

Date of Publication
April 1, 2025



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

24 to 30 MARCH 2025

Table Of Contents

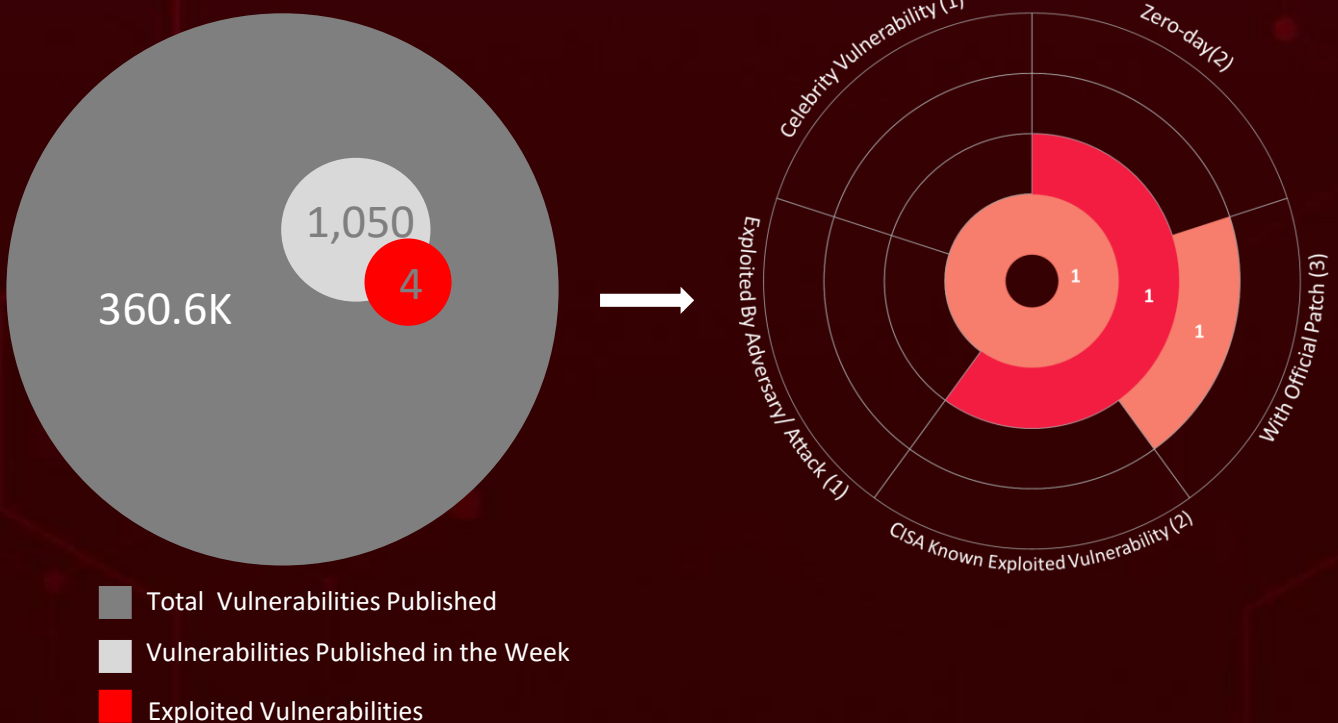
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	13
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	25

Summary

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

One major concern is [CVE-2024-27564](#), an SSRF vulnerability in ChatGPT's pictureproxy.php, which has been actively exploited in over 10,479 attacks within a week, primarily affecting U.S. financial and government institutions. Meanwhile, [VanHelsing](#), a newly emerged RaaS operation launched on March 7, 2025, leverages double extortion tactics. Its ransom demands reach up to \$500,000, and it targets multiple platforms, including Windows, Linux, BSD, ARM, and VMware ESXi.

In addition, [UAT-5918](#), an APT group, is targeting Taiwan to establish long-term intelligence access. It uses web shells and open-source tools for persistence, credential theft, and post-compromise operations. Similarly, the China-linked threat actor [Weaver Ant](#) has infiltrated a major Asian telecom provider, relying on web shells and tunneling techniques to maintain access and facilitate long-term espionage. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

9

Attacks
Executed

4

Vulnerabilities
Exploited

3

Adversaries in
Action

- [China Chopper](#)
- [INMemory](#)
- [VanHelsing](#)
- [EncryptHub](#)
- [DarkWisp](#)
- [SilentPrism](#)
- [Rhadamanthys](#)
- [Stealc](#)
- [MSC EvilTwin](#)

- [CVE-2024-27564](#)
- [CVE-2025-2783](#)
- [CVE-2025-29927](#)
- [CVE-2025-26633](#)

- [UAT-5918](#)
- [Weaver Ant](#)
- [Water](#)
[Gamayun](#)



Insights

UAT-5918 APT

Group Targeting Taiwan for Long-Term Espionage.

CVE-2025-26633 (MSC EvilTwin),

is a critical zero-day in Microsoft MMC, exploited by Russia-linked **Water Gamayun** to execute malicious code via manipulated .msc files, enabling unauthorized access and data theft.

VanHelsing, a newly

emerged RaaS, uses double extortion tactics with ransom demands up to \$500,000, targeting Windows, Linux, BSD, ARM, and VMware ESXi.

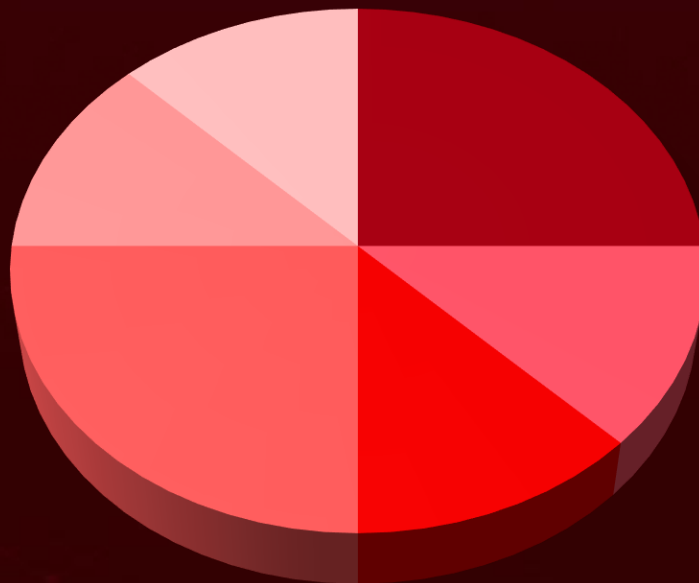
Weaver Ant, a stealthy China-linked APT,

infiltrated a major Asian telecom provider, using web shells for persistence and lateral movement to enable long-term cyber espionage.

Google has patched **CVE-2025-2783**, a high-severity **zero-day** in Chrome's Mojo framework, exploited in Operation ForumTroll phishing attacks targeting Russian organizations.

CVE-2024-27564, an SSRF flaw in ChatGPT's pictureproxy.php, has been exploited in 10,000+ attacks, heavily targeting U.S. financial and government sectors.

Threat Distribution



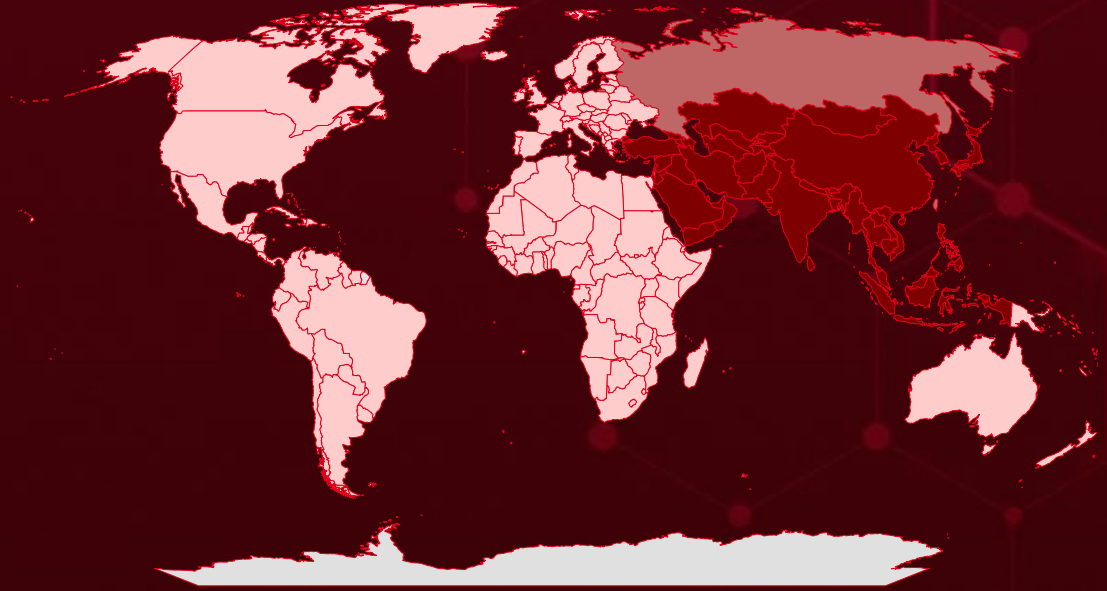
- Web Shell
- Ransomware
- MaaS
- Backdoor
- Information stealer
- Loader



Targeted Countries

Most

Least

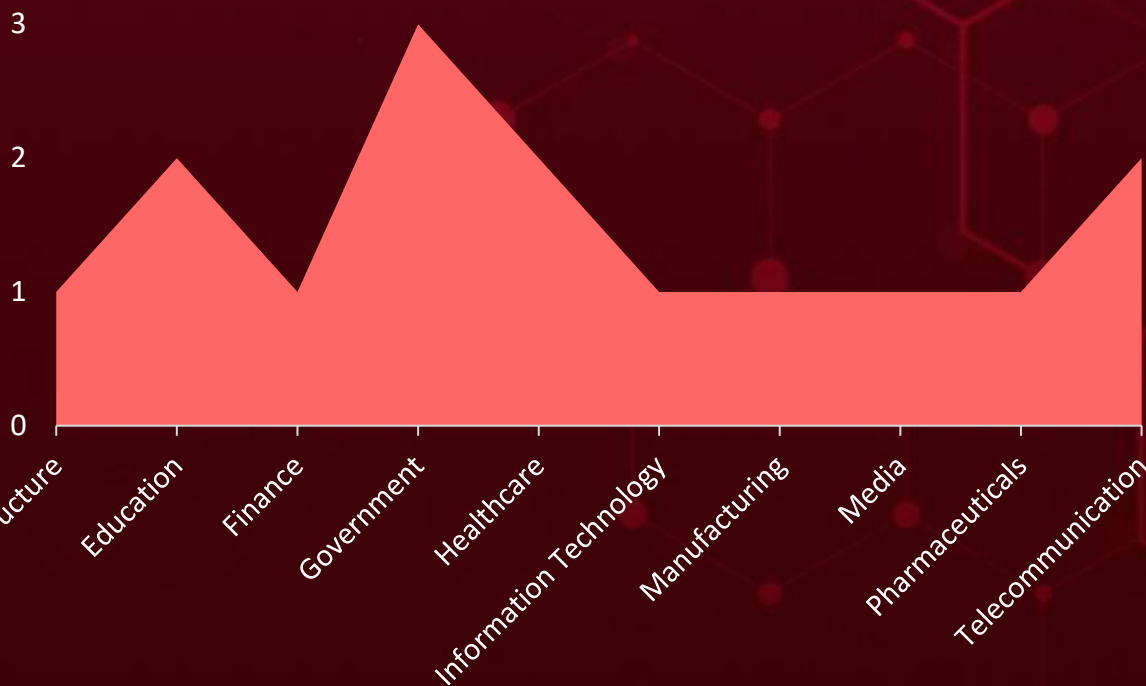


Powered by Bing

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

Countries	Countries	Countries	Countries
Oman	Indonesia	North Macedonia	Netherlands
Uzbekistan	Myanmar	Ecuador	Greece
State of Palestine	Iran	South Sudan	Nigeria
Armenia	North Korea	Egypt	Grenada
Mongolia	Iraq	Nauru	Canada
Azerbaijan	Pakistan	El Salvador	Guatemala
Saudi Arabia	Israel	Peru	Papua New Guinea
Bahrain	Qatar	Equatorial Guinea	Guinea
Timor-Leste	Japan	Sierra Leone	Poland
Bangladesh	Singapore	Eritrea	Guinea-Bissau
Malaysia	Jordan	Switzerland	Rwanda
Bhutan	Sri Lanka	Estonia	Guyana
Nepal	Kazakhstan	United Kingdom	San Marino
Brunei	Syria	Eswatini	Haiti
Philippines	Kuwait	Nicaragua	Serbia
Cambodia	Thailand	Ethiopia	Holy See
South Korea	Kyrgyzstan	Palau	Slovakia
China	Turkey	Fiji	Honduras
Tajikistan	Laos	Chile	South Africa
Cyprus	United Arab Emirates	Finland	Hungary
Turkmenistan	Lebanon	Australia	Congo
Georgia	Vietnam	France	Iceland
Afghanistan	Yemen	Solomon Islands	Suriname
India	Taiwan	Gabon	Bahamas
Maldives	Russia	Costa Rica	Cuba
		Gambia	Algeria

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190

Exploit Public-Facing Application

T1566

Phishing

T1059

Command and Scripting Interpreter

T1204

User Execution

T1068

Exploitation for Privilege Escalation

T1588.006

Vulnerabilities

T1553

Subvert Trust Controls

T1036

Masquerading

T1204.001

Malicious Link

T1588

Obtain Capabilities

T1105

Ingress Tool Transfer

T1133

External Remote Services

T1204.002

Malicious File

T1588.005

Exploits

T1027

Obfuscated Files or Information

T1566.001

Spearphishing Attachment

T1203

Exploitation for Client Execution

T1547

Boot or Logon Autostart Execution

T1041

Exfiltration Over C2 Channel

T1140

Deobfuscate/Decode Files or Information

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>China Chopper</u>	<p>The China Chopper web shell is a lightweight malicious tool that allows attackers to remotely control compromised web servers. It provides features like file management, command execution, and data exfiltration. Its small size and stealth make it effective for maintaining persistent access, enabling further exploitation, and avoiding detection by conventional security measures. Additionally, China Chopper supports AES encryption for its payload.</p>	Compromised Zyxel CPE routers	-
TYPE		IMPACT	AFFECTED PRODUCTS
Web Shell		Remote Control, Data Exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
Weaver Ant			-
IOC TYPE	VALUE		
SHA1	23c4049121a9649682b3b901eaac0cc52c308756, 9022f78087e1679035e09160d59d679dc3ac345d, be52275b0c2086735dac478dc4f09fd16031669a, c879a8eb6630b0cd7537b068f4e9af2c9ca08a62, 25a593b9517d6c325598eab46833003c40f9491a		

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>INMemory</u>	InMemory Web Shell runs malicious code entirely in memory to avoid detection. It decodes a hardcoded GZipped Base64 string into a file called 'eval.dll' and executes it without saving anything to disk. The process involves decoding the string, decompressing it, and then loading the code directly into memory for execution.	Compromised Zyxel CPE routers	-
TYPE		IMPACT	AFFECTED PRODUCTS
Web Shell		Remote Control, Data Exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
Weaver Ant			-
IOC TYPE	VALUE		
SHA1	F31920d636224356e8c7a182c2b9b37e42a09181, 9dc3d272652851428f5cc44f2fd9458bff1d6a78, 4dd22a08a5b103e1f2238aed7f7ce66c5a542533, 02065bbdb3209e0522db3225600b8e79f8a10293, 81622512757f897206a84b29ee866fb933fa3d48		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>VanHelsing</u>	VanHelsing is a new ransomware-as-a-service (RaaS) operation that uses a double extortion strategy. It encrypts files with a ".vanhelsing" extension and exfiltrates sensitive data from the victim. Written in C++, it employs advanced encryption methods.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Exfiltration, Financial Loss	Windows, Linux, BSD, ARM, and VMware ESXi
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17, 99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98		
SHA1	4211cec2f905b9c94674a326581e4a5ae0599df9, 79106dd259ba5343202c2f669a0a61b10adfaff, e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948		

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
EncryptHub	EncryptHub is a sophisticated malware-as-a-service platform that enables multi-stage attacks, including credential theft, keylogging, and remote access. It targets high-value systems using trojanized applications and pay-per-install services.	Phishing	CVE-2025-26633
TYPE		IMPACT	AFFECTED PRODUCT
MaaS			Microsoft Management Console
ASSOCIATED ACTOR			PATCH LINK
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633
IOC TYPE	VALUE		
Domains	encrypthub[.]net, encrypthub[.]org, raw[.]githubusercontent[.]com		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DarkWisp	DarkWisp is a PowerShell-based backdoor designed for persistent unauthorized access and reconnaissance. It exfiltrates sensitive data and executes commands via TCP and HTTPS communication channels.	Phishing	CVE-2025-26633
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor			Microsoft Management Console
ASSOCIATED ACTOR			PATCH LINK
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633
	Persistent control, data exfiltration		

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	
<u>SilentPrism</u>	<p>SilentPrism is a stealthy backdoor used by Water Gamayun for long-term system control. It's designed to establish persistent access to compromised Windows systems, execute arbitrary shell commands, and maintain remote control.</p>	Phishing	CVE-2025-26633	
TYPE		IMPACT	AFFECTED PRODUCT	
Backdoor				Microsoft Management Console
ASSOCIATED ACTOR		Remote control, modular attacks	PATCH LINK	
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE	
<u>Rhadamanthys</u>	<p>Rhadamanthys is information-stealing malware distributed through large-scale phishing campaigns. It is designed to exfiltrate sensitive data from infected systems, including credentials and financial information. Targeting various sectors globally has been observed, often masquerading as legitimate communications to deceive victims.</p>	Phishing	CVE-2025-26633	
TYPE		IMPACT	AFFECTED PRODUCT	
Information stealer				Microsoft Management Console
ASSOCIATED ACTOR		Data theft, espionage	PATCH LINK	
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	
IOC TYPE	VALUE			
SHA256	cbb84155467087c4da2ec411463e4af379582bb742ce7009156756482868859c, 015f0fdf24a19b98447fab5fa16abf929c1cf9be33e9455ce788909dd5a8dbfe, b1fa0ded2f0cc42a70b7a0c051f772cd6db76b15d50ec119307027e670998728, f381a3877028f29ec7865b505b5c85ce77d4947d387d3f30071159fa991f009a, b4f66a5e2876e04db93aae029049a07efed2d6dca05c89c393fe5aba03b949a7			





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
<u>Stealc</u>	Stealc is an advanced information stealer capable of extracting credentials, browser data, cryptocurrency wallets, and other sensitive information from infected systems.	Phishing	CVE-2025-26633
TYPE		IMPACT	AFFECTED PRODUCT
Information stealer		Credential theft, financial loss	Microsoft Management Console
ASSOCIATED ACTOR			PATCH LINK
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633
IOC TYPE	VALUE		
SHA256	725df91a9db2e077203d78b8bef95b8cf093e7d0ee2e7a4f55a30fe200c3bf8f		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>MSC EvilTwin</u>	MSC EvilTwin is a PowerShell trojan loader exploiting MMC vulnerabilities to execute malicious payloads. It uses fake directories and manipulated .msc files to maintain persistence and steal data.	Phishing	CVE-2025-26633
TYPE		IMPACT	AFFECTED PRODUCT
Loader		Code execution, system compromise	Microsoft Management Console
ASSOCIATED ACTOR			PATCH LINK
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633
IOC TYPE	VALUE		
SHA256	5588d1c5901d61bb09cd2fc86d523e2ccbc35a0565fd63c73b62757ac2ee51f5, b1b3d27deb35dd8c8fed75e878adae3f262475c8e8951d59e5df091562c2779b, 7f8bd2d63bb95d61fcbdb22827c3a3e46655f556da769d3880c62865e6fde820, 43eab8488dce80c1086aafdf4594b1a438347e32275abeaa8b2bb14475fb3f98, 1b3309c7a4c3940eff1e1ab1905641b23ea743c4f11d82107ce36fa1ec2299e9		



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-2024-27564</u>		pictureproxy.php component (dirk1983/mm1.ltd, a third-party ChatGPT implementations)	-
	ZERO-DAY		
		AFFECTED CPE	
NAME	CISA KEV	cpe:2.3:a:dirk1983:chatgpt:2023-05-23:*:*:*:*:*:*	-
ChatGPT Pictureproxy.php Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy; T1135: Network Share Discovery; T1133: External Remote Services	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-2783</u>		Google Chrome (Windows) Version prior to 134.0.6998.178	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Google Chromium Mojo Sandbox Escape Vulnerability		cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1036: Masquerading	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-29927</u>		Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Next.js Middleware Bypass Vulnerability		cpe:2.3:a:vercel:next.js:-:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-285	T1505: Server Software Component; T1553: Subvert Trust Controls; T1574: Hijack Execution Flow	https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw , https://github.com/vercel/next.js/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-26633</u>	MSC EvilTwin	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	Water Gamayun
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* :*:*	EncryptHub, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader
Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability	CISA KEY		
			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-707	T1553: Subvert Trust Controls; T1204:User Execution; T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UAT-5918</u>	-	Critical Infrastructure, Information Technology, Telecommunication Providers, Universities, Healthcare	Taiwan, Asia
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0042: Resource Development; TA0043: Reconnaissance; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation; T1090: Proxy; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1590: Gather Victim Network Information; T1136: Create Account; T1217: Browser Information Discovery; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1003: OS Credential Dumping; T1082: System Information Discovery; T1592: Gather Victim Host Information; T1505: Server Software Component; T1505.003: Web Shell; T1555: Credentials from Password Stores; T1016: System Network Configuration Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Weaver Ant</u>	China	Telecommunication	Asia
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	China Chopper, INMemory	Windows

TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1590: Gather Victim Network Information; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1059.007: JavaScript; T1078: Valid Accounts; T1078.002: Domain Accounts; T1078.003: Local Accounts; T1505: Server Software Component; T1505.003: Web Shell; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1055: Process Injection; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1003: OS Credential Dumping; T1003.002: Security Account Manager; T1087: Account Discovery; T1087.002: Domain Account; T1083: File and Directory Discovery; T1135: Network Share Discovery; T1018: Remote System Discovery; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1570: Lateral Tool Transfer; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1074: Data Staged; T1074.001: Local Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1572: Protocol Tunneling; T1090: Proxy; T1090.001: Internal Proxy; T1048: Exfiltration Over Alternative Protocol

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u>Water Gamayun (aka EncryptHub and Larva-208)</u></p>	Russia	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-26633	EncryptHub, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader	Microsoft Management Console

TTPs

TA0004: Privilege Escalation; TA0001: Initial Access; TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0005: Defense Evasion; TA0011: Command and Control; T1218.014: MMC; T1218: System Binary Proxy Execution; T1543: Create or Modify System Process; T1566: Phishing; T1204: User Execution; T1189: Drive-by Compromise; T1059.001: PowerShell; T1036: Masquerading; T1068: Exploitation for Privilege Escalation; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1041: Exfiltration Over C2 Channel; T1059.003: Windows Command Shell; T1222: File and Directory Permissions Modification

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 **UAT-5918, Weaver Ant, Water Gamayun**, and malware **China Chopper, INMemory, VanHelsing, EncryptHub, DarkWisp, SilentPrism, Rhadamanthys, Stealc, MSC EvilTwin**.

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 **UAT-5918, Weaver Ant**, and malware **VanHelsing, Rhadamanthys, Stealc** in Breach and Attack Simulation(BAS).

Threat Advisories

[UAT-5918: Silent Intruder in Taiwan's Cyber Battlefield](#)

[CVE-2024-27564: SSRF Vulnerability Puts AI-Integrated Systems at Risk](#)

[Web Shell Warfare: Weaver Ant's Covert Cyber Espionage Campaign](#)

[A New Ransomware Threat: VanHelsing's Rapid Expansion](#)

[Chrome Zero-Day Exploited in Operation ForumTroll](#)

[Next.js Under Siege as CVE-2025-29927 Opens the Floodgates for Attackers](#)

[Water Gamayun's MSC EvilTwin Attack Targets MMC Framework](#)

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>China Chopper</u>	SHA1	23c4049121a9649682b3b901eaac0cc52c308756, 9022f78087e1679035e09160d59d679dc3ac345d, be52275b0c2086735dac478dc4f09fd16031669a, c879a8eb6630b0cd7537b068f4e9af2c9ca08a62, 25a593b9517d6c325598eab46833003c40f9491a, a9bbea73504139ce91a0ec20fef303c68a131cd4, 334a88e288ae18c6e3fd7fb2d1ad9548497d52ce, 4aeae023766153a91b83d02b1b24da20c0dd135, 3cac6ff7cddcb8f82409c79c85d976300fc60861, 55eeaa904bc6518a2715cc77648e6c5187416a46, ff7b2c3938306261881c42e78d0df51d9bccdd574, 089439168d3c75b4da94ab801f1c46ad6b9e1fdc, a5c36b8022751cfeb4a88a21153847df3870c7c0, ad3dbec2b621807fa9a2f1b2f575d7077e494626, 4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb
<u>INMemory</u>	SHA1	f31920d636224356e8c7a182c2b9b37e42a09181, 9dc3d272652851428f5cc44f2fd9458bff1d6a78, 4dd22a08a5b103e1f2238aed7f7ce66c5a542533, 02065bbdb3209e0522db3225600b8e79f8a10293, 81622512757f897206a84b29ee866fb933fa3d48, 151dc47b213aaec3751ffd1427737c65757ab410, 492cbe143f795888d8e5006ac595f65f4565ed6e

Attack Name	TYPE	VALUE
<u>VanHelsing</u>	Bitcoin Wallet	bc1q0cuvj9eglxk43v9mqmyjzzh6m8qsvsanedwrru
	TOX Address	FEE914521FB507AB978107ACE3B69B4CA41DA89859408BAE23E1512E8C2E614A26C5FFD482A3
	TOR Address	vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd[.]onion, vanhelqmjstkvhrjwzgzjq422iku6wllggiz5y5r3rmfdeiaj3ljaid[.]onion, vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad[.]onion, vanheltarnbfjhuvggbniciap56dscnzz5yf6jmxqivqmb5r2gmllad[.]onion, vanhelvuu04k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd[.]onion, vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad[.]onion, vanhelxjo52qr2ixcmtjayqqrccodkuh36n7uq7q7xj23ggoty3y72yd[.]onion
	SHA256	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17, 99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98
	SHA1	4211cec2f905b9c94674a326581e4a5ae0599df9, 79106dd259ba5343202c2f669a0a61b10adfadff, e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948
	MD5	3e063dc0de937df5841cb9c2ff3e4651, 5c254d25751269892b6f02d6c6384aef, cd9563b4cbc415b3920633b93c0d351b
	<u>EncryptHub</u>	Domains
<u>Rhadamanthys</u>	SHA256	cbb84155467087c4da2ec411463e4af379582bb742ce7009156756482868859c, 015f0fdf24a19b98447fab5fa16abf929c1cf9be33e9455ce788909dd5a8dbfe, b1fa0ded2f0cc42a70b7a0c051f772cd6db76b15d50ec119307027e670998728, f381a3877028f29ec7865b505b5c85ce77d4947d387d3f30071159fa991f009a, b4f66a5e2876e04db93aae029049a07efed2d6dca05c89c393fe5aba03b949a7, bad43a1c8ba1dacf3daf82bc30a0673f9bc2675ea6cdedd34624ffc933b959f4,

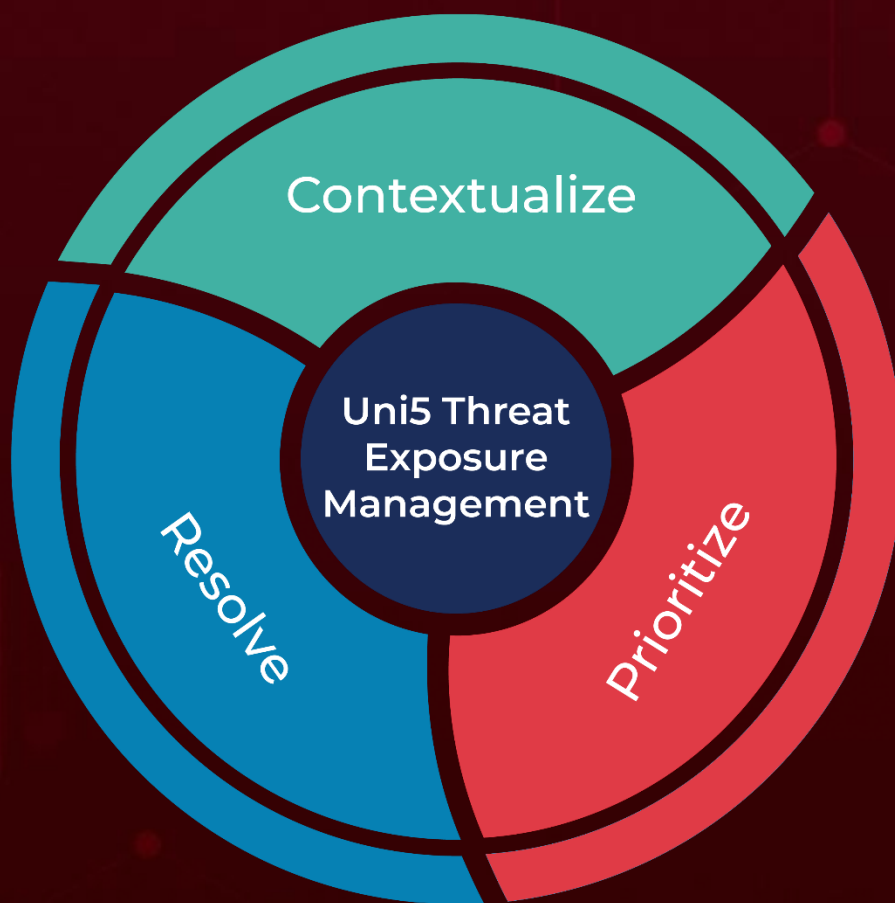
Attack Name	TYPE	VALUE
<u>Rhadamanthys</u>	SHA256	fcfb94820cb2abbe80bdb491c98ede8e6cfa294fa8faf9bea09a9b9cae35bf3, d639cd267b05b4cd420e4547dd7aa4d99fff2d070598de044c7cf0d1b99cd264, 5f6dbe487af0fe7d1cf9beca7e31fcd804d6bdf9a80308d7aeb3ed9abd9bba3, ab58281273e7299f86cfadc1c8235789379543339035c5b4d80becd785bad552
<u>Stealc</u>	SHA256	725df91a9db2e077203d78b8bef95b8cf093e7d0ee2e7a4f55a30fe200c3bf8f
<u>MSC EvilTwin</u>	SHA256	5588d1c5901d61bb09cd2fc86d523e2ccbc35a0565fd63c73b62757ac2ee51f5, b1b3d27deb35dd8c8fed75e878adae3f262475c8e8951d59e5df091562c2779b, 7f8bd2d63bb95d61fcbdb22827c3a3e46655f556da769d3880c62865e6fde820, 43eab8488dce80c1086aafdf4594b1a438347e32275abeaa8b2bb14475fb3f98, 1b3309c7a4c3940eff1e1ab1905641b23ea743c4f11d82107ce36fa1ec2299e9, 2aeb9aeca5739ea1cb5a30d284d65e36fe18f47db9e5e504063d982b9c3bc3e9, 9b830c2979cbce45573aa21d765adda76f52db254155ae49648ef5050ceaf774, 4e6f35ab5eb9242335bee01d6df9b50f665043f9930a630df7e170b904f52a24, d76c25e2761210783055b43349370253d794e94ee913a2be7596b9554eacf107, 5357279bad530c3af89713aaf6befe19a22e438f22952aed46097590130551fa, 413dea8ea8cb09cd3ac49531a8e0a13f767c09f78fb77856f4668377532a64ef, 0943b0f328282504c2661cd56e4bd83e3b3e5a4cce89e2e5523f83a2d535a07e, f5c97f23543e904944120ef738f300049eae85c3b0bf8b86b346572f7bc6dec1, 9e9ca325f44eeff4087bb67052536ba565da18e70e5b29c79ed77c14c5548131, 94ee2227696da3049ff67592834b4b6f98186f91e6d1cd1eeec44f24b9df754b, cedf4589428ae05d3d2dca1d1bd7fa28f6cafe54a077a6090f873053e04fd5ce, bb563180196989dcee91417aa56d6f1bfc9320b2427536c200dffcd784774906,

Attack Name	TYPE	VALUE
<u>MSC EvilTwin</u>	SHA256	9d2aaa8672d583af4c03c23127d6cac509799a49ff9293ed63628d5b710b7528, 3761060c509b9444bdd3d0e65d7f68e39ff5c52fa87fdc59db02c1553e21e403, 47e4142fa6ab10a2d7dc0423d41f9bdbb3ced0f4fae5c58b673386d11dd8c973, 6b99530953010dd8061a3a328c04c30653bba26439dd30a752262582b0d02933

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

April 1, 2025 • 11:45 PM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com