451574d543882ddec3020417964d2faa9, e345d793477abbecc2c455c8c76a925c0dfe99ec4c65b7c353e8a8c8b14da2b6, c601721933d11254ae329b05882337db1069f81e4d04cd4550c4b4b4fe35f9cd, fdc86a5b3d7df37a72c3272836f743747c47bfbc538f05af9ecf78547fa2e789, 25b1ec4d62c67bd51b43de181e0f7d1bda389345b8c290e35f93ccb444a2cf7a, 964ec70fc2fdf23f928f78c8af63ce50aff058b05787e43c034e04ea6cbe30ef, d92bb6e47cb0a0bdbb51403528ccfe643a9329476af53b5a729f04a4d2139647, b249814a74dff9316dc29b670e1d8ed80eb941b507e206ca0dfdc4ff033b1c1f, 925e6375deaa38d978e00a73f9353a9d0df81f023ab85cf9a1dc046e403830a8, 96ada593d54949707437fa39628960b1c5d142a5b1cb371339acc8f86dbc7678, b912f06cf65233b9767953ccf4e60a1a7c262ae54506b311c65f411db6f70128, 2852770f459c0c6a0ecfc450b29201bd348a55fb3a7a5ecdcc9986127fdb786b, 5dd629b610aee4ed7777e81fc5135d20f59e43b5d9cc55cdad291fcf4b9d20eb
RevengeRAT	SHA256	7a8c864ed8b7ca908d3f317d7e63a30a85fb3e8c94070f23f2cf0bfa01c5e0b5, 837f60772b83b9aed7304d8e56f4aa8a49f7b79122e6d394447e9225105d6b6d, a30fa780cca1e7ab27f5802c749737ead187b8139e39cb736237087da1660024, 382593c547f7b0f4f9bebe0039ff7194ad8bf5969aae5f7d8267d48ece91bc96
	IPv4	104[.]26[.]3[.]158

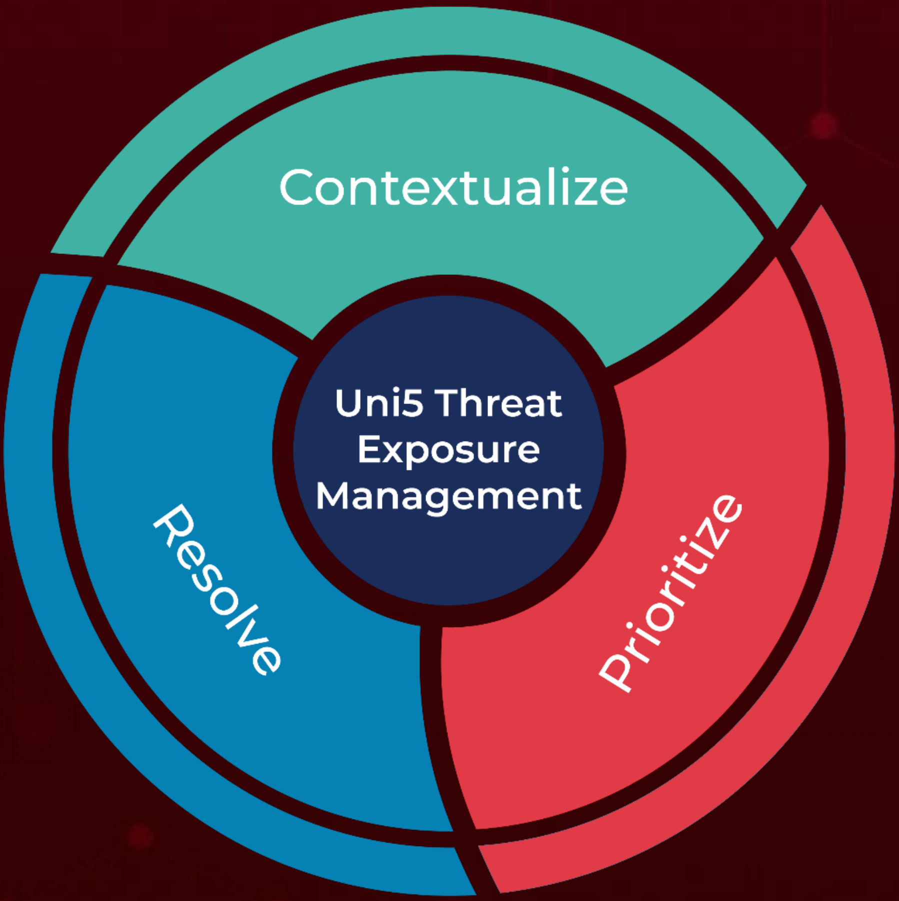
Attack Name	TYPE	VALUE
Gunra Ransomware	Filename	gunraransome.exe R3ADM3.txt
	MD5	9a7c0adedc4c68760e49274700218507
	SHA1	77b294117cb818df701f03dc8be39ed9a361a038
	SHA256	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
	Tox ID	2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22
	TOR Address	gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd[.]onion
PylangGhost	SHA256	267009d555f59e9bf5d82be8a046427f04a16d15c63d9c7ecca749b11d8c8fc3
DragonForce Ransomware	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9, ba1be94550898eedb10eb73cb5383a2d1050e96ec4df8e0bf680d3e76a9e2429

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

June 24, 2025 • 1:00 AM

More at www.hivepro.com