

Date of Publication
May 12, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

5 to 11 MAY 2025

Table Of Contents

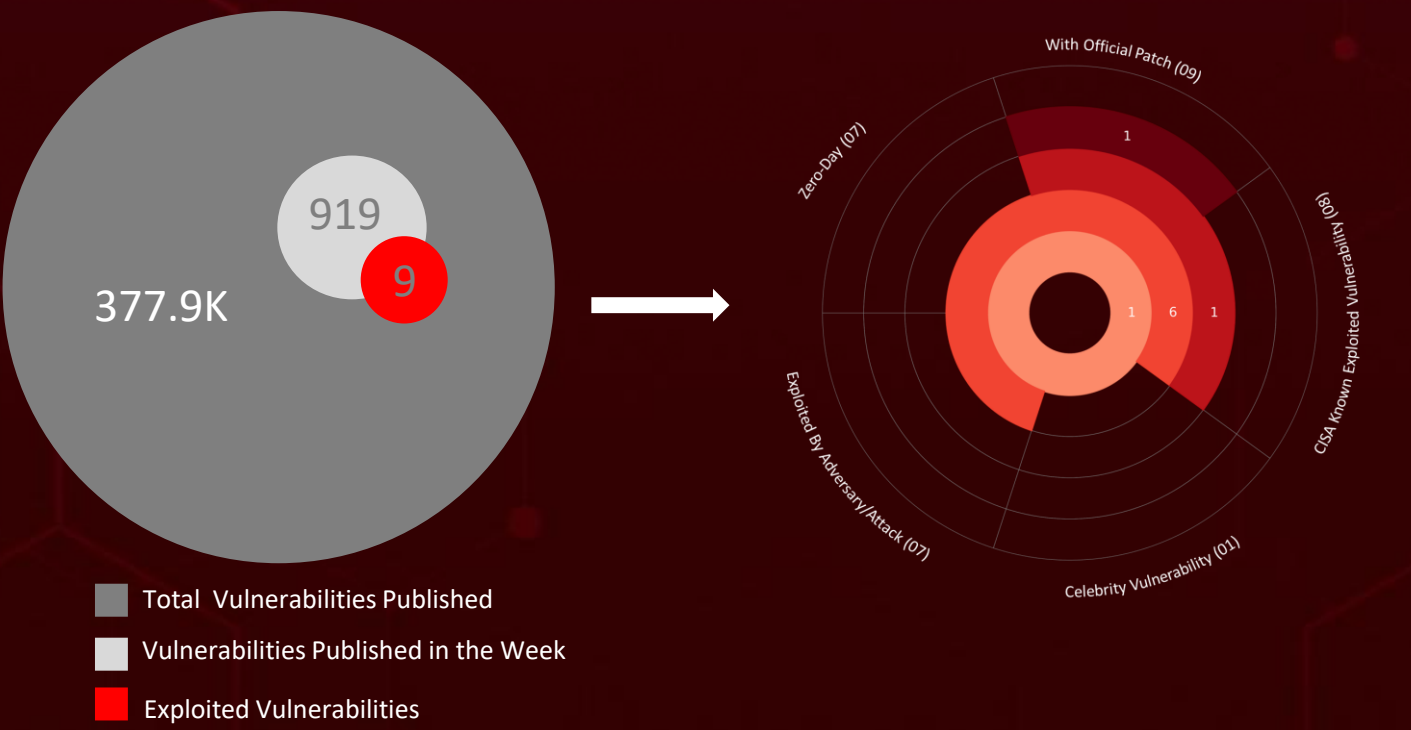
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	19
<u>Recommendations</u>	22
<u>Threat Advisories</u>	23
<u>Appendix</u>	24
<u>What Next?</u>	28

Summary

HiveForce Labs has identified a surge in cyber threats, with **ten** attacks executed, **nine** vulnerabilities uncovered, and **three** active adversaries exposed in the past week alone highlighting the relentless nature of cyberattacks.

HiveForce Labs has uncovered a surge in cyber threats, headlined by **CVE-2025-3248**, a critical unauthenticated remote code execution (RCE) vulnerability in **Langflow**. Public proof-of-concept exploits are already available, and active attacks have been observed. Meanwhile, attackers exploited a Windows privilege escalation flaw (**CVE-2025-29824**) to breach a U.S.-based organization. Using a custom-built infostealer named **Grixba** and stealthy tools, they silently harvested sensitive data and navigated the network undetected demonstrating a calculated and evasive approach to compromise. Moreover, ransomware groups are evolving fast.

DragonForce, which emerged in late 2023, has grown into a formidable Ransomware-as-a-Service (RaaS) platform, attracting cybercriminals with a streamlined business model and low affiliate cuts, offset by advanced tooling and aggressive exploitation tactics including past use of **Log4Shell**. At the same time, the **Agenda** (Qilin) gang is deploying layered attacks with **NETXLOADER** and **SmokeLoader**, leveraging memory injection and stealthy payload delivery to evade defenses before launching full-scale ransomware encryption. These developments signal a clear message: organizations must prioritize rapid patching, threat detection, and cybersecurity resilience to stay ahead of increasingly sophisticated adversaries.



High Level Statistics

10

Attacks
Executed

- [StealC V2](#)
- [More eggs](#)
- [Grixba](#)
- [DragonForce](#)
- [NOOPDOOR](#)
- [ANEL](#)
- [ROAMINGMOUSE](#)
- [Agenda](#)
- [SmokeLoader](#)
- [NETXLOADER](#)

9

Vulnerabilities
Exploited

- [CVE-2025-3248](#)
- [CVE-2025-29824](#)
- [CVE-2025-2857](#)
- [CVE-2021-44228](#)
- [CVE-2023-46805](#)
- [CVE-2024-21412](#)
- [CVE-2024-21887](#)
- [CVE-2024-21893](#)
- [CVE-2022-26134](#)

3

Adversaries in
Action

- [RomCom](#)
- [Venom Spider](#)
- [Earth Kasha](#)



Insights

Earth Kasha uses spear-phishing emails to deploy ROAMINGMOUSE, triggering DLL sideloading for stealthy, in-memory execution of ANEL malware.

CVE-2025-29824: zero-day flaw was weaponized with Grixba, a custom-built infostealer, enabling silent data theft and deeper system infiltration in targeted attacks.

Agenda group has leveled up its tactics, using NETXLOADER and SmokeLoader to orchestrate stealthy, multi-stage attacks.

CVE-2025-3248: A critical Langflow flaw allowing unauthenticated remote code execution, opening the door to full system takeover with a single exploit.

Operation Deceptive Prospect:

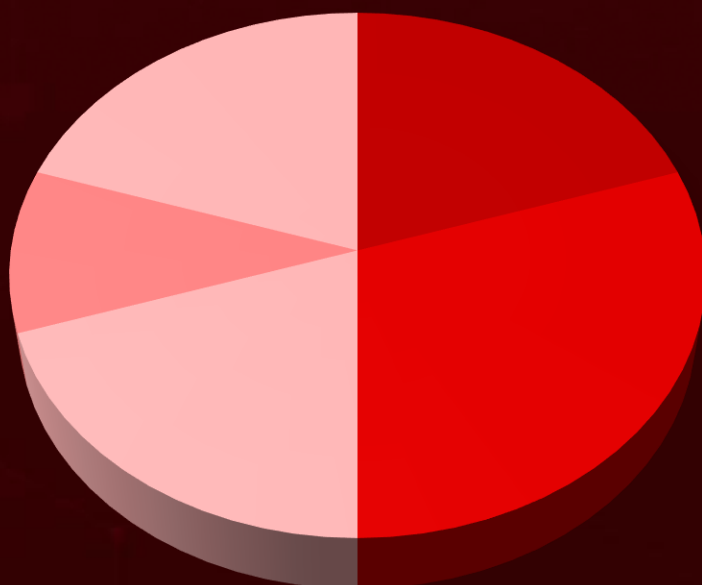
RomCom threat actors went undercover as irate customers, slipping phishing links into fake complaint emails, baiting UK-based services into opening the door to compromise.

DragonForce

Ransomware:

Executing as a brutal multi-extortion playbook that steals data, leaks secrets, and paralyzes critical systems.

Threat Distribution



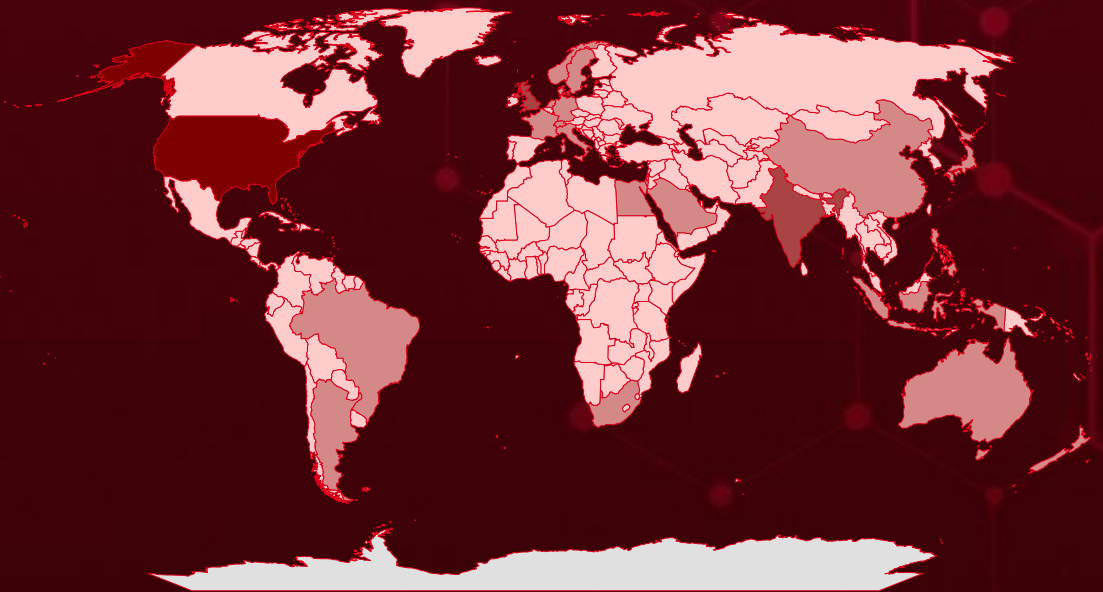
■ Information Stealer ■ Backdoor ■ Ransomware ■ Dropper ■ Loader



Targeted Countries

Most

Least



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

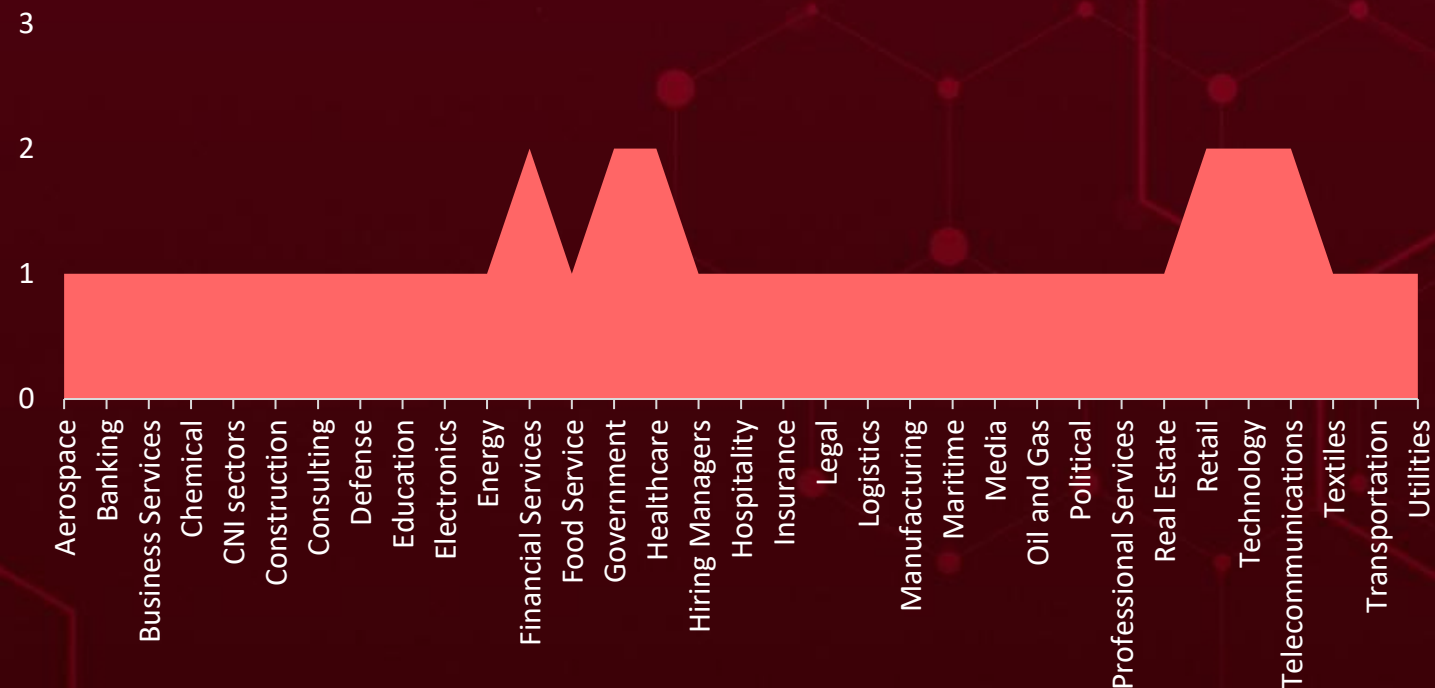
Countries
United States
India
United Kingdom
Norway
Italy
South Africa
Argentina
Netherlands
Australia
Saudi Arabia
Brazil
Israel
China
Switzerland
Denmark
New Zealand
Egypt
Philippines
France
Singapore
Germany

Countries
Sweden
Indonesia
Japan
Serbia
Namibia
Malaysia
Bulgaria
Paraguay
Burkina Faso
Suriname
Burundi
Micronesia
Cabo Verde
North Korea
Cambodia
Rwanda
Cameroon
Botswana
Canada
Lithuania
Central African Republic

Countries
Montenegro
Chile
Belize
Armenia
Pakistan
Colombia
Portugal
Comoros
San Marino
Congo
Slovakia
Costa Rica
Sri Lanka
Côte d'Ivoire
Afghanistan
Croatia
Madagascar
Cuba
Mali
Cyprus
Mauritius
Czech Republic (Czechia)

Countries
Iran
Poland
Iraq
Qatar
Ireland
Russia
Bangladesh
Saint Kitts & Nevis
Barbados
Samoa
Jamaica
Sao Tome & Principe
Belarus
Senegal
Syria
Seychelles
Tanzania
Bosnia and Herzegovina
Timor-Leste
Slovenia
Tonga

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1204

User Execution

T1588

Obtain Capabilities

T1027

Obfuscated Files or Information

T1566

Phishing

T1071

Application Layer Protocol

T1573

Encrypted Channel

T1071.001

Web Protocols

T1036

Masquerading

T1497

Virtualization/ Sandbox Evasion

T1588.006

Vulnerabilities

T1566.002

Spearphishing Link

T1547

Boot or Logon Autostart Execution

T1573.001

Symmetric Cryptography

T1588.005

Exploits

T1059.001

PowerShell

T1190

Exploit Public-Facing Application

T1057

Process Discovery

T1204.002

Malicious File

T1082

System Information Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StealC V2	<p>StealC V2 is an enhanced version of the popular StealC information stealer, first observed in March 2025. This updated variant introduces a streamlined command-and-control (C2) protocol using a JSON-based format, with recent versions incorporating RC4 encryption to secure communication. It features a versatile loader capable of delivering payloads via Microsoft Software Installer (MSI) packages and PowerShell scripts. StealC V2 expands its data theft capabilities with multi-monitor screenshot capture and a unified file grabber that targets a wide array of applications, including cryptocurrency wallets, gaming platforms, messaging apps, email clients, VPNs, and browsers. Additionally, it supports server-side brute-force functionality for credential harvesting.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c, e205646761f59f23d5c8a8483f8a03a313d3b435b302d3a37061840b5cc084c3, a1b2aecdd1b37e0c7836f5c254398250363ea74013700d9a812c98269752f385		
URLs	hxxp[:]//45[.]93[.]20[.]64/c090b39aa5004512[.]php, hxxp[:]//45[.]93[.]20[.]28/3d15e67552d448ff[.]php		

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>More_eggs</u>	More_eggs, also known as SpicyOmelette, is a versatile backdoor malware designed to give attackers remote access to compromised systems. Its modular nature allows threat actors to use it for a range of malicious activities, such as data theft, system surveillance, and delivering additional malware. More_eggs enables attackers to craft highly customized lures and payloads that align closely with the intended victim, increasing the chances of successful compromise.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Venom Spider			-
IOC TYPE	VALUE		
MD5	ec103191c61e4c5e55282f4ffb188156, ebb5fb96bf2d8da2d9f0f6577766b9f1, 2da2f53ffd9969aa8004d0e1060d2ed1		
SHA256	f7a405795f11421f0996be0d0a12da743cc5aaf65f79e0b063be6965c8fb8016, 2fef6c59fbf16504db9790fcc6759938e2886148fc8acab84dbd4f1292875c6c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Grixba</u>	Grixba is an infostealer tool used by attackers to scan networks and enumerate all users and computers within a targeted domain. Typically employed in the early stages of an attack, Grixba helps adversaries map out the environment, identify potential targets, and gather valuable information that can facilitate lateral movement, privilege escalation, or data theft.	Exploiting Vulnerability	CVE-2025-29824
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Steal Data	Microsoft Windows
ASSOCIATE D ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824
IOC TYPE	VALUE		
SHA256	6030c4381b8b5d5c5734341292316723a89f1bdbd2d10bb67c4d06b1242afd05		

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
DragonForce	<p>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.</p> <p>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.</p>	Exploiting Vulnerabilities, Phishing	CVE-2021-44228, CVE-2023-46805, CVE-2024-21412, CVE-2024-21887, CVE-2024-21893, CVE-2022-26134
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data, Data Theft	Apache Log4j2, Ivanti Connect Secure and Policy Secure, Microsoft Windows Internet Shortcut Files, Pulse Connect Secure, ZTA gateways, Pulse Policy Secure, Atlassian Confluence Server and Data Center
ASSOCIATED ACTOR			PATCH LINK
-			https://logging.apache.org/security.html , https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412 , https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US , https://jira.atlassian.com/browse/CONFSERVER-79016
IOC TYPE	VALUE		
SHA1	343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd		

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>NOOPDOOR</u>	NOOPDOOR is a stealthy and sophisticated backdoor that has been exclusively used by the threat group Earth Kasha since at least 2021. Engineered for covert command-and-control (C&C) communication, NOOPDOOR leverages the DNS-over-HTTPS (DoH) protocol to obscure IP address lookups, making its network activity harder to detect. It comes pre-configured with public DoH-compatible DNS servers like Google and Cloudflare, allowing it to bypass traditional DNS monitoring and blend in with normal encrypted web traffic, significantly enhancing its stealth and persistence within compromised environments.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Earth Kasha			-
IOC TYPE	VALUE		
SHA256	7fb4c9f041d4411311437e12427aaf09d369bc384faa2de4b5bc8ae36a42190e, 4f3ec89d5ea0a513afa3f49434f67b7e1540a4a8a93d078def950bd94d444723		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ANEL</u>	ANEL, also known as UPPERCUT, is a backdoor that exists solely in an encrypted form on disk. Its decrypted DLL is only loaded into memory after being decrypted by a loader in preparation for execution. ANEL communicates with its command-and-control (C&C) server over HTTP, using encryption to protect transmitted data from potential interception. It supports basic commands for file manipulation, payload execution, and screenshot capture.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATE D ACTOR			PATCH LINK
Earth Kasha			-
IOC TYPE	VALUE		
SHA256	362b0959b639ab720b007110a1032320970dd252aa07fc8825bb48e8fdd14332, 78f7b98b1e6f089f5789019dab23ac38f77c662fd651ee212d8451ee61b2fc0c		

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
ROAMINGMOUSE	ROAMINGMOUSE is a macro-enabled malicious Excel dropper used by Earth Kasha as the initial infection vector. It employs a simple sandbox evasion technique that requires user interaction to activate its malicious routine, helping it avoid detection in automated analysis environments. Once executed, ROAMINGMOUSE decodes an embedded ZIP archive encoded in Base64, drops it onto the disk, and extracts its contents to deploy ANEL malware components, paving the way for further compromise and persistence.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Dropper		Drops another malware	-
ASSOCIATED ACTOR			PATCH LINK
Earth Kasha			-
IOC TYPE	VALUE		
SHA256	1e0a7737a484699d035c0568771c4834c0ff3fb9ba87aded3c86705e10e9bb0e, 2110b9a4c74d1c8be1aed6ebcff2351cad3d16574026fe4697a9c70810fb1d9e, 488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e58dd2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agenda (aka Qilin, Water Galura)	The Agenda ransomware group, also known as Qilin, has been an active and evolving cyber threat since it was first identified in July 2022. Initially developed in the Go programming language, the ransomware has since transitioned to Rust, a move that enhances its performance, stealth, and resistance to reverse engineering. The newer Rust-based variants include advanced capabilities such as remote execution, improved spread within virtualized environments, and evasion techniques specifically designed to bypass modern security defenses	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATE D ACTOR		Encrypt Data, Data Theft	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	f995ec5d88afab30f9efb62ea3b30e1e1b62cdc3, 05bf016c137230bfdc6eaae95b75a56aff76799d		

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>SmokeLoader</u>	SmokeLoader is a versatile malware loader designed to deploy additional threats on infected systems while offering optional modules for information stealing. It frequently obscures its C2 traffic by generating requests to legitimate websites, making detection more challenging. Once installed, SmokeLoader can deliver various payloads, including cryptominers, ransomware, and password stealers. Beyond deploying malware, it may also exfiltrate sensitive data, corrupt files, and disrupt system operations, posing a significant risk to compromised devices.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft, System compromise and Espionage	-
ASSOCIATE D ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	4684aa8ab09a70d0e25139286e1178c02b15920b, Bdf33e2ba85f35ea86fb016620371fe80855fe68		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>NETXLOADER</u>	NETXLOADER is a stealthy, .NET-compiled loader designed to deliver additional malicious payloads such as Agenda ransomware and SmokeLoader. Operating discreetly in the background, it attempts to load assemblies by name, enabling the execution of follow-on malware without raising immediate suspicion. Its use of the .NET framework allows for flexible payload delivery and evasion of traditional detection mechanisms, making it a valuable tool in multi-stage attack chains.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Loads another malwares	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	16b776ff80f08105b362f9bc76c73a21c51664c2, 1399e63d4662076eeed3b4498c2f958c611a4387		




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




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-29824</u>		Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	Grixba
Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-2857</u>		Firefox versions prior to 136.0.4 Firefox ESR versions prior to 128.8.1 Firefox ESR versions prior to 115.21.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*	-
Mozilla Firefox Sandbox Escape Vulnerability		*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion, T1611: Escape to Host	https://www.mozilla.org/en-US/security/advisories/mfsa2025-19/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>	Log4shell	Apache Log4j2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*	DragonForce
Apache Log4j2 Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46805</u>		Ivanti Connect Secure and Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure-*:*:*:*:*:*	DragonForce
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21412</u>		Microsoft Windows Internet Shortcut Files	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	DragonForce
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204: User Execution T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21887</u>		Ivanti Connect Secure and Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*	DragonForce
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21893</u>		Pulse Connect Secure, ZTA gateways, Pulse Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*.:.:.:.:.*	DragonForce
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-26134</u>		Atlassian Confluence Server and Data Center	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*.:.:.:.:.* cpe:2.3:a:atlassian:confluence_server:*.:.:.:.:.*	DragonForce
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://jira.atlassian.com/browse/CONFSERVER-79016



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><u>RomCom (aka Storm-0978, Tropical Scorpion, Void Rabisu, DEV-0978, UNC2596, UAC-0180)</u></div>	Russia	Retail, Hospitality, and CNI (Critical National Infrastructure) sectors	UK
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; T1036: Masquerading; T1036.008: Masquerade File Type; T1199: Trusted Relationship; T1497: Virtualization/Sandbox Evasion; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1566: Phishing; T1566.002: Spearphishing Link; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1585: Establish Accounts; T1585.002: Email Accounts; T1587: Develop Capabilities; T1587.002: Code Signing Certificates; T1588: Obtain Capabilities; T1588.007: Artificial Intelligence; T1656: Impersonation; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Venom Spider (aka Golden Chickens, badbullz, badbullzvenom)</u>	Russia	Hiring Managers	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	More_eggs	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.007: JavaScript; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1027.013: Encrypted/Encoded File; T1027.014: Polymorphic Code; T1105: Ingress Tool Transfer; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1518: Software Discovery; T1518.001: Security Software Discovery; T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Earth Kasha (aka MirrorFace, Operation LiberalFace)</u></p>	China	Government and Public Sector organizations	Taiwan and Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	NOOPDOOR, ANEL, ROAMINGMOUSE	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1047: Windows Management Instrumentation; T1071: Application Layer Protocol; T1071.004: DNS; T1547: Boot or Logon Autostart Execution; T1036: Masquerading; T1204: User Execution; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1574: Hijack Execution Flow; T1574.001: DLL; T1497: Virtualization/Sandbox Evasion; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1113: Screen Capture; T1057: Process Discovery; T1572: Protocol Tunneling; T1637: Dynamic Resolution; T1637.001: Domain Generation Algorithms			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **RomCom, Venom Spider, Earth Kasha** and malware **StealC V2, More_eggs, Grixba, DragonForce, NOOPDOOR, ANEL, ROAMINGMOUSE, Agenda, SmokeLoader, NETXLOADER**.

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 **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **RomCom, Venom Spider, Earth Kasha** and malware **StealC V2, More_eggs, DragonForce, ANEL, ROAMINGMOUSE, Agenda**, and **NETXLOADER** in Breach and Attack Simulation(BAS).

Threat Advisories

[StealC V2: A Sharpened Blade in the Info-Stealing Arsenal](#)

[Operation Deceptive Prospect: RomCom's New Social Engineering Playbook](#)

[CVE-2025-3248: Langflow AI Workflow Platform RCE](#)

[Hiring Trap: Threat Actors Exploit Job Portals to Breach Corporate Systems](#)

[Silent Escalation: CLFS Zero-Day Used in Targeted Attack](#)

[Critical Firefox Flaw CVE-2025-2857 Lets Attackers Escape Sandbox](#)

[DragonForce Is Selling DIY Ransomware Kits](#)

[Earth Kasha Returns with New Tools in Its Cyber Espionage Campaign](#)

[Agenda Ransomware Group Escalates Attacks with New Multi-Stage Loaders](#)

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>StealC V2</u>	SHA256	0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c, e205646761f59f23d5c8a8483f8a03a313d3b435b302d3a37061840b5cc084c3, a1b2aecdd1b37e0c7836f5c254398250363ea74013700d9a812c98269752f385, 27c77167584ce803317eab2eb5db5963e9dfa86450237195f5723185361510dc, 87618787e1032bbf6a6ca8b3388ea3803be20a49e4afaba1df38a6116085062f
	URLs	hxxp[:]//45[.]93[.]20[.]64/c090b39aa5004512[.]php, hxxp[:]//45[.]93[.]20[.]28/3d15e67552d448ff[.]php, hxxp[:]//88[.]214[.]48[.]93/ea2cb15d61cc476f[.]php
<u>More_eggs</u>	MD5	ec103191c61e4c5e55282f4ffb188156, ebb5fb96bf2d8da2d9f0f6577766b9f1, 2da2f53ffd9969aa8004d0e1060d2ed1, 17158538b95777541d90754744f41f58, 46f142198eeeadc30c0b4ddfbf0b3ffd, b1e8602e283bbdbf52df642dd460a2a2
	SHA256	f7a405795f11421f0996be0d0a12da743cc5aaf65f79e0b063be6965c8fb8016, 2fef6c59fbf16504db9790fcc6759938e2886148fc8acab84dbd4f1292875c6c,

Attack Name	TYPE	VALUE
<u>More_eggs</u>	SHA256	0af266246c905431e9982deab4ad38aaa63d33a725ff7f7675eb23dd75ca4d83, f873352564a6bd6bd162f07eb9f7a137671054f7ef6e71d89a1398fb237c7a7b, 184788267738dfa09c82462821b1363dbec1191d843da5b7392ee3add19b06fb, ccb05ca9250093479a6a23c0c4d2c587c843974f229929cd3a8acd109424700d
<u>Grixba</u>	SHA256	6030c4381b8b5d5c5734341292316723a89f1bdbbd2d10bb67c4d06b1242afd05
<u>DragonForce</u>	SHA1	343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c, 229e073dbcb72bdfec2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4, 577b110a8bfa6526b21bb728e14bd6494dc67f71, 7db52047c72529d27a39f2e1a9ffb8f1f0ddc774, 81185dd73f2e042a947a1bf77f429de08778b6e9, a4bdd6cef0ed43a4d08f373edc8e146bb15ca0f9, b571e60a6d2d9ab78da1c14327c0d26f34117daa, e1c0482b43fe57c93535119d085596cd2d90560a, eada05f4bfd4876c57c24cd4b41f7a40ea97274c, fc75a3800d8c2fa49b27b632dc9d7fb611b65201
	TOR Address	3pktrcbmssvrnwe5skburdwe2h3v6ibdn5kbjqihsg6eu6s6b7ryqd[.]onion, ljbw7iiodqzpg6ooewbgn6mv2pinoer3k5pzdecoejsw5nyoe73zvad[.]onion, Kfgjwkho24xiwckcf53x7qyruobbkhx4eqn2c6oe4hprbn23rcp6qcqd[.]onion, Rnc6scfbqslz5aqxfg5hrjel5qomxsccltc6jvhahi6qwt7op5qc7iad[.]onion, rrrbay3nf4c2wxmhprc6eotjlpqkeowfuobodic4x4nzqtosx3ebirid[.]onion, rrrbayguhtgxrdg5myxkdc2cxei25u6brknfqkl3a35nse7f2arblyd[.]onion, rrrbaygxp3f2qtgvfqk6ffhdrm24ucxvbr6mhxsga4faefqyd77w7tqd[.]onion, Z3wqggtxft7id3ibr7sriyv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion
	Tox ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20, 258C79F73CCC1E56863030CD02C2C7C4347F80CAD43DD6A5B219A618FD17853C7BB1029DAE31

Attack Name	TYPE	VALUE
<u>DragonForce</u>	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9
<u>NOOPDOOR</u>	SHA256	7fb4c9f041d4411311437e12427aaf09d369bc384faa2de4b5bc8ae36a42190e, 4f3ec89d5ea0a513afa3f49434f67b7e1540a4a8a93d078def950bd94d444723
<u>ANEL</u>	SHA256	362b0959b639ab720b007110a1032320970dd252aa07fc8825bb48e8fd d14332, 78f7b98b1e6f089f5789019dab23ac38f77c662fd651ee212d8451ee61b2fc0c
<u>ROAMINGMOUSE</u>	SHA256	1e0a7737a484699d035c0568771c4834c0ff3fb9ba87aded3c86705e10e9bb0e, 2110b9a4c74d1c8be1aed6ebcff2351cad3d16574026fe4697a9c70810fb1d9e, 488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e58dd2, 517ef26be8b9fb1af0e9780b244827af4937ad2fa4778a0bd2d9c65502ce54e1, 63e813b5bf94bdec9ce35c9d7311f76c3a35728d158ade0a6487fc99c73dcf31, 69e2a259e0136b61a3acad3f8fad2c012c75c9d8e26e66a3f0af1e7c23506b5c, 6edf72495e03ca757fa55beb2ea02492f2e7a4b85ca287a9d08bbe60e390c618, 705e5f1245e59566895b1d456aee32d4bff672a6a00f2cd390d7d50c12316dee, 712b81f1a82b9ea9a304220ed87c47c329392c2ce040ed3bff936fe33456acff, 72ece359a3c6f286d174b9cccc7c963577749e38e28f5ecf00dd4c267478a693, 75d6f82962f380f7726142490068879240c3c507427f477cf25268b524c30339, 7b61ed1049ba5f5b8d9725f32cff1ef1e72ef46e2a1dd87bd2b33e73e7333f44, 8cdcd674a0269945dd4c526b5868efb6df8854a127fd5449e57e89905511391d, 9569c4044f8cf32bc9a0513ed7c4497bb6ab71b701c53e58719ef259b3716751, 9c24b60574f39b0565442a79a629a2944672f56acca555e81275e5079382d98b, 9e4c155f4d096d9a0529e83fd21197f3dba20cc4eef48045fd018334384dd513, a12a34d329ccc305dca2306e2d698945f1413c013fe99d4bb069db2127f47806,

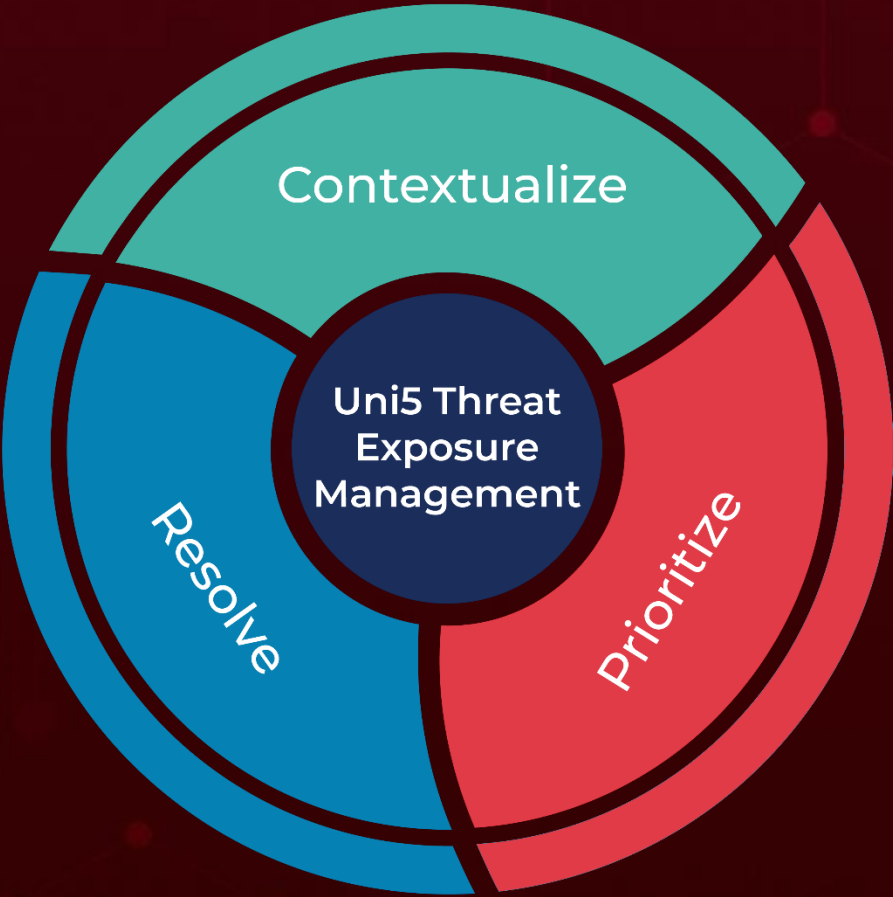
Attack Name	TYPE	VALUE
<u>ROAMINGMOUSE</u>	SHA256	a14c9ae22ca8bdb4971a03f61b2bcc5f140abb51c6922ab7c92ea09ee14dd3bd, a347e1efbfca3722c9e8cc86eba3b288f7e4fae9d386f2a8969faffb125a74c5, ac8c36075ac0085c7d1e96b3fc08c15a151373186e564486dd91d2e49b2dd287, ad050545b65ecbb2178f678c654d84d14986a77051897927e56b5c2893c33608, b56aa48721cd1119a9e06ed9c2f923a1dda5f9aa079dc0e4fd66ab37e33649e8, cb0848d79d2eef76e1d4ff602e0844d03b614d4c25a1b5e3f0ae5c33ea5500b9, cf6ed83d7dcc13f500486044d1af606ceb12c387568ccbb498e01cc7d8005dbd, e123fa2abf1a2f12af9f1828b317d486d1df63aff801d591c5e939eb06eb4cfc, e5b99572581df7a5116511be3f03b9f1a90611235b8288d9f59141876adb1ef1, eeec3a94500ecd025ecdd559e15e4679e26c1347e534944721abe416b49f3871, f502102c5c598d5b9e24f689a3b09b1d2f6702226049a573c421b765867391b3, Fc8c574088af4f74cf84c5c04d522bb1665f548cb17c6192552eb9b783401009
<u>Agenda</u>	SHA1	f995ec5d88afab30f9efb62ea3b30e1e1b62cdc3, 05bf016c137230bfdc6eaae95b75a56aff76799d
	SHA256	8518d0342196772a9e34447484ac5f4944d649f8aa96d36e9e6d47db3f041a78
<u>SmokeLoader</u>	SHA1	4684aa8ab09a70d0e25139286e1178c02b15920b, Bdf33e2ba85f35ea86fb016620371fe80855fe68
	URL	hxxp[:]//]serverlogs295[.]xyz/statweb255/index[.]php, hxxp[:]//]servblog475[.]cfid/statweb255/index[.]php, hxxp[:]//]demblog797[.]xyz/statweb255/index[.]php, hxxp[:]//]admlogs457[.]cfid/statweb255/index[.]php, hxxp[:]//]blogmstat599[.]xyz/statweb255/index[.]php, hxxp[:]//]bloglogs757[.]cfid/statweb255/index[.]php, hxxp[:]//]pzh1966[.]com/statweb255/index[.]php, hxxp[:]//]mxblog77.cfd/777/
<u>NETXLOADER</u>	SHA1	16b776ff80f08105b362f9bc76c73a21c51664c2, 1399e63d4662076eed3b4498c2f958c611a4387
	SHA256	53895523bf8d64b4f8f10d0b38972ceaaed52d9c0486b34ad7cb53b5af017ac4

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
May 12, 2025 • 6:15 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com