

Date of Publication
April 14, 2025



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

7 to 13 APRIL 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>	11
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	23

Summary

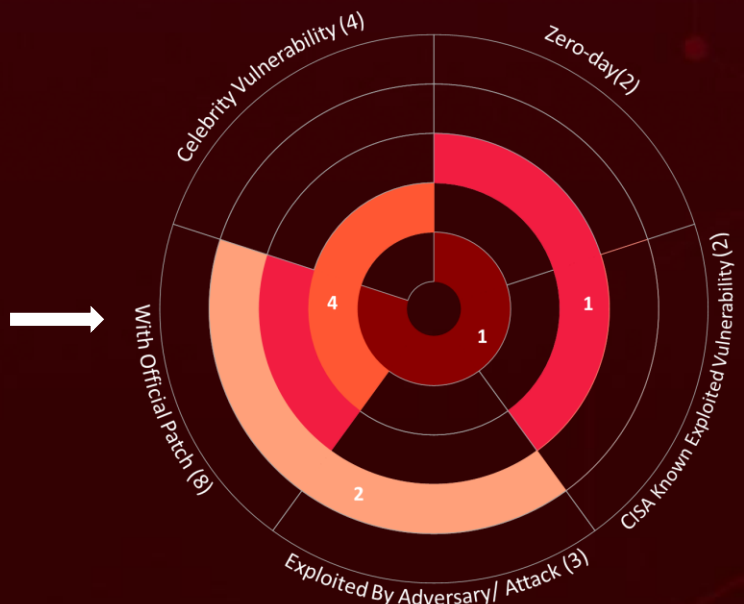
HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **four** attacks, reported **eight** vulnerabilities, and identified **three** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Microsoft's April 2025 Patch Tuesday resolves 126 security flaws, including a critical zero-day (CVE-2025-29824) in the Windows CLFS driver. Meanwhile, over 6,500 Kubernetes clusters are exposed due to **IngressNightmare**, a set of four critical flaws in the NGINX Ingress Controller allowing unauthenticated RCE and full cluster takeover with a single crafted request.

In addition, the **ToddyCat APT** exploited CVE-2024-11859 in ESET's command-line scanner by using DLL proxying and a custom tool (TCESB) to stealthily load malicious code and manipulate kernel structures. Similarly, the **UAC-0226** campaign targets Ukrainian entities with phishing emails, deploying GIFTEDCROOK malware to steal browser data and exfiltrate it via Telegram, thus compromising security. These rising threats pose significant and immediate dangers to users worldwide.



- Total Vulnerabilities Published
- Vulnerabilities Published in the Week
- Exploited Vulnerabilities



High Level Statistics

4

Attacks
Executed

- [PipeMagic](#)
- [GIFTEDCROOK](#)
- [Hellcat](#)
- [Neptune](#)

8

Vulnerabilities
Exploited

- [CVE-2025-29824](#)
- [CVE-2025-30406](#)
- [CVE-2024-11859](#)
- [CVE-2021-36276](#)
- [CVE-2025-1974](#)
- [CVE-2025-1097](#)
- [CVE-2025-1098](#)
- [CVE-2025-24514](#)

3

Adversaries in
Action

- [ToddyCat](#)
- [Storm-2460](#)
- [UAC-0226](#)



Insights

UAC-0226 targets Ukraine with phishing emails that deploy GIFTEDCROOK malware to steal and exfiltrate browser data via Telegram.

PoisonSeed is a phishing campaign that hijacks email platforms to spread crypto scams using seed phrase poisoning to steal wallets and drain funds.

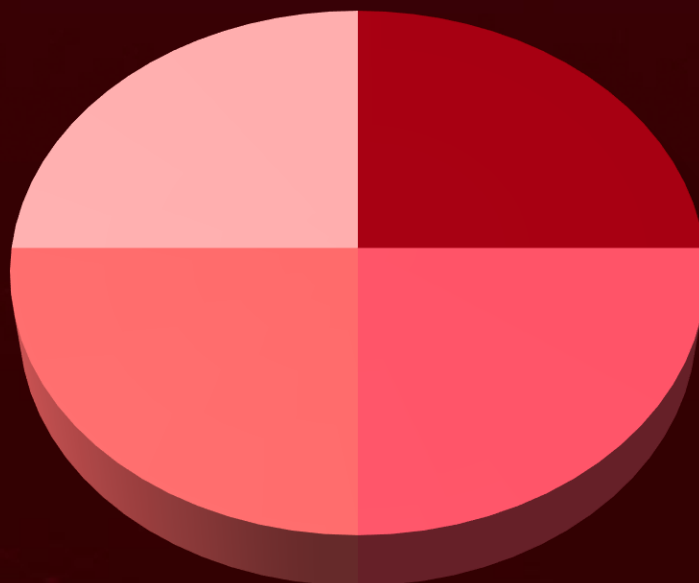
CVE-2025-30406, a critical zero-day in Gladinet CentreStack, allows remote code execution via a hard-coded cryptographic key.

Microsoft's April 2025 Patch Tuesday fixes 126 vulnerabilities, including a **zero-day (CVE-2025-29824)** in the CLFS driver, urging immediate updates to prevent exploitation.

HellCat, a 2024 Ransomware-as-a-Service, uses a decentralized model to deliver custom payloads, exfiltrate data, and encrypt systems in a double-extortion scheme targeting high-value sectors.

Neptune RAT disguises as a remote access tool, stealing credentials, intercepting crypto transactions, and compromising systems via platforms like GitHub and Telegram.

Threat Distribution



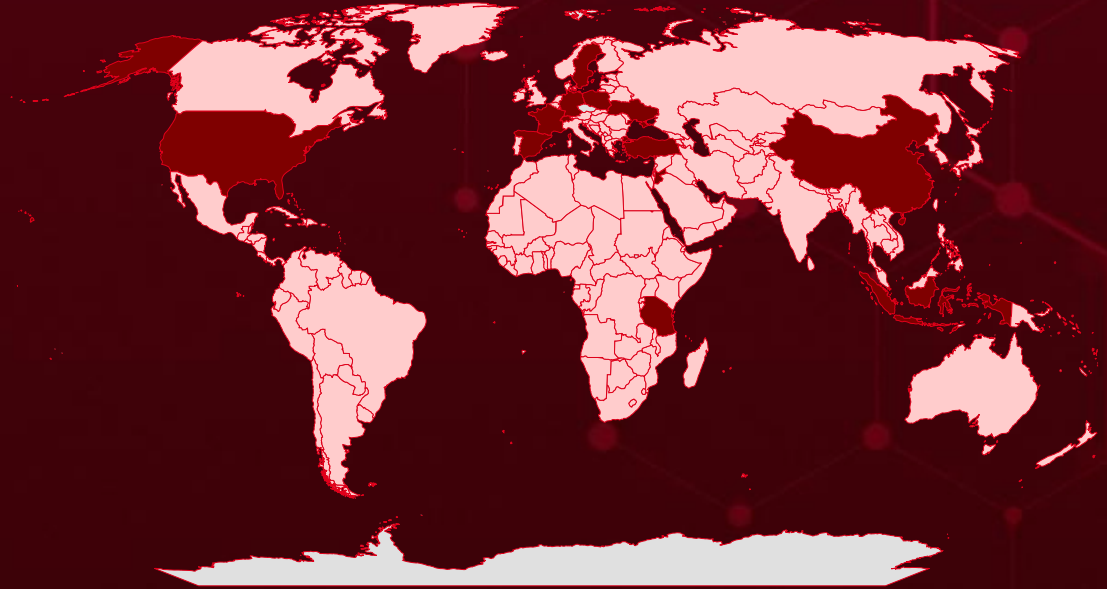
■ Modular RAT ■ Ransomware ■ Backdoor ■ Infostealer



Targeted Countries

Most

Least

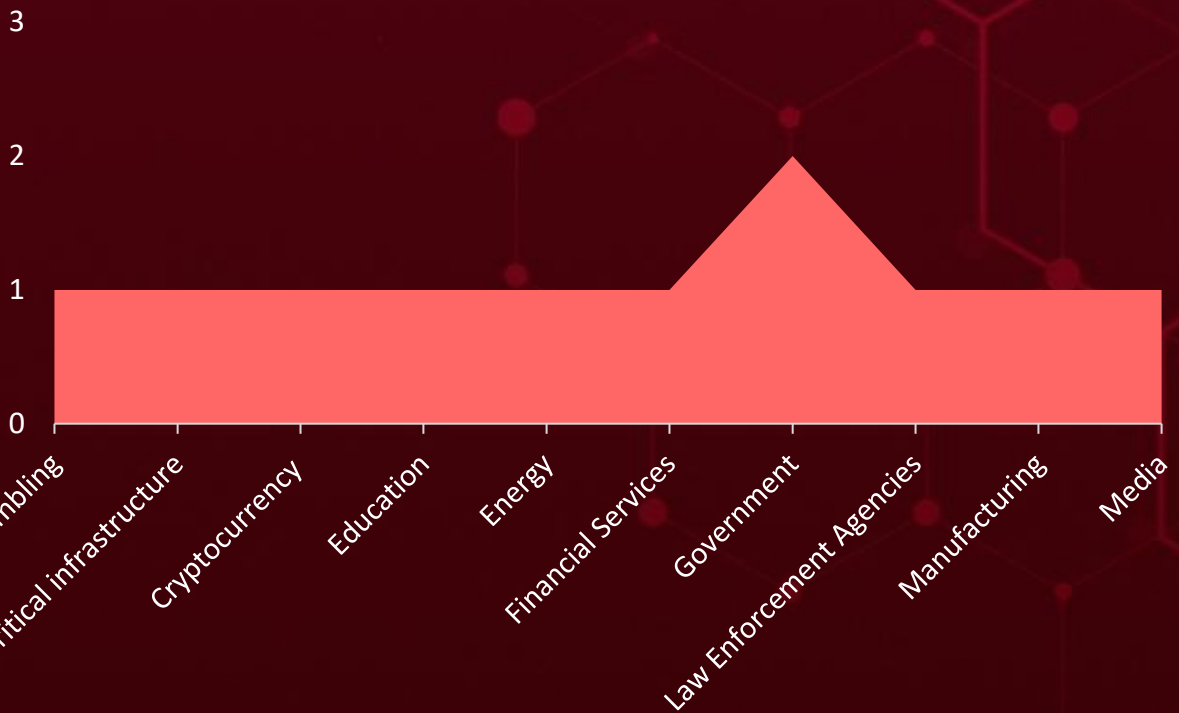


Powered by Bing

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

Countries	Countries	Countries	Countries
Spain	Benin	Turkmenistan	Mongolia
Turkey	Oman	Chad	Rwanda
Switzerland	Bhutan	Luxembourg	Djibouti
China	Saint Lucia	Chile	Serbia
Poland	Bolivia	Maldives	Dominica
France	South Sudan	Albania	Slovakia
Sweden	Bosnia and Herzegovina	Mauritania	Dominican Republic
Germany	Tonga	Colombia	South Africa
Tanzania	Botswana	Moldova	DR Congo
Indonesia	Malawi	Comoros	Sri Lanka
Ukraine	Brazil	Morocco	Ecuador
Jordan	Mexico	Congo	Suriname
United States	Brunei	Nauru	Egypt
Argentina	Myanmar	Costa Rica	Taiwan
Malta	Bulgaria	Nicaragua	El Salvador
Austria	Nigeria	Côte d'Ivoire	Timor-Leste
Barbados	Burkina Faso	North Macedonia	Equatorial Guinea
Netherlands	Burkina Faso	Croatia	Tunisia
Belarus	Papua New Guinea	Palau	Eritrea
Sierra Leone	Burundi	Cuba	Uganda
Belgium	Romania	Peru	Estonia
United Arab Emirates	Cabo Verde	Cyprus	Lithuania
Belize	Saudi Arabia	Qatar	Malaysia
Madagascar	Cambodia	Czech Republic (Czechia)	Fiji
Ethiopia	Solomon Islands	Denmark	Algeria
	Cameroon	San Marino	Mauritius
	State of Palestine		French Guiana

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1068

Exploitation for Privilege Escalation

T1588.006

Vulnerabilities

T1588

Obtain Capabilities

T1566

Phishing

T1588.005

Exploits

T1041

Exfiltration Over C2 Channel

T1203

Exploitation for Client Execution

T1204

User Execution

T1204.001

Malicious Link

T1133

External Remote Services

T1105

Ingress Tool Transfer

T1140

Deobfuscate/Decode Files or Information

T1566.001

Spearphishing Attachment

T1027

Obfuscated Files or Information

T1547

Boot or Logon Autostart Execution

T1036

Masquerading

T1553

Subvert Trust Controls

T1204.002

Malicious File

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PipeMagic</u>	PipeMagic is a sophisticated backdoor Trojan malware distributed via fake ChatGPT applications developed in Rust, targeting entities globally since 2022. The malware uses encrypted communication through named pipes and grants attackers remote access, enabling further infections like ransomware or data theft	Exploiting vulnerabilities	CVE-2025-29824
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Remote Control, Data Exfiltration and Data Theft	PATCH LINK
Storm-2460			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824
IOC TYPE	VALUE		
SHA256	2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe		

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>GIFTEDCROOK</u>	GIFTEDCROOK is a custom malware developed in C/C++ used in the UAC-0226 cyber-espionage campaign. It extracts sensitive data from browsers like Chrome, Edge, and Firefox, including credentials and cookies. The stolen data is exfiltrated via PowerShell commands to a Telegram bot, enabling covert communication.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer			
ASSOCIATED ACTOR			
UAC-0226		Data Theft	PATCH LINK

IOC TYPE	VALUE
SHA256	8427dc6e7da4c163d20c7f188232cf3f83c78ddb6fcad04cec84b33e0f9bdfc0, 7ca3f2505e1778e6de3927571ba49d27b36447e6c28a60161d55fd2254966bce, 2930ad9be3fec3ede8f49cecd33505132200d9c0ce67221d0b786739f42db18a, 530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1, ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Hellcat</u>	HellCat is a Ransomware-as-a-Service (RaaS) operation that emerged in 2024, leveraging a decentralized affiliate model to deliver customized payloads and infrastructure. It gains access through phishing or exploiting vulnerabilities, then exfiltrates data and encrypts systems in a double-extortion scheme.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR			
-		Data Exfiltration, Financial Loss	PATCH LINK




IOC TYPE	VALUE
SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599




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>Neptune</u>	Neptune RAT is a deceptive and dangerous malware posing as a remote access tool, spreading through platforms like GitHub and Telegram. Beneath the surface, it functions as a versatile tool for cybercriminals capable of stealing credentials, intercepting cryptocurrency transactions, monitoring user activity, and severely compromising system integrity.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Modular RAT			Windows
ASSOCIATED ACTOR			PATCH LINK
-		Data theft and Financial gain	-
IOC TYPE	VALUE		
SHA256	8df1065d03a97cc214e2d78cf9264a73e00012b972f4b35a85c090855d71c3a5, e8c8f74ae15e7d809d9013bdfa2a10dd54e00d4ea5ff4ed6cd4a163b80d2d318, add3e9a1c6654d1ec9b7fd0ffea6bdcd0eb7b3e4afa70c6776835cc238e8f179, 9a35113e1d9412701d85b5af01b4ad2b1e584c6e0963e439053808b29b4da90a, 684d2d50dd42e7ba4e9bd595e9b6f77eb850185556c71db4eda6f78478a5e6fb		




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-2025-29824</u>		Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	Storm-2460
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* :*:*	PipeMagic
Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	<u>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824</u>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30406		Gladinet CentreStack through 16.1.10296.56315	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability		cpe:2.3:a:gladinet:centres tack:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-321	T1552.004 Unsecured Credentials: Private Keys; T1190 : Exploit Public-Facing Application	https://www.centrestack.com/p/gce_latest_release.html



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11859		ESET Multiple Products	ToddyCat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
ESET Multiple Products DLL Search Order Hijacking Vulnerability		cpe:2.3:a:eset:multiple_products:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-427	T1574.001 Hijack Execution Flow: DLL Search Order Hijacking; T1059: Command and Scripting Interpreter	https://support.eset.com/en/ca8810-dll-search-order-hijacking-vulnerability-in-eset-products-for-windows-fixed

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-36276</u>		Dell DBUtilDrv2.sys Driver	ToddyCat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dell:dbutildrv2.sys_firmware:*:*:*:*:*:*	-
Dell DBUtilDrv2.sys Driver Insufficient Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-285	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://www.dell.com/support/kbdoc/en-us/000190105/dsa-2021-152-dell-client-platform-security-update-for-an-insufficient-access-control-vulnerability-in-the-dell-dbutildrv2-sys-driver

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-1974</u>	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*	-
Kubernetes Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-1097</u>	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*	-
Kubernetes Arbitrary Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-1098</u>	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*	-
Kubernetes Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24514</u>	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*	-
Kubernetes Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://github.com/kubernetes/ingress-nginx/releases

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ToddyCat	China	-	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2024-11859 CVE-2021-36276	-	Windows

TTPs

TA0042: Resource Development; TA0005: Defense Evasion; T1588: Obtain Capabilities; T1574: Hijack Execution Flow; TA0007: Discovery; TA0003: Persistence; T1036: Masquerading; T1059: Command and Scripting Interpreter; TA0002: Execution; TA0011: Command and Control; TA0004: Privilege Escalation; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1027: Obfuscated Files or Information; T1574.001: DLL Search Order Hijacking; T1211: Exploitation for Defense Evasion; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1588.006: Vulnerabilities; T1082: System Information Discovery; T1083: File and Directory Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Storm-2460</u>	-	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-29824	PipeMagic	Windows

TTPs

TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1055: Process Injection; T1059: Command and Scripting Interpreter; T1555: Credentials from Password Stores; T1071: Application Layer Protocol; T1562: Impair Defenses; T1486: Data Encrypted for Impact; T1082: System Information Discovery; T1547: Boot or Logon Autostart Execution; T1005: Data from Local System; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UAC-0226</u>	-	Military, Law Enforcement Agencies, Government	Ukraine
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	GIFTEDCROOK	Windows

TTPs

TA0001: Initial Access; TA0006: Credential Access; TA0005: Defense Evasion; T1059: Command and Scripting Interpreter; T1140: Deobfuscate/Decode Files or Information; TA0010: Exfiltration; TA0009: Collection; T1566.001: Spearphishing Attachment; T1027: Obfuscated Files or Information; TA0002: Execution; TA0011: Command and Control; T1059.001: PowerShell; TA0007: Discovery; TA0003: Persistence; T1204: User Execution; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1204.002: Malicious File; T1539: Steal Web Session Cookie ; T1041: Exfiltration Over C2 Channel; T1567.002: Exfiltration to Cloud Storage; T1567: Exfiltration Over Web Service; T1555.003: Credentials from Web Browsers; T1566: Phishing

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actors **ToddyCat, Storm-2460, UAC-0226**, and malware **PipeMagic, GIFTEDCROOK, Hellcat, Neptune RAT**.

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 **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **ToddyCat**, and malware **GIFTEDCROOK, Hellcat, Neptune RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[PoisonSeed: The Silent Harvest of Trust in Email Supply Chains](#)

[CVE-2025-30065: A Ticking Time Bomb in Apache Parquet](#)

[ToddyCat Hackers Exploit ESET Flaw to Deploy Hidden Malware](#)

[Microsoft's April 2025 Patch Tuesday Fixes Active Zero-Day Exploits](#)

[IngressNightmare Isn't Just a Bug, It's a Blueprint for Breach](#)

[UAC-0226: Targeted Cyber-Espionage Against Ukrainian Innovation Hubs](#)

[CentreStack RCE Vulnerability Actively Exploited in the Wild](#)

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

[Neptune RAT's Triple Threat: To Steal, Spy, and Encrypt](#)

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)

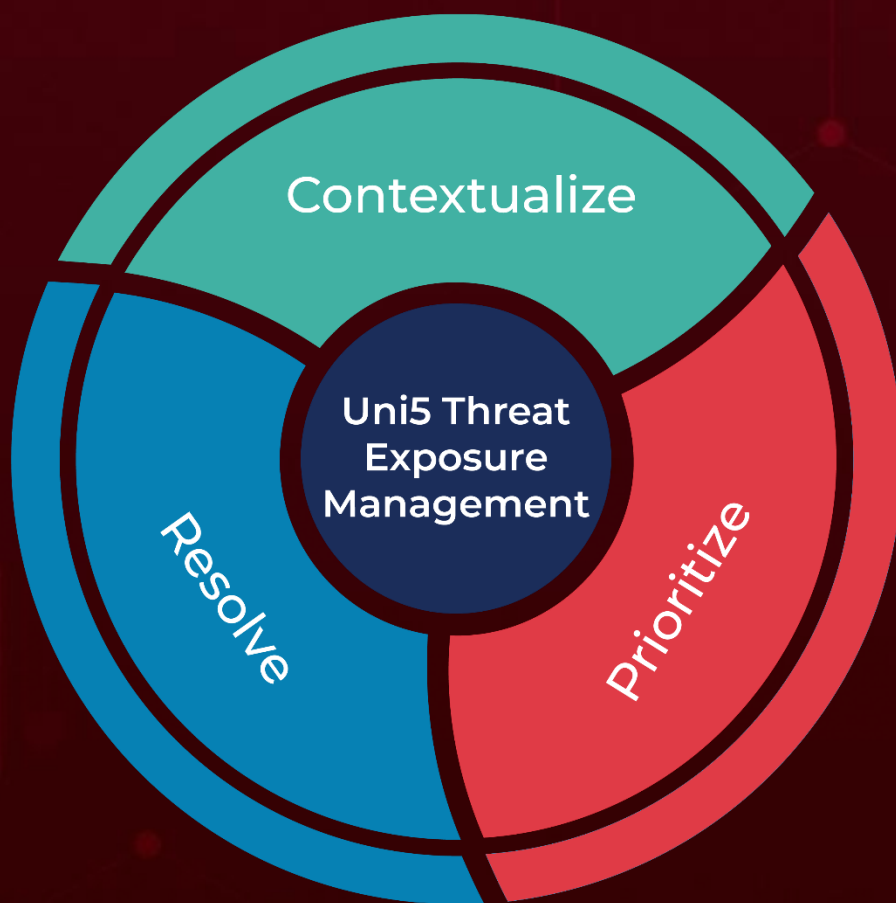
Attack Name	TYPE	VALUE
<u>PipeMagic</u>	SHA256	2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe
<u>GIFTEDCROOK</u>	SHA256	8427dc6e7da4c163d20c7f188232cf3f83c78ddb6fcad04cec84b33e0f9bdfc0, 7ca3f2505e1778e6de3927571ba49d27b36447e6c28a60161d55fd2254966bce, 2930ad9be3fec3ede8f49cecd33505132200d9c0ce67221d0b786739f42db18a, 530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1, ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a, d7a66fd37e282d4722d53d31f7ba8ecdabc2e5f6910ba15290393d9a2f371997
<u>Hellcat</u>	SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599,

Attack Name	TYPE	VALUE
<u>Hellcat</u>	SHA256	b8e71845cc8ccd668a3436d1952a6c57649974bb8399e599dc33afc4c0843be7, dcd7995038ad4839e88e5bb3bf654b4f7c2ad09780a39c9d47596ce717fd4ac2
	MD5	931396d6332709956237cf76ee246b01
	SHA1	b834d9dbe2aed69e0b1545890f0be6f89b2a53c7
	Tor Address	hellcakbszllztlyqbjzwcdbdhfrod55wq77kmftp4bhnhsnn5r3odad[.]onion
<u>Neptune</u>	SHA256	8df1065d03a97cc214e2d78cf9264a73e00012b972f4b35a85c090855d71c3a5, e8c8f74ae15e7d809d9013bdfa2a10dd54e00d4ea5ff4ed6cd4a163b80d2d318, add3e9a1c6654d1ec9b7fd0ffea6bdcd0eb7b3e4afa70c6776835cc238e8f179, 9a35113e1d9412701d85b5af01b4ad2b1e584c6e0963e439053808b29b4da90a, 684d2d50dd42e7ba4e9bd595e9b6f77eb850185556c71db4eda6f78478a5e6fb, 9ca70da0ea94b3bea68c9a3259ec60192c5be1ae7630a08924053168bbf41335, 1bbd4262c8821a0290fe40a8e374c6e5fa2084331670ede42e995d3d5902efcd, 20c31ac326b5c6076f9b1497f98b14a0acd36ff562dfa2076589a47a41d0e078, 6d02eb3349046034cf05e25e28ef173c01d9e0ea1f4d96530defe9e2a3d5e8a0, cd2b320433843d4d694ae8185c7ef07a90d7dce6d05a38ac4481ad2eab9bcfe5, 630b1879c2e09b2f49dd703a951fb3786ede36b79c5f00b813e6cb99462bf07c

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 14, 2025 • 6:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com