Date of Publication
December 22, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

15 to 21 DECEMBER 2025

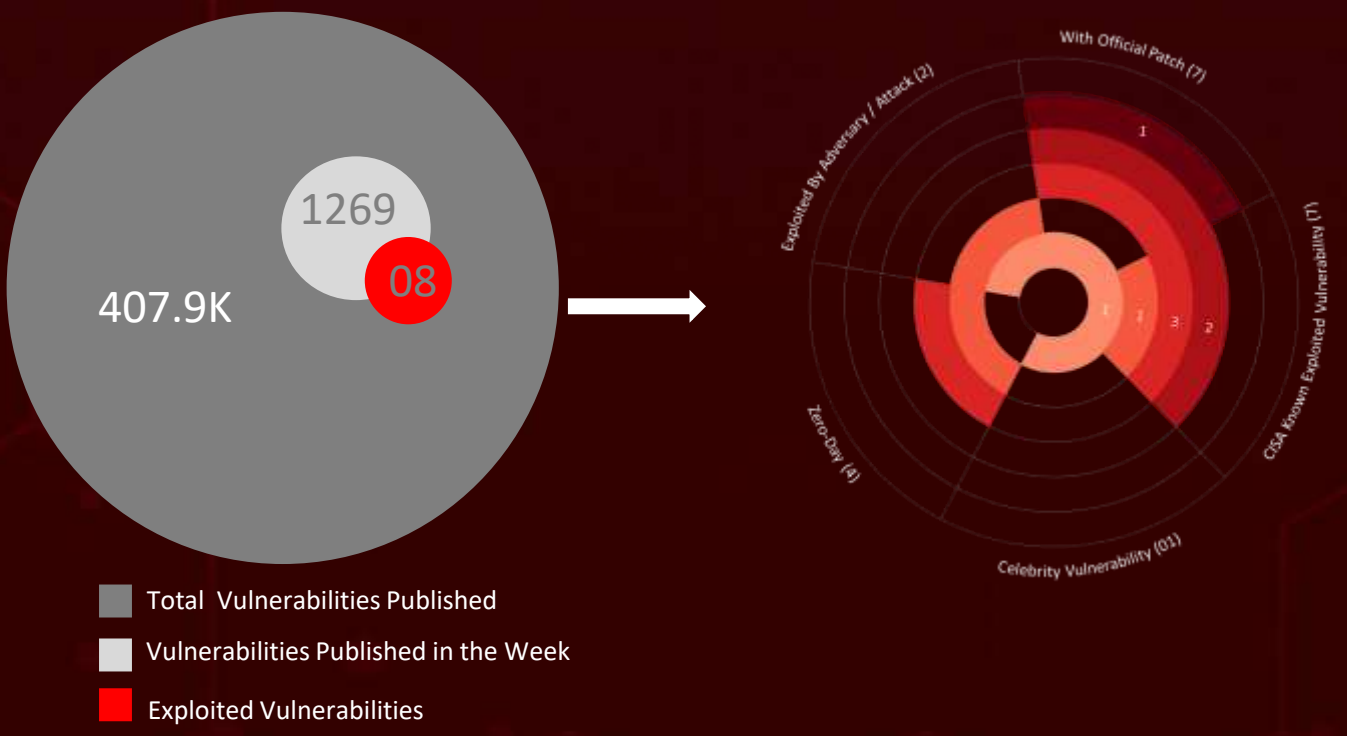
Table Of Contents

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **eighteen** major attacks were detected, **eight** vulnerabilities were publicly disclosed, and **six** active threat actor group was monitored, signaling a concerning escalation in malicious activity.

Several high-impact vulnerabilities and zero-day exploits are driving this surge. Apple issued emergency security updates to patch two actively exploited WebKit zero-days, **CVE-2025-43529** and **CVE-2025-14174**, which were leveraged in highly targeted attacks and could enable remote code execution. Additionally, SonicWall also addressed **CVE-2025-40602**, an actively exploited vulnerability affecting the SMA 1000 series Appliance Management Console. Adding to the urgency, Cisco disclosed **CVE-2025-20393**, a critical zero-day in Cisco AsyncOS that allows unauthenticated remote command execution with root privileges through the Spam Quarantine interface. The flaw has been exploited since late November 2025 by the China-linked APT group **UAT-9686**, and no official patch is currently available.

On the malware front, **GhostPoster** has emerged as a stealthy and large-scale campaign abusing trusted Firefox extensions to infect users, concealing malicious JavaScript within PNG logo files using steganography. Moreover, **Operation MoneyMount-ISO** continues to target victims through phishing emails carrying fake payment confirmations, ultimately deploying the Phantom information stealer via ZIP archives containing malicious ISO files. Together, these developments highlight the urgent need for timely patching, continuous monitoring, and layered security controls to keep pace with an increasingly aggressive and fast-moving threat landscape.



High Level Statistics

18
Attacks Executed

8
Vulnerabilities Exploited

6
Adversaries in Action

- Snowlight
- Vshell
- Noodle RAT
- KSwapDoor
- Auto-color
- Minocat
- Compood
- Hisonic
- Phantom
- SantaStealer
- AquaShell
- AquaTunnel
- AquaPurge
- Chisel
- GhostPoster
- GachiLoader
- Kidkadi
- Rhadamanthys

- CVE-2025-55182
- CVE-2025-43529
- CVE-2025-14174
- CVE-2025-59718
- CVE-2025-59719
- CVE-2025-40602
- CVE-2025-23006
- CVE-2025-20393

- UNC6600
- UNC6588
- UNC6603
- UNC6595
- UNC5342
- UAT-9686

Insights

Operation MoneyMount-ISO is a Russia-linked phishing campaign delivering Phantom malware via fake payment lures and ISO files.

SonicWall has patched **CVE-2025-40602** after attackers actively exploited the flaw and chained it with **CVE-2025-23006** to escalate privileges and gain unauthenticated root-level remote code execution on SMA 1000 series appliances.

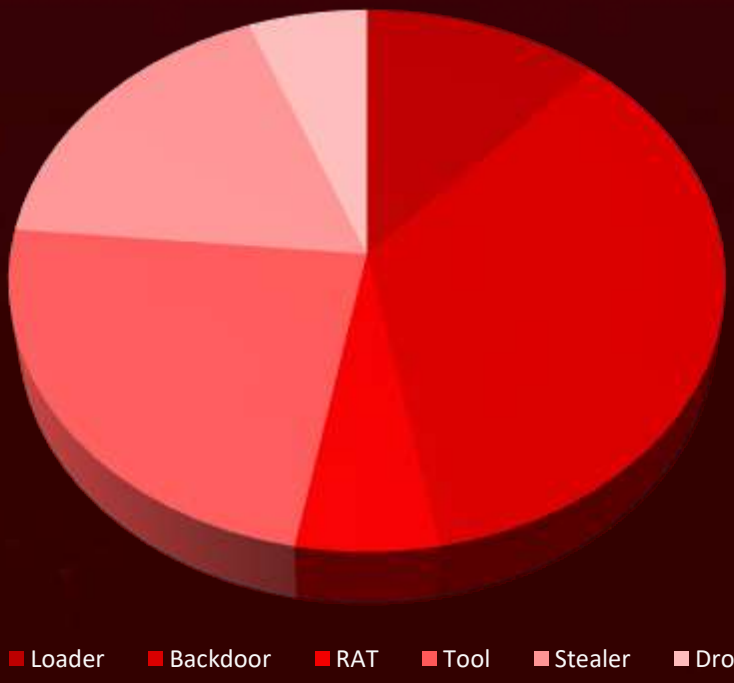
CVE-2025-20393 is a critical zero-day in Cisco AsyncOS, actively exploited by China-linked APT **UAT-9686** for unauthenticated root access, with no patch available.

Apple has rushed out emergency patches after attackers began actively exploiting two WebKit zero-day flaws, **CVE-2025-43529** and **CVE-2025-14174**, highlighting the immediate risk to users.

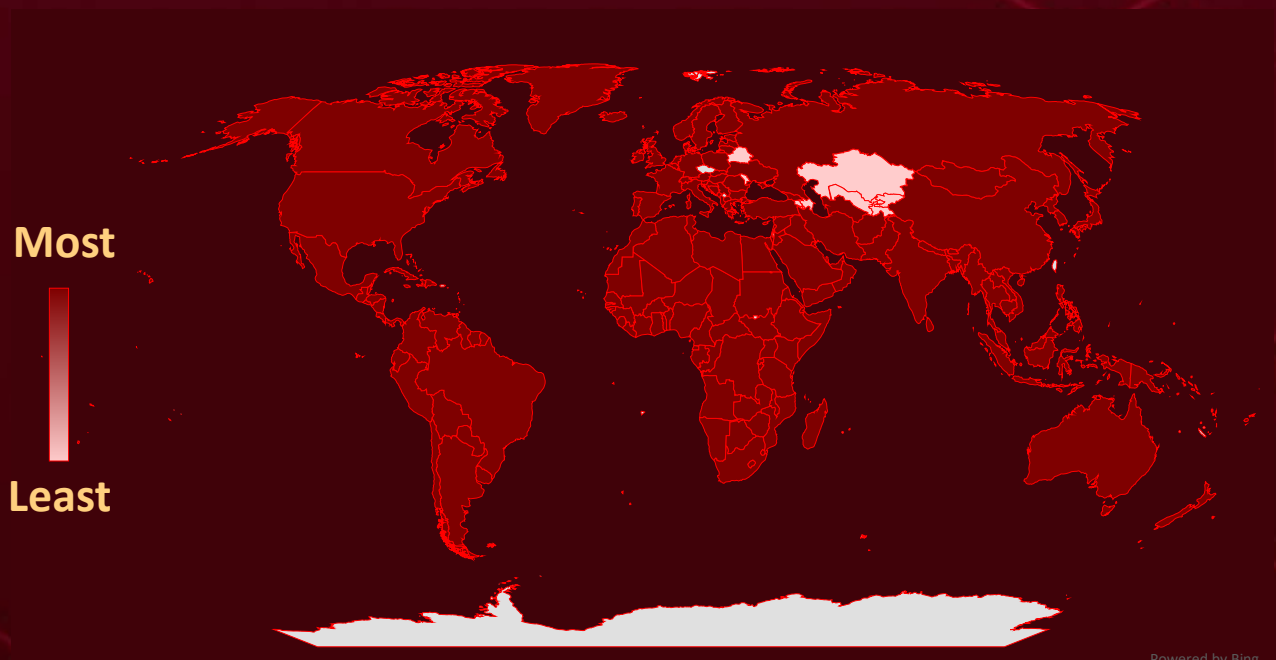
Apple has issued emergency updates to contain active exploitation of two WebKit zero-days, **CVE-2025-43529** and **CVE-2025-14174** reinforcing how quickly browser flaws can translate into real-world risk.

GachiLoader is a Node.js–based loader abusing compromised YouTube accounts to distribute the Rhadamanthys infostealer at scale.

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
Pakistan	Barbados	Mauritania	Holy See
Liechtenstein	Namibia	Cabo Verde	Serbia
Spain	Belgium	Monaco	Honduras
Albania	North Korea	Cambodia	Sierra Leone
Montenegro	Belize	Mozambique	Hungary
Algeria	Paraguay	Cameroon	Slovakia
Samoa	Benin	Nepal	Iceland
Andorra	Russia	Canada	Solomon Islands
Turkey	Bhutan	Niger	India
Angola	Senegal	Central African Republic	South Africa
Malta	Bolivia	Norway	Indonesia
Antigua and Barbuda	Somalia	Chad	South Sudan
New Zealand	Bosnia and Herzegovina	Panama	Iran
Argentina	Sudan	Chile	Sri Lanka
Portugal	Botswana	Philippines	Iraq
Australia	Togo	China	State of Palestine
Singapore	Brazil	Republic of Congo	Ireland
Austria	Ukraine	Colombia	Suriname
Syria	Brunei	Saint Kitts & Nevis	Israel
Bahamas	Yemen	Comoros	Switzerland
Uruguay	Bulgaria	Sao Tome & Principe	Italy
Bahrain	Luxembourg	Congo	Tanzania
Malawi	Burkina Faso	Seychelles	Jamaica
Bangladesh	Maldives	Costa Rica	Timor-Leste
Mexico	Burundi	Slovenia	

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1071** Application Layer Protocol	**T1027** Obfuscated Files or Information	**T1588.006** Vulnerabilities
T1140 Deobfuscate/ Decode Files or Information	**T1588** Obtain Capabilities	**T1059.007** JavaScript	**T1068** Exploitation for Privilege Escalation	**T1071.001** Web Protocols
T1057 Process Discovery	**T1070** Indicator Removal	**T1555** Credentials from Password Stores	**T1082** System Information Discovery	**T1588.005** Exploits
T1497 Virtualization/ Sandbox Evasion	**T1555.003** Credentials from Web Browsers	**T1189** Drive-by Compromise	**T1041** Exfiltration Over C2 Channel	**T1036** Masquerading

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Snowlight	A lightweight Linux loader used to stage and deploy additional payloads. Commonly observed executing follow-on implants such as VSHELL and establishing persistence via system services or cron jobs.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Loads other payloads	Meta React Server Components
Loader			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
UNC6586, CL-STA-1015			
IOC TYPE	VALUE		
SHA256	a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Vshell	A lightweight Linux webshell and backdoor providing remote command execution. Often deployed alongside SNOWLIGHT for interactive access and lateral movement.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://nextjs.org/blog/CVE-2025-66478
CL-STA-1015			
IOC TYPE	VALUE		
SHA256	4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b		

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
Noodle RAT	Noodle RAT (aka ANGRYREBEL.LINUX) is a Linux RAT associated with DPRK-linked activity, providing remote command execution and persistence. Frequently observed masquerading as legitimate system components.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Command Execution	Meta React Server Components
RAT			
ASSOCIATED ACTOR			PATCH LINK
UNC6595			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
SHA256	33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
KSwapDoor	A stealthy Linux backdoor disguised as a kernel-related service, using encrypted communications and peer-to-peer-style C2. Designed for long-term persistence and evasion.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
SHA256	1f3f0695c7ec63723b2b8e9d50b1838df304821fcb22c7902db1f8248a812035		

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
Auto-color	A backdoor masquerading as a legitimate PAM or system library. Enables remote command execution and persistence while blending into normal system processes.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43, 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Minocat	A tunneling tool used to expose internal services and maintain remote access. Commonly deployed post-exploitation to bypass network segmentation and firewall controls.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		Expose Internal Services	Meta React Server Components
Tool			
ASSOCIATED ACTOR			PATCH LINK
UNC6600			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
SHA256	776850a1e6d6915e9bf35aa83554616129acd94e3a3f6673bd6ddaec530f4273		

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
Compood	A custom-built backdoor enabling remote command execution and persistence. Often deployed in targeted intrusions rather than mass exploitation campaigns.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC6588			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
IPv4	45[.]76[.]155[.]14		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Hisonic	A lightweight Linux backdoor used for sustained access and execution of attacker-supplied commands. Typically observed in conjunction with other implants during advanced intrusion campaigns.	Exploiting Vulnerability	CVE-2025-55182
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Meta React Server Components
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC6603			https://nextjs.org/blog/CVE-2025-66478
IOC TYPE	VALUE		
SHA256	df3f20a961d29eed46636783b71589c183675510737c984a11f78932b177b540, 92064e210b23cf5b94585d3722bf53373d54fb4114dca25c34e010d0c010edf3		

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
Phantom	Phantom Stealer is promoted as an 'ethical hacking' tool for 'educational purposes' and is sold using a pricing model ranging from $70 to $700. Once installed and executed, it gathers extensive system information, including The Windows version, hardware details, browser cookies, passwords, card data, images, and documents are sent to attackers through channels like Telegram, Discord, or SMTP, containing the stolen data.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	4b16604768565571f692d3fa84bda41ad8e244f95fbe6ab37b62291c5f9b3599		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SantaStealer	SantaStealer is an emerging malware-as-a-service (MaaS) information stealer that is being actively promoted across Telegram channels and Russian-speaking underground hacker forums. Marketed as a rebranded evolution of the earlier BluelineStealer project, the malware features a modular, multi-threaded architecture that allows operators to flexibly expand its capabilities. Its primary focus is on harvesting sensitive documents, login credentials, cryptocurrency wallet data, and information from popular applications such as Telegram, Discord, and Steam.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Steal Data	Windows
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1a277cba1676478bf3d47bec97edaa14f83f50bdd11e2a15d9e0936ed243fd64, abbb76a7000de1df7f95eef806356030b6a8576526e0e938e36f71b238580704		

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
AquaShell	Custom Python-based backdoor developed by UAT-9686 that embeds itself into existing web server files on Cisco AsyncOS appliances. It passively listens for specially crafted unauthenticated HTTP POST requests, decodes incoming payloads using a proprietary algorithm combined with Base64, and executes arbitrary commands in the system shell with root privileges. The implant is designed to blend with legitimate application code, enabling persistent remote access that survives reboots and standard remediation efforts.	Exploiting Vulnerability	CVE-2025-20393
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Cisco AsyncOS Software (physical and virtual appliances)
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UAT-9686			-
IOC TYPE	VALUE		
File Path	/data/web/euq_webui/htdocs/index.py		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AquaTunnel	GoLang-compiled reverse SSH tunnel implant derived from the open-source ReverseSSH project, previously associated with Chinese APT groups including APT41 and UNC5174. It establishes outbound SSH connections from compromised systems to attacker-controlled infrastructure, effectively bypassing perimeter firewalls and NAT configurations. The tool provides UAT-9686 with reliable encrypted remote access channels for long-term persistence on targeted Cisco email security appliances.	Exploiting Vulnerability	CVE-2025-20393
		IMPACT	AFFECTED PLATFORM
TYPE		Extended Persistence	Cisco AsyncOS Software (physical and virtual appliances)
Tool			
ASSOCIATED ACTOR			PATCH LINK
UAT-9686			-
IOC TYPE	VALUE		
SHA256	2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef		

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
AquaPurge	Specialized anti-forensics utility deployed by UAT-9686 to systematically erase evidence of intrusion activity from compromised systems. It leverages the egrep command with inverted matching to filter out log entries containing attacker-specified keywords, then overwrites the original log files with sanitized versions. This selective log manipulation complicates incident response investigations and allows threat actors to maintain stealth on compromised appliances.	Exploiting Vulnerability	CVE-2025-20393
		IMPACT	AFFECTED PLATFORM
TYPE		Erase Traces, Maintain Stealth	Cisco AsyncOS Software (physical and virtual appliances)
Tool			
ASSOCIATED ACTOR			PATCH LINK
UAT-9686			-
IOC TYPE	VALUE		
SHA256	145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Chisel	Open-source tunneling tool legitimately used for penetration testing but weaponized by UAT-9686 for malicious lateral movement operations. It creates TCP/UDP tunnels encapsulated within HTTP connections over a single port, enabling attackers to proxy traffic through compromised edge devices into internal network segments. The tool's legitimate origins and encrypted communications make detection challenging without behavioral analysis of network traffic patterns.	Exploiting Vulnerability	CVE-2025-20393
		IMPACT	AFFECTED PLATFORM
TYPE		Lateral Movement	Cisco AsyncOS Software (physical and virtual appliances)
Tool			
ASSOCIATED ACTOR			PATCH LINK
UAT-9686			-
IOC TYPE	VALUE		
SHA256	85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc		

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
GhostPoster	GhostPoster is a stealthy malware that abuses trusted Firefox extensions to compromise users at scale by concealing malicious JavaScript within PNG logo files using steganography. Once deployed, the final payload quietly manipulates browser behavior for financial gain, hijacking affiliate links, injecting tracking code, stripping security headers, bypassing CAPTCHA protections, and embedding hidden iframes, effectively converting the victim's browser into a covert monetization engine without the user's awareness.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Malicious browser extension–based		System Compromise, Code Execution	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GachiLoader	GachiLoader is a newly identified and heavily obfuscated malware loader written in Node.js, designed to deploy multiple malicious payloads on compromised Windows systems. In the observed campaign, its primary function is to act as an initial delivery mechanism for the Rhadamanthys information stealer.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Loads Other payloads	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	00bcfecad4b679f72c50cbdcd883caf55b6a1f641258a636317871c7b8940156, 00db4aa911e95ecfafa6f10ebfeb9f0a8051ee63de51ea1d9515ece5be2a294b		

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
Kidkadi	Kidkadi is a notable malware loader that stands out for its use of a novel PE injection technique, abusing the Windows loading process to deceive the system into loading a malicious executable directly from memory in place of a legitimate DLL. This approach allows the malware to execute without writing a traditional payload to disk, significantly reducing its visibility and making detection and analysis more challenging.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Drops other payloads	Windows
Dropper			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	01bdbb37d4b5d22ab98f1977f89c0eb69b35cdbf1d690c434a9d21dc1d0c56b0, 02bdf8a8206b520db3d55fb7426ecef1ad10518f22eba26c848e548b75bc9999		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Rhadamanthys	Rhadamanthys is an advanced infostealer distributed via multi-stage loaders. It collects credentials, system data, financial information, and browser data. It uses obfuscation and underground updates to bypass defenses.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Windows
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
URL	hxxp[:]//176[.]46[.]152[.]18[:]8181/gDatFeDway/r26ggaap[.]dssde,		

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 PRODUCT	ASSOCIATED ACTORS
CVE-2025-14174	ZERO-DAY	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac), iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium Out of Bounds Memory Access Vulnerability	**CWE ID**	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-122	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://www.google.com/intl/en/chrome/?standalone=1, https://support.apple.com/en-us/100100, https://support.apple.com/en-us/125892, https://support.apple.com/en-us/125886, https://support.apple.com/en-us/125885, https://support.apple.com/en-us/125884, https://support.apple.com/en-us/125892, https://support.apple.com/en-us/125889, https://support.apple.com/en-us/125890, https://support.apple.com/en-us/125891

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-55182</td><td>React2Shell</td><td rowspan="3">react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack versions: 19.0.0, 19.1.0, 19.1.1, 19.2.0
Next.js versions: 14.3.0-canary.77+, 15.x, 16.x (before 16.0.7)
React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc</td><td rowspan="3">UNC6600, UNC6588, UNC6603, UNC6595, UNC5342</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:*
cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:*
cpe:2.3:a:remix:react_router:*:*:*</td><td rowspan="2">Snowlight, Vshell, Noodle RAT, KSwapDoor, Auto-color, Minocat, Compood, and Hisonic</td></tr>
<tr><td rowspan="2">Meta React Server Components Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter</td><td>https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-43529	 ZERO-DAY	iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use-After-Free WebKit Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/100100 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125886 , https://support.apple.com/en-us/125885 , https://support.apple.com/en-us/125884 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125889 , https://support.apple.com/en-us/125890 , https://support.apple.com/en-us/125891 , https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-59718	✗	Fortinet Fortios Before 7.0.18, Before 7.2.12, Before 7.4.9, Before 7.6.4; Fortinet Fortiproxy Before 7.0.22, Before 7.2.15, Before 7.4.11, Before 7.6.4; Fortinet Fortiswitchmanager Before 7.0.6, Before 7.2.7	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	-
Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-347	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol, T1556 Modify Authentication Process	https://www.fortiguard.com/psirt/FG-IR-25-647

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-59719	✗	Fortinet Fortiweb Before 7.4.10, Before 7.6.5, Before 8.0.1	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*:*	-
Fortinet FortiCloud SSO Login Authentication Bypass	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-347	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol, T1556 Modify Authentication Process	https://www.fortiguard.com/psirt/FG-IR-25-647

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-40602	✗	SMA1000 12.4.3-03093 (platform- hotfix) and earlier versions, 12.5.0-02002 (platform-hotfix) and earlier versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Missing Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862, CWE-250	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-23006	✗	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and Earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:sonicwall:sma1000:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Deserialization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059 Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20393		Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM): All Cisco AsyncOS versions (physical and virtual appliances)	UAT-9686
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:secure_email_and_web_manager_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_and_web_manager:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_gateway:-:*:*:*:*:*:*:*	AquaShell, AquaTunnel, AquaPurge, and Chisel
Cisco Multiple Products Improper Input Validation Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6600	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	MINOCAT	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6588	-	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	COMPOOD	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6603	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	HISONIC	Meta React Server Components

TTPs

TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6595	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	ANGRYREBEL.LINUX	Meta React Server Components

TTPs

TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC5342	Korea	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-55182	-	Meta React Server Components

TTPs
TA0010: Exfiltration; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059.004: Unix Shell; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1496: Resource Hijacking; T1567: Exfiltration Over Web Service; T1036: Masquerading; T1505.003: Web Shell; T1053: Scheduled Task/Job; T1552.001: Credentials In Files; T1552: Unsecured Credentials; T1102: Web Service; T1053.003: Cron; T1543.002: Systemd Service; T1543: Create or Modify System Process; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1070.006: Timestomp; T1070: Indicator Removal; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1090: Proxy; T1568: Dynamic Resolution; T1568.003: DNS Calculation; T1505: Server Software Component

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-9686	China	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-20393	AquaShell, AquaTunnel, AquaPurge, and Chisel	Cisco Secure Email Gateway (SEG) & Cisco Secure Email and Web Manager (SEWM)
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0011: Command and Control; TA0003: Persistence; TA0005: Defense Evasion; T1203: Exploitation for Client Execution; T1140: Deobfuscate/Decode Files or Information; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1090: Proxy; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.006: Python; T1505.003: Web Shell Server; T1505: Software Component; T1070.002: Clear Linux or Mac System Logs; T1070: Indicator Removal; T1572: Protocol Tunneling; T1095: Non-Application Layer Protocol; T1027: Obfuscated Files or Information			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploitable vulnerabilities** and block the indicators related to the threat actor **UNC6600, UNC6588, UNC6603, UNC6595, UNC5342, UAT-9686,** and malware **Snowlight, Vshell, Noodle RAT, KSwapDoor, Auto-color, Minocat, Compood, Hisonic, Phantom, SantaStealer, AquaShell, AquaTunnel, AquaPurge, Chisel, GhostPoster, GachiLoader, Kidkadi,** and **Rhadamanthys.**

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

- Run a Scan to discover the assets impacted by the **eight exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **UNC6600, UNC6588, UNC6603, UNC6595, UNC5342, UAT-9686,** and malware **Snowlight, Vshell, Noodle RAT, Auto-color, Minocat, Phantom, SantaStealer, GachiLoader,** and **Rhadamanthys** in Breach and Attack Simulation(BAS).

Threat Advisories

Google Chrome Zero-Day Exploited in ANGLE Graphics Engine

React2Shell Flaw in React Server Components Under Active Attack

Phantom Stealer Hidden in Fake Bank Confirmations

SantaStealer: An Emerging MaaS Infostealer Ahead of Its 2025 Debut

Apple WebKit Zero-Days Exploited in the Wild

Fortinet Authentication Bug Sparks Rapid Exploitation

SonicWall SMA Flaw Leads to Unauthenticated Root Access

CVE-2025-20393: Critical Cisco AsyncOS Zero-Day Actively Exploited

GhostPoster: A Multi-Stage Malware Campaign Hiding Inside Firefox Extensions

GachiLoader Deployed via the YouTube Ghost Network

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
Snowlight	SHA256	a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665, 18c68a982f91f665effe769f663c51cb0567ea2bfc7fab6a1a40d4fe50fc382b, 1a3e7b4ee2b2858dbac2d73dd1c52b1ea1d69c6ebb24cc434d1e15e43325b74e, 1cdd9b0434eb5b06173c7516f99a832dc4614ac10dda171c8eed3272a5e63d20, 1e31dc074a4ea7f400cb969ea80e8855b5e7486660aab415da17591bc284ac5b, 2b0dc27f035ba1417990a21dafb361e083e4ed94a75a1c49dc45690ecf463de4, 2ca913556efd6c45109fd8358edb18d22a10fb6a36c1ab7b2df7594cd5b0adbc, 4ff096fbea443778fec6f960bf2b9c84da121e6d63e189aebaaa6397d9aac948, 55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864, 62e9a01307bcf85cdaeecafd6efb5be72a622c43a10f06d6d6d3b566b072228d, 7d25a97be42b357adcc6d7f56ab01111378a3190134aa788b1f04336eb924b53, 7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a, 9c931f7f7d511108263b0a75f7b9fcbbf9fd67ebcc7cd2e5dcd1266b75053624, ac2182dfbf56d58b4d63cde3ad6e7a52fed54e52959e4c82d6fc999f20f8d693

Attack Name	TYPE	VALUE
Snowlight	SHA256	ac7027f30514d0c00d9e8b379b5ad8150c9827c827dc7ee54d906fc2585b6bf6, b38ec4c803a2d84277d9c598bfa5434fb8561ddad0ec38da6f9b8ece8104d787, bc31561c44a36e1305692d0af673bc5406f4a5bb2c3f2ffdb613c09b4e80fa9f, bf602b11d99e815e26c88a3a47eb63997d43db8b8c60db06d6fbddf386fd8c4a, d704541cde64a3eef5c4f80d0d7f96dc96bae8083804c930111024b274557b16, d9313f949af339ed9fafb12374600e66b870961eeb9b2b0d4a3172fd1aa34ed0, E2d7c8491436411474cef5d3b51116ddecfee68bab1e15081752a54772559879
	IPv4	115[.]42[.]60[.]223
Vshell	SHA256	4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b
Noodle RAT	SHA256	33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f
	URL	hxxp[:]//146[.]88[.]129[.]138:5511/443nb64
	IPv4	192[.]238[.]202[.]17
KSwapDoor	SHA256	1f3f0695c7ec63723b2b8e9d50b1838df304821fcb22c7902db1f8248a812035
	IPv4	140[.]99[.]223[.]178
Auto-color	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43, 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4, 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a633, a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d53d0a, bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f02d6b, e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc3048f7, 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042bb255, bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b051510d1ca
Minocat	SHA256	776850a1e6d6915e9bf35aa83554616129acd94e3a3f6673bd6ddaec530f4273
Compood	IPv4	45[.]76[.]155[.]14
Hisonic	SHA256	df3f20a961d29eed46636783b71589c183675510737c984a11f78932b177b540, 92064e210b23cf5b94585d3722bf53373d54fb4114dca25c34e010d0c010edf3

Attack Name	TYPE	VALUE
Phantom	SHA256	4b16604768565571f692d3fa84bda41ad8e244f95fbe6ab37b62291c5f9b3599
SantaStealer	SHA256	1a277cba1676478bf3d47bec97edaa14f83f50bdd11e2a15d9e0936ed243fd64, abbb76a7000de1df7f95eef806356030b6a8576526e0e938e36f71b238580704, 5db376a328476e670aeefb93af8969206ca6ba8cf0877fd99319fa5d5db175ca, a8daf444c78f17b4a8e42896d6cb085e4faad12d1c1ae7d0e79757e6772bddb9, 5c51de7c7a1ec4126344c66c70b71434f6c6710ce1e6d160a668154d461275ac, 48540f12275f1ed277e768058907eb70cc88e3f98d055d9d73bf30aa15310ef3, 99fd0c8746d5cce65650328219783c6c6e68e212bf1af6ea5975f4a99d885e59, ad8777161d4794281c2cc652ecb805d3e6a9887798877c6aa4babfd0ecb631d2, 73e02706ba90357aeeb4fdcbdb3f1c616801ca1affed0a059728119bd11121a4, e04936b97ed30e4045d67917b331eb56a4b2111534648adcabc4475f98456727, 66fef499efea41ac31ea93265c04f3b87041a6ae3cd14cd502b02da8cc77cca8, 4edc178549442dae3ad95f1379b7433945e5499859fdbfd571820d7e5cf5033c, 926a6a4ba8402c3dd9c33ceff50ac957910775b2969505d36ee1a6db7a9e0c87, 9b017fb1446cdc76f040406803e639b97658b987601970125826960e94e9a1a6, f81f710f5968fea399551a1fb7a13fad48b005f3c9ba2ea419d14b597401838c
	IPv4:Port	31[.]57[.]38[.]244:6767, 80[.]76[.]49[.]114:6767
AquaShell	File Path	/data/web/euq_webui/htdocs/index.py
AquaTunnel	SHA256	2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef
AquaPurge	SHA256	145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca
Chisel	SHA256	85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc
	IPv4	172[.]233[.]67[.]176, 172[.]237[.]29[.]147, 38[.]54[.]56[.]95

Attack Name	TYPE	VALUE
GachiLoader	SHA256	00bcfecad4b679f72c50cbdcd883caf55b6a1f641258a636317871c7b8940156, 00db4aa911e95ecfafa6f10ebfeb9f0a8051ee63de51ea1d9515ece5be2a294b, 01a3da42f74578c0b7c1146f30eceb2a2bc26c2d814a48fcf29ae527a1048aff, 028711c1b435c773ba600a863f4d4a2d1218860de799a1275d15d4ea93f0cbef, 02c0de5116d9b05d930e4858cd9768cc2ba70e91be62690439537fdf0f52de53, 032a297bfbdc94226f0d88c77ab27148c54ebde6bfa2750fed09b1d8667ddcd6, 03d55245ef2766943813c0d1eaa3859d3918ee6fed2705bb5eeb38f4f87a5643, 079a180eeed0f4fc84c2412ba0398a79c5262efa1d9e8fd53290cd001b5abf9f, 094240cd298de1121da36adb96b3cdd632f866837f27e3951b6a0a544e5437f6, 0a6d41411ef3c65540a525dc5c3ab0964cd595aa73c3a477a8a96ec986277660, 0bd44592e75854a1c763384bf9dcea6dfe1174f6f45df342ebd9dfaa3a27dc85, 0c03845b9e2ff5ddac56f6e75b8e9dadf1a7bd1681d074e732478596b3173922, 0f81656ce724b65c230c4d63259c3a0edff20cc664de964f16451417eda60005, 14bfaf75b5c7ffac451f41352f8e94b6cc060efe7d645189795fa921f4e602bc, 16b2f7d9d4ace9e3004bd47f97c252a7fea21662656ec6b906d30a6b21900fc4, 18649874ab887ab613a3ccdd7cddc683e2b21f7cbe0762d2ce8201fc7e57540c, 1d28c23b271eb2156bf2780cb0dd042573f38f4758ef61877a7347bbbc756c8b, 1ebeca5dc62d759904c47597ebeb67865017a99892081c94d7647206b78a6cd2, 1f35a5ee4ead5c286f3e0d3ddecaf8789f12da7b8b7422b0511af619353284b7, 2038f38ccd42cd1df84abfb5915e3a6eb9c976b8d822768068343716f46a09f1, 210d821109ec1dff3b92ad3cfdde59912581327f4017b754864ba1e263c3c366, 2601d2c2b4515d3f1414d4543cfe2091490e2502457eab6c437a310f7e5e2a1a,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	266216b097561e57448b940c3087b82c4cea7581b67e5dcc52c8c4dfcbbf8333, 278c5a0acd6603947e59e1961642279e29cc4b9be299c8edb7b719d6568eb8da, 29fac0ce48b9114990a4dd942d6de1da55bf9c49938929123fb1f221be385eff, 2a87f4d47ad95f4eb46c08a4d33fd4732c10a1408db1b758871dfe6b1059c6bb, 2e5389a32a6c21fec476fdc6e80fcb577de31c43adb7c090c3a11f3b048787ed, 2fee47e12ca72863ee132d63dcac3b39aeace1a4d71b0aa14a30b56ecabf29c9, 30bcfa6bbb5e9d9bc64c65a27e1565a9ad21af3d5e1f202933a340cc400abdb9, 3124fe59b26dc77c1e4b4d615112928ca1830c890c8c77e853ac6948069ba463, 3151700d8f13cf55ad46148cd46ccb0b3409c0adf253433f16ef6612e9280eb2, 31dac5bc21b0dabfac51cb99c821e62421c39949971a44898a1ec15efe33e8c4, 32855dba1ec6b3c9ba422cf9203d8130e59dcb5235764b8f56b6d02970a5e5b5, 33dce93dfdb43f47ef1d36e2dd16725ed365300c371dc45491b52afe13b6e412, 3630538febdedf693ca9d996c3f1998d50c97052ab99e653d95b381ddb3546ef, 38a7feb5ab611e6a487ce8b048732f7721484ceebb316fd34c9cc611dbc4e3cc, 38ac7917ce895448203e6d14f121850ecc4ff89f530e792c794d771f881c7b07, 3c16548ab32996a58298978b20db1d4133827298e166f93b7c943dc3ffc51782, 3d8c1469de3bb01ef72992e07d1feea938018398332757697885 1b8c78ea7fc9, 3ed63941e7411e93f644a064094b5a6c7e2a9547840a5198dd7f6b4d45ef9eea, 401e7b72f4b7ed4119b625ab34c2c7d37c0dabc08bbdf943fd291445e2fe753c, 40f899294ea02f7a9823ada63c869ede18a8afc6238aedb62d2b30a2744cb846, 4210e9e1df0bc41e497285483782609c0b4777ef6682fb40b0d25c8149c9f3d2, 428f86204b69f31dfc3f3479d18d23b15cad63d72998a8418e8da22941c74956, 43b1a11962f83db6bb59bb7467d5456e852d0421ca5eaeae3a249a34839e67b4, 43d9130c8f077a5885842bda24bee19e4dd231c49f88629442e5b9f02ff5f33a,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	45fd42669157357f1e16c0b542eab5836061f5b2e2160a5104a4bde38cac85bf, 47ab9b9deaa14202b94320df16f52c8d98adee49c9bff8909ab5deefcbdfe401, 48a269d2c083868e2b5347012afb85bb3c233c9f042985bcab764f7788316660, 4b71d8cb7ce8de8d557283df3543aa2aed89dd5446c7acf855c0ea2e5e7e89dd, 4be48937c603c910c29de2af3b0d3e3bc05b809b19190e90ade2489a347d8b03, 4ed90af2fb3fe13eb8ab69fe2fcd82a0775426da33da4ba043d7e7e2fd4a18f7, 4f8c55cb3f99741f4fcccdbcff07c7d0b8ab7fa23dcbf8847d7a37a35f6d3f5e, 4f95af5b4a1569eb54f6995e547584f429a49895d0d81c71d74970275b170a08, 5173c6b57642dd89dba2f039a1ad630d6d73d3557248dd09ca2a51a329e6119e, 53ac3b1601f2fa43121cfd43ac9b49f6751a8b84b4ffcc5a1241f71eb1e8d7b8, 5538d6f24e1330c934cdfc95188aede5c9668154376e507c41fe1c752cdd7a5b, 561436df09f87be34317eeb25a2b7bf5c67201fa501262f72a9a63b9977ae217, 59c93f81063e8b77b20292d1d03598f74d997690aac41f5fb7a248ac8ad866c2, 5c88a6efd0a713460dcf8b828575285be3a43d6481e245662bafb3472d344dd1, 5d1bf72af319901f22d78625d60c877d7a8d6c54bbbcbcfc643376558e176211, 5dbdd6d45021383a3c76b2e0c7258a7b0fcfd70904602eb2fb1afe3b33efc80e, 60de97fff85ba6f0b114fe565f53ffc1ef43a19de95c31299884e034f05dc037, 616b74a6b17b70bae357c43cf03fe1946abc36eea1d0e7d911ca29bd067f63ae, 61e215ccf73cba014ecd72abd38ff78d5a23c2727577c5b3e2c8f52b90dc2a4a, 62bab101900a92db76e2c368c4a83f7340f42c460b16d11dea94c8db002d5bc9, 62bcb939df4a8b7bdc896cd229cf34f55d93555c14e5816ac2aa6285d1cf4112, 6463e7f48f01f482fa846bc106de245c833ad7c3ea7fae4caa7ead54b2901cb9, 64d6d018e3b7a1d718b96d9950b3579af2a784ab004ad575e13cb41b2c27aa25,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	66e684ab10b1daf2a46df1031c6ddc331ab80af4e21144a68997d4a1859e9fd7, 6985717a754fe121e99c337cc33b0e9a25852fa33c580dc9caaffefaf0908233, 69c0084b78bf963997033759fa45933b61de425aea7612a06289ec6c78492745, 6a8dd64af57926514131efdc388c9883db2c23aebfd8b97c44e808d637f0fc23, 6b80c4fa88fbb35af2b254c63586fd6e0455d0e917b842afc79b821ac87a2b9d, 6c428016506c2ae076d049deeba60514cb8c0afa6fd00fc349722cdbc6e1b305, 6d5af67f05c9db6763cd494f64c5f62faeb8f1b67ba26a7ab278e27d4c9b8f22, 6f1b97838bc5702954ef5f536de86a8477e0008f25bcfba72b7fda4c1f37b9d2, 6fcd071c6ab51e71407e8bf242fac8552a10aedff113c9efb92ccc53cc49fbed, 7029d2c60ee04772d9dc4d8d34f5effd3e3be17769584bbf912954e926280131, 71415238f740c7528f3314f94dc07ffd9b802a34c3997b09ad02da1bcd3c8137, 717f05b96a344b1fdd159b4c45e3089a26d1f64e63cd4ac2ed3bf2db33074c3a, 765041cdf97bf0b55734cd5619d7d4568a641ae3fc35540344a488184839674b, 78908b01a8d959b80f7fa1f42c734c4c64a8cec58394f94cf362b8efd38c7b9c, 78b6c96910d8f1e3889bad17f97cd26aed5f6c7a15432cc11c2224a8c9adf691, 7a155a20c1e5df83b566fdad3bf59ca49ac6559e0561233a95c7cd70a5caa6dc, 7db2025192f4f2497bdc356c1920dfc4740bb868de8a6b5786f01865dfa9e564, 825bd0b103d647c296bd2b9eee251b04b7f5dc72f27898fcf0fc25ca24587125, 8295cddaf1c23d554b90e4d1ee1ca064f68124df63003a046f58241c3513cd1e, 8383a421e9a4f55af53cf1911680042659b28722cff8a30cd202bc728a8fea23, 8443994a687269f2d7d19678e571ce1a1658df7da69c25b4bd902f87f849c98d, 857f68127546f829861e796b11b80304e2c53e70e54191fec8087f64d7c8146d, 86082a735440124bae953c0a68e5eff6a7fe6792f90ea1e71cc0c83a724bc273,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	87c1c62369657904418affebca3f706a4e968dd1a672729274ba287dfae43be4, 88938ad37225074c923ac4baa0b4a171076c273cb064a4905c66a25ca3acfee0, 8d473631c12231079a241d63ddc9e4b537d2531135e9aa4d795abf22f2aefd39, 8db4cf8f666b7c4ec5051139570b5d3b88569c9e62de31249a70b6cdc716aecd, 9211d6fb5db70a51ba5795e0a7126aa1efd0f4b78262031dfb72e98c319ce37e, 95760397b9cc05d0180258afee22cd8e6bc997e13754a11cb737733d0beeb444, 95f875c01b889f9ba811dae11822c6c83eb28d8260f16ca070c76e83f6f7e7cb, 96d2c11dd5bb43da5945259494d7e26a68b5c48eaa32d5eb2d1dc61aa0dfb7fe, 980d0d78b3e288f24bcb793d2e49a4e26138cfe4ef272171557658be751d277d, 99a3a973caf956102c563773a9a58ff79c539c7c77480873dd0e09fa259b3594, 99cc25edbc65ea201b957abbd6cfbd7b3b6f04759cbb47fc999d35508a654748, 9a0ccafc516df1e931ba2028ea59f39b31e1cc812c3a2ab1765b9e91fb8cc507, 9a28d80ce2c191d743554313edbb8eef09e6f72b34c4d701c0a84090d61264e9, 9b60930efa096a98d9fb6392c74f8d3e5f2df6ba8a5b31a304b7fac3d847e7f1, 9c562c28323e7681c1cb5a4b23e703c21cda8bc020946de691b6765fcb613a16, a9ec251b719b2ebb85e50f43eea4e2944e0a065daaf5c92420efc852b594d96f, ad27bfdd9d51f81e6e743ed351c47812874565e89f6ace03ac39d6c85fefa949, af0891bff41d67815ed7a979fc2127295ea662079afa16d09d1a377684d678ba, b1b72689afa038d413e36f5aca61b971b69e4e411976cbd01e3cbf5b2e83141e, b67ac42c0ef7402dd53dc950e8162e9a213aa65d5a7901a5cc4aee0b93058b93, b6a3ad06c57b45142dd7ac2c77ea70980296b5d168517f5d7ec4100ec10d305a, b8eaa5c0686fb49f6f3e4edd5716df48581001249d5e62563f2468db73526cce, bd378786d84743beb0adc8d3dd14ff3d7996caaf6a1eb8783c665091ee9ae225,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	bd7df13098f3984a18c4a21282ba04ed802bb73c1f91c7eb5a35b89544c545cb, bfd049ef7d1384a25c3edaf857b94539525b5f442dbe543fafa2356315780d8d, c164232a5a3a2b49705257e62c5f8e004df68e3cf32d7702e4af879abd55008b, c1a6587fb04a94943ab616cf0ce8b3d0c55e59ffbd4bc9b3a1add955391210ae, c1fb323ed08adca20912906e8756e6f8a805cd1d08cf20226f37cb51f33117eb, c4cd91a5ce722f3c510151513501e9aab54ad535b934132e6e6f6c9c76be2e9e, c50c73ef1be87b84055ee73bda503ad20884fcf67b207fa918190f40f4353729, c5e9eaaa5dc6ec4780c319c26a4f552f7030438dcfb008ccfd52358512dc3f81, c605642e0edac4b63e9819648f79d54d5f47cac240480fad808cbfb61f31c88a, c67bad311a48bb86a865b08ad2ef175a17e46063ef3c5de734fb3c4a5ea07578, ca0c525bf22b499b2f374d41f7e07a60ed9181645af485b0183c65eea68d364d, ca1465224a206c9323a4a3215afa402ce7f592ddf17db5d477d2a5905e982d56, cd6c1ebc720ba509967f9e508657ad02d8fafee1d958af0174bfd0d192291d0a, d2c3f54b03d50271dad1eba0abf1cad6529d67b74015e530f716bd18f943c6b5, d52894f027b8ce185efa3f584024b8a9a7f6694f6e294aba8ddac9789d00468f, d56afbac1b7eebdb1aa03744cb45a260975de75a08e7f4d9a89ccb57656d9b65, d5e05fa6ddbaf68f6b08e188d444b664a08a69a6102df37c4c3c3cbc7ebfd326, d5e530f607260ee2ce19ef3f6ac277b202cd15fc947b0c02ba9060421f799bc3, d64d4ede406cc439617a2f17e31a3d9c1adb81d35cbb97de1a7e0145b03a08cd, d666dcf48f569d6ba9defd87e149408373c0ac237a017624fd51aacfcfeb89d0, d66fb9cc2c40311df8af5aee664303f5226338cd0f2046cb2f8d8d42bda6f9b9, d737d53d2fb7a233b9732bfcd9c99ac8ef9846ad65af07cae490c8ffd9dc02ee, d858fd5207e758e84b7ea1a84f27b0e782d0cf3a39db9fd72c3869bd136f9440,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	d9133df2668bac02ab8150fe9bc7b44a69936322b624fdf80a4f0de635970e81, df481a8014760def4bdd933639d01e8381fed910f5cf6d0e974560afc446451b, dff27eb46d17a25416a9cbefb705d13ccaf8bbc03461f3112fd5132c6261a187, e111cbbc94fa932ad24e84cb308195ad7d05fa2d9bb2716a0f6f9c11a4c3f570, e17622f041536a253ab17dfc10011a65225356cb120970b4c4948df1c37ced23, e1d90617390211860b40839338c235df016cafeed7bdda9f39b17b86f48a9fe8, e37d2b812d6ce5653ee7c54157b6288469152dd64a4cb3cb25943bbc3b28e909, e6cdc47ab4a4496d42d84281d5d89c4fdad665cad0546e820aa29e9a18d454f2, e70516e7aa7c9dbfc459993516cde705685f1e44a75c29c55d9f71abe7733c78, eb3f6f8f99b86d4a68490e56a6f5a963523743685ecb6c8bd1d87389dbe0fde0, ed74747bb58f78df2c11f247cc173051cc0e058fad7def595d14b8ce03889a53, f09e67864cc19f5b831fde944c7ee917cbd3af9ff89ed4893d2fa441d12bf5d9, f25531eef40e268b251ce117375bbcaa1a586506d3fa56fa722b200713ee4c1b, f37df47e517702f3becf6e3c85733dfea0031572bf199c1f56faad951b354573, f566a942a7c59f53efd9418f0c97850a749a806ee84e88056138c699d3b4d08a, f624c81e47e350123490897fa04fe43886ae9cec9b128e8b9ef54fe9405b4612, f64a20a44a60dd899bf0cccb5de57897dd80819cd36c55878a56ed0d1c995352, f8a881216fce67e89b8a56774504b5ea86ebb763d87ff7426a9344d13790e7ea, f94c8771545fd31371dcdfbe80260378709e686b44c2b440957cb923aa952b37, f9bc90f545b3eb8d5bd963d00debc6f3ff22403f94f91d063f18a7fb85be59eb, fa1bd55fc9aecc625992448306e0dd456e4011bc07a926046ed6d3280aededae, fbfa7f980b0d29f8c12933ef68daff306e2cbec3247db8242a5d97e6a96927d7, ff02edab9a670769ce074b2f6d6728909950785d2c8507e01d3333de98156c58,

Attack Name	TYPE	VALUE
GachiLoader	SHA256	ff89d6917b775ef0bd38e4ee3a401bb310c4276eba79ff872b827920f72185b3, ffd7d43487fa1e15d8ea2a1e8737533cfcf7763cad6cb7504f270500a37f4261
	IPv4	94[.]154[.]35[.]99, 176[.]46[.]152[.]18, 213[.]209[.]150[.]104, 62[.]60[.]226[.]233, 66[.]63[.]187[.]72, 178[.]16[.]52[.]231
	Domains	davpniktonevidit[.]cfd, nupogodi[.]cfd, nexus-cloud-360[.]com, globalmarket247online[.]com, vault-360-nexus[.]com, iietrich[.]cfd, mceenzie[.]sbs, digitalservice365cloud[.]com
Kidkadi	SHA256	01bdbb37d4b5d22ab98f1977f89c0eb69b35cdbf1d690c434a9d21dc1d0c56b0, 02bdf8a8206b520db3d55fb7426ecef1ad10518f22eba26c848e548b75bc9999, 04bb04bbea55fa1dabda974b2c2f4aceb44ddccb7b9c1715e0aa67318369a768, 0577a28c0bcc1b033f44f458ab2d068fc301ef30d4175a3d2012d3601e9e13e1, 0859936dff1e2af60940c5f0764e187c642ffea5344118eb702a7ac59f5a9281, 08b5875f9867aa6c71cb8d96fb79de9f8975e0f7d1298388c95845aaa49e55de, 0ef9623e3ba8bc2c5be6de9cccd4a9e17bf74d1f8f83455da40c35f72fb34922, 110a17f1d65790337329d22d94ac10a9b6581202d5eab02897cb41ac543f1007, 13f1ee54ec2f7ca835313b828c64d1b0ffd6288c59e3361013a17c765da7335c, 178a24418d3057eb38b80e63786f9908a856618f1d19a9b667a55dff2717c9db, 20179c8ceeede0056b0d3f545d0641160490642c90b23dce5603b8b47acb62d0, 2101d91dc775638f1f392d0867aca9a15d9139f0c986ed7004df134c9c52fcfe, 254abb6da9296f8c6f8e567186e3d59ddba2392fa4baf791492f7e76b4ff5af7, 28a9a74d8eeae80de63a1938cadfa55a5a0f334e593e975cb32af8ec3cae79e6,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	2aea932e216145e38e5751f4daa9788974dd8e4ad4e90d7b426133d3df6341aee, 2e519a26e3cb67b9e1186065c4245f89b8cdfb5b3346fc86b028213e0f08c286, 2ed1c34780a3e9d2972f14d2828abf77a329075bd4c055458ef2f064237544b9, 354a66191805500b4a45d7455fd02527ffe0b76ae9285eabf8f182ea7d893c19, 38063272da02cf4fd383c634df988c07dcb2ce59cc3cdb036c4ff155fefc62e2, 38da058e5fafbdd9c371f4d64e7cc0e317ad1e59291470ddf01c7681c0c03c43, 3903bab79a2fa38e05df6f311d2dc9640c5916f8050bffab0d47ab8e58837210, 396caae9215849b674eecb0f8d5b91985f81986069c09e50454cb8f607ad4231, 39c72a4467ead5190ab2aff718c1d8fe66dd03760b3c2bb085466d56a6d10f3e, 39cdf78fdfeeb8ce82f5a8b0abbbfb1a74fd0bf9568e11a9b5f5d47060c33dc7, 3dbea0934dd2de6441ba27b762dc6424ce518f4882555fb96cd5225f9167339a, 405072e611a49489d1074dafcd84791f60ab9daebf55be36b924718e9d847c48, 416b81138d3c20578228c9610dca686eb7193e8d93cc4a2a18e6815efeacb810, 425d78b7a5cbd87b36e4ca991171e90851d0dac29fe5934fe9b289ea88793298, 46926ff7f778ea242603d233eabc0916a8a6945769fa0ea20c60cbac1f164150, 4a509f3605cb039c6f426e110b23ce82f1ef67db06c32e4bc5ebfb3ae3ca1e31, 4bdf84addb7e9bce6bb98086e6554f68fd529c49ae20b770d8db9ffc9debd3df, 4bf54789913bfbca6bb87263137ff6a662e32eb9e9ff124441af6304cc2b401e, 568e8082704d7fd2473862e93120412de1d043da5d106a12f9d1d5f1492eb173, 56e4bb0f077b2081f0fcdaeaa90d8c6da48beedfb0a381ae054030e5a2988f05, 574934eeab1d23c163c4e59cad869de2f5c3d46dbdd563b17fb4320b53e95770, 5982d92d6a3bd210fd13a9986bda7f9fc6cb0321e523506acf9dc2e9ee6501de, 59a17d129944bf8bc426d23746b285522d94b293eb2c2808d56a307022e5b92d,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	5a290d01a08f774f13f0991b7cf5c8c48b8cd2c0eb896ad069f02a474d8747f2, 5bd83b8ecfb1efd13191a76cb0998cf6d645491b76b6fe4f1a516bfd756bed3b, 5e4ae0bdc6081a22357e73aff3023a63623f3475610b23c35ff073b0b6890175, 6253d1285a7579f482ba1983a2c4db2c01f9f11194dac76aca4424e3d6977a02, 62db621c97bdaadffc1e900aac8d3af6e4e759b27018da635418c3921e1c8068, 679ff95c8c383d55b60d80d1803f347e206bd358e3980ee8de1de105680ffb37, 6bcb16d0ceae1b27bc7860477aa60a8c2a2588fb7625aa3a2dd78ee543658437, 6dc57007880918de4ef89d98b70dfa0cb1ac4c7a9d1eeffc57408d3f18524980, 6e087f40e4aac5fa780bfd1046c1d65e2b59c6abf391f9507718e61be61ddf42, 6edb286fa173145e8bb9597d8f02ec3d86f9f680468ba48618bcc5d2240ad121, 73cf316dc4359d80022e0ff7be22b9c86530e982a1d939e78a20090b9373b8a4, 77c728333ebff9d313d87b763b9d8e4a9d580b76f734ea6e43d7cc7bc81da260, 7a70e48a2721d5f5946ec2904dee105ba6c8561b205e5e8fce2aa5f6f3ef0549, 7c53826ea6a9f4ba8d44ca455f1723af9d72b99e97d5053babcfd528fb344e24, 80e8a40be533b4470275d567f7f9d21f6ba4e41e9b3272de77ff67ab9f8442b4, 828c2b61686f9dd8ee888a89ad92793b586a273b57bfd0ad57be6ae2f72616b1, 861c9536994ea3bb6c7aa5463001b79ab61fd945cf44956074d9034e384b3834, 8b30ecb0376e7853c4b323e6b504c967d76f22aa880c587878aa4d5de9bd9808, 8ee29bb1ea8f289d2233fd8053001a29b4fb7d5275120bbcb3e92f5cd5a77b47, 8fb633896f714598c3b935cc45658f3fa14c99a006708c0a78e2f7d29b4c2b1f, 90f4f2c7d5fd9ea10e05cd9bb28a7700fe3fd5cc97d5d59b7e0f043e74f4adbd, 9dc8628aa94effdb2e982d10a6daa4b7897b75db9d452d806f839c9099c01fd4, 9f074ac880d8ae454c84dc03fcbaf0a9c4a15b32a28a590708a38ec6542fc620,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	9f38d473a87c4c72760dd3e578c21f23b271c3c6a28d92e9ffa842073c4abc3b, a0857210ed5a0e38a73a908158905f4271bf82d3f18e0f73494c1846043102f6, a21d016f92be196e4d101a9f20d928ededa930dca835e5bdaffa0ea96372530e, a3bdc6f2f7930af9d4f3378c88fa9c84ee36c8a79b6689c0907fb4e065d7b572, a66220bea0f76e47ca218b99a2b91c7347cb3a291f2df03329009fde23c1a02a, a745b6efbb006d7c9c33503c12f247a95d3d72b98e22f6aa883d7ef45359afdc, aa71db5eb8ec06fbf676dacbb53bc3fdab62169b7287fe5d489713661ddf6360, af14df77f75b1440cd98dc39e4fd24e4d4da62904a699ca2e977c91db30ecc0d, afdcb3443f1b46fe4bd0818654dcbf48a542afdebef4c0725618cd66b2dbddf9, b10e7bbe60e82ec581a3dea4d829838d9c9603f4581125d0200b620d366c75cb, b281b6ffb8cf114b5836ead7cbc424179ac4070e2b15721a5a84af6be0b376d1, b8d46875182730276cf2a67de909ab4b8f3f298554f39928b418984d8cb515b0, bb359ebb2ddc1489a3489c0c37b974d05f9a37e23d4e74517d882fb5c7e493b0, bb88a06cff4e8d73eef046c6a8352dfff7f52903761ced27acd68c065391a464, bd2fb7d2bb7c15d634a986068d5cf811faa83aed72cb7e81df5e5082b22356d2, be68dd32a6b3375935fac1cebf132a2fc7fbfd4074cb8c53022d8eb4e7e17db1, bf5ce4b2911f2d6592abafaf5096936e61d23f98fd9a6b6bbcd763269fba729b, c0b239f989ecd535b9e80570487a39ad67c1e77ba3133caba150da7bf553b724, c10d286de8111a7133831d57394164586584157da2b50d7f3bb85582d69c2b17, c26b86a7e9ff0fb61a2ac0e9eaf78ed34e97a0326df66c7d2311ee7a6033e590, c2b66d97a64d87ce48eb5fb972d23a6b834a677ae154f9f8d4300e9699922ca5, c7646b0f6de08759e19928e25f2ca65cd023a9b820101ae52eb2dc7c7f6f1a69, cbeb46542f05028aee563efb5afa3616612637b31928f98b3d880de2ca524fb0,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	ce5b2579a7893c29ad24ad7126cb83ab629e1d879f69348ad2eb5f9b884d4c44, d1b7ae2d2e12faa4244bd4e5625ffbb2e525586f888bf5b292386221672b5b6d, d5038061e4d308341f6dfd7e807c84266442dbd0afe3b567082ebf6fdbd4c5d4, d51e67e9d81041500994880ecbad47f43a66fc4779a5f79c2c1f47517b8b14ec, d79722670889cf3ce869ed23be59c12029e0df3e536162045b6a87f0b522672d, d80cd0fe212dcfd4a0e683d36c48ba73a7e500a31dbf3f629a13c89565db7580, d8d138f4ebb7a5f12691e2c4edddcf906b66bd5640f8e09e1196a629a624a2ca, d9e2773a56847f4d28e82b2e7215bc4db05807a08d49588f6d6b40be9a430d1b, dbb8a2943af9559d4b3ec8e4c0879cfee3edd882e78b1cd1fb4546acdd7365ee, dce1732d7e260843a9930dea78ff1dc6c469bd306817c827318b56d754f77a98, dd851d7d8b79900e151f91f82d9f1826db493b67f012829783001ab5ffe392e2, ddf5f0ac5484e8e3090b9ce51f53f57cba9550be0e5fcdc2b60787ffc31c15c5, de13a7f1f2cc3cfeeaed063b558134631add81f74e58595bfdf921ff78470a9c, de40f512a3ead48f8c334bcd92198304df41d166ee0c0a90dc4a281464ee7980, ded2e57b60ba81fe9fc9a52ee0591db262527a0b6d166c6ca7165bfb99c4e835, e076d0d1bac228175f0ea23046f0bb7241b0a0457d245ae365ec3de8554a3499, e2627e6c31bb30f791ae80fbbf7d6b57a9ce6ae9e568cff6942ccf6f72195a5e, e4d7ace20cd9704805d144c26bd8c54f6a1b3175b549b6c8279e2d0ee81da9d2, e58ed739c3e6f0f1b0aee262ce0cd99cff6fa04ec7bd665c7c9de7fdfd289c1e, e7372984816703e5664bb1a0632bd7689d573e2868ceccd138c0a5a2977b2a23, e79d67e6c265ff53fb428123711db25b5fc3612ae650b55a2c6484bce3385bec, e806c33313e0490293edeb998abcd9413744e307af5619662ae6a62f6224aee7, ec55eadc6aab2a8c519c016e4b238b39463345c87160b7e2005e6e38ef05ff21,

Attack Name	TYPE	VALUE
Kidkadi	SHA256	eca5155749b0f83671e8c17094a4380c19a3b5096781bd7b88cd9f93a70fc574, ed0cbb7b137a1049331947361020901 6f2c1a8b9560876bc32999b472a32e18f, ee363c5bdc5e786b0b47840d8fe69a5bd71f3684a9eec5d9e49b9ab68c64c793, ee752ce83f645fe4d3db0b1d8c41428d7b9adf37e72a9c21c153450862d30906, eed231bda3ad5a946a254d06865610e50b05eabaece8f09f84323d9fb23e2742, ef4d2a7ca4306626ff90e53ebad63e243a50dff63f34eb0eeaeb4acb2f39c42b, f0269f2b26534acc3ef8bee5b243c54b14812769249a974b2e2b7eba9734a967, f1de30fa0eeedc1f1a7d97736cf751c88fb01456a182f97ede7294bc89bf69af, f4f18af4acee36826b8e2162749250ffb96fc7f8f154d181dd1b8179cf4da68d, f73e65f624f15d967951a6795c712daf31363ab1602485c164549b04989caaaf, f9648d34727738abe86310378929ab7a8d5c8f2698c913bc84dee9be49e3b96a, f98ce437118aeca437a43612858068f4ea6099bb93c63f1b4ffc4d4335e8eaed, fbae3424943aec7aea7ce380c7a83c89ca9c6ff243bfac5186edba6e560f5b66, fd06caf741fd4e5fc9f00c575cc22c00f1a7fd55e826a16dbabc8b3436ed64c4
Rhadamanthys	URLs	hxxp[:]//176[.]46[.]152[.]18[:]8181/gDatFeDway/r26ggaap[.]dssde, hxxp[:]//178[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/mh3af5md[.]wg4ja, hxxp[:]//180[.]178[.]189[.]34[:]8181/gDatFeDway/ujp8k5q9[.]kbtsk, hxxp[:]//185[.]141[.]216[.]120[:]1888/gateway/st2jdbg8[.]gsg45, hxxp[:]//78[.]16[.]53[.]193/mK2k20ajW7kairt1mg88vT1aT9vwU5AZN9AkYYs2QBNbnXV3ph/YEr2KP0jEBhSDdVcS9cWNhbKUgDxcEm9kqxLwFAdHgmKyw7FZq[.]exe, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/el3tkioe[.]xcg4w, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/mbw0n34s[.]gibis, hxxp[:]//94[.]154[.]35[.]99[:]1888/gateway/wwpac3ey[.]q23nf, hxxp[:]//cxbnqdytjgrxutmzawczv[.]cg/gateway/0f4m3h8r[.]trz19, hxxp[:]//jfbcrmphnnikoktsmcpzirlplkwp[.]zl/gateway/8pv47lge[.]93qfg

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

December 22, 2025 . 9:30 AM

More at www.hivepro.com