Date of Publication
April 6, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

30 MARCH to 05 APRIL 2026

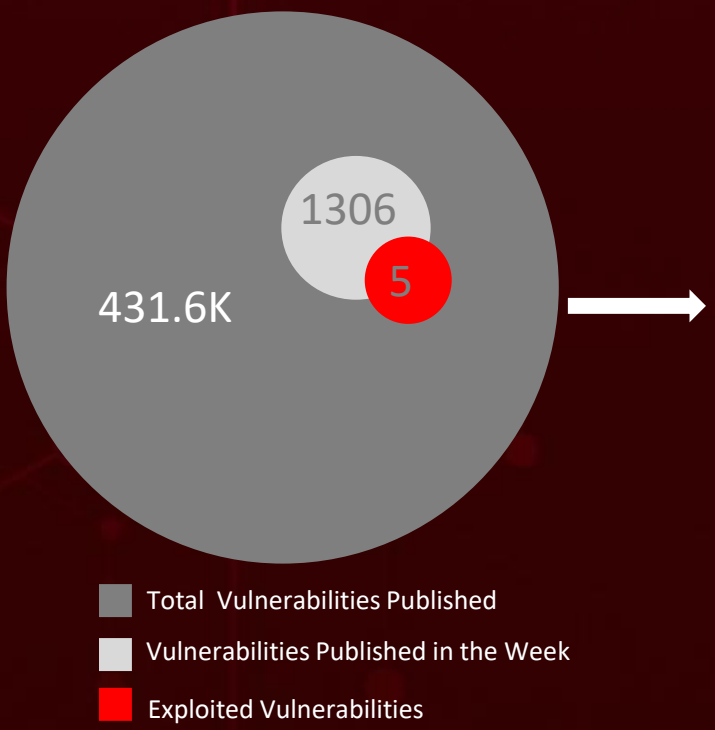
Table Of Contents

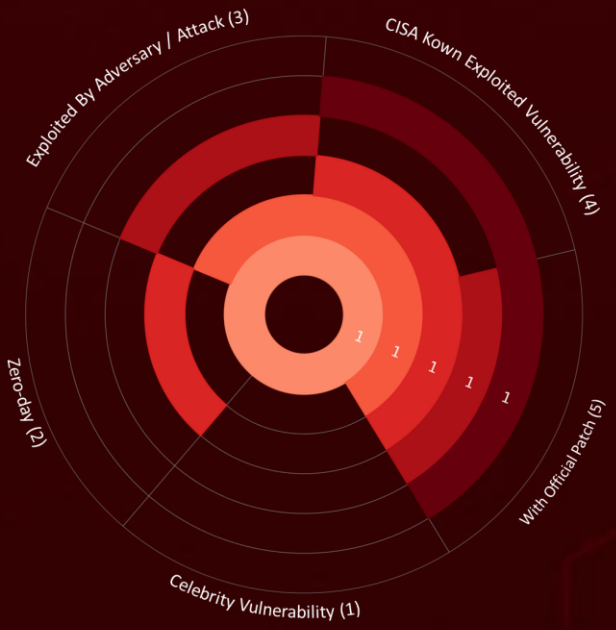
Summary

HiveForce Labs has flagged a noticeable surge in cyber threats, underscoring how rapidly the global threat landscape is evolving. In just a week, defenders tracked **three** significant attacks, **five** critical vulnerabilities, and **two** active threat groups, clear indicators that both the volume and sophistication of malicious activity are accelerating at an uncomfortable pace.

At the vulnerability front, urgency is mounting. Google pushed out emergency patches for **CVE-2026-5281**, a Chrome zero-day already under active exploitation, stemming from a use-after-free flaw in the WebGPU-based Dawn component. The vulnerability allows attackers to manipulate memory and execute arbitrary code, making immediate patching non-negotiable. Meanwhile, Citrix NetScaler is facing active exploitation of **CVE-2026-3055**, a critical SAML flaw that enables unauthenticated attackers to extract sensitive memory data, including session tokens, posing a serious risk to exposed enterprise environments.

Adding to the pressure, a North Korea-linked actor, **UNC1069**, successfully compromised the npm maintainer account for the widely used Axios library, poisoning legitimate versions with a stealthy malicious dependency. This supply chain attack deployed cross-platform RATs across Windows, macOS, and Linux systems, enabling credential theft, reconnaissance, and persistent access before wiping traces to evade detection. Taken together, these incidents highlight a stark reality: threat actors are moving faster, operating smarter, and leaving defenders with virtually no room for complacency.





High Level Statistics

3
Attacks Executed

5
Vulnerabilities Exploited

2
Adversaries in Action

- WAVESHAPER.V2
- SILKBELL
- Vect ransomware

- CVE-2026-3055
- CVE-2026-5281
- CVE-2026-33634
- CVE-2025-29927
- CVE-2025-55182

- TeamPCP
- UNC1069

Insights

UNC1069 weaponizes the Axios npm supply chain, slipping a malicious dependency that deploys cross-platform RATs, steals credentials, and erases its tracks to evade detection.

TeamPCP turns trusted dev tools into attack vectors, exploiting CI/CD pipelines to weaponize a single weak link into a cascading, multi-ecosystem supply chain breach.

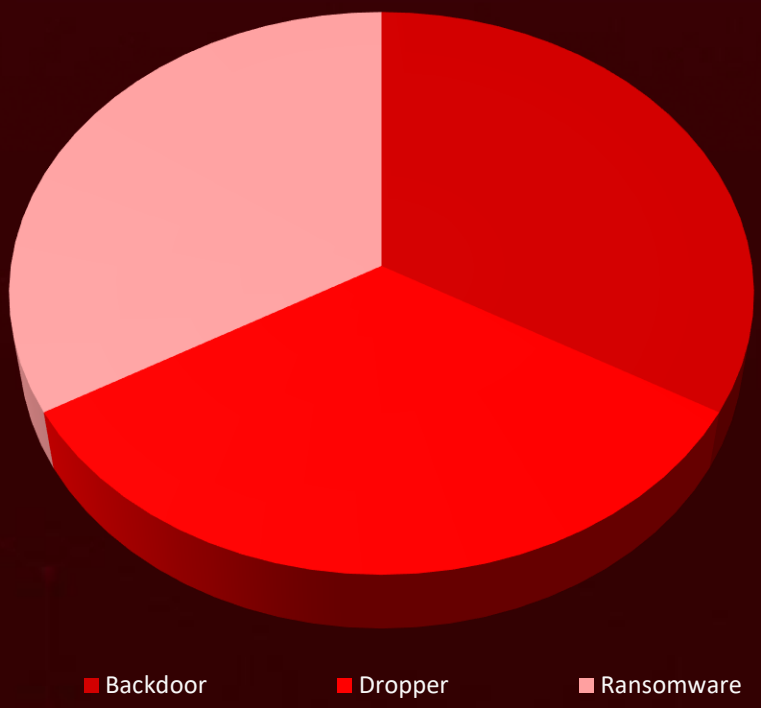
TeamPCP industrializes supply chain attacks, automating the abuse of trusted developer pipelines to turn minor misconfigurations into widespread compromise.

Active exploitation of **CVE-2026-3055** in Citrix NetScaler turns a critical SAML flaw into a silent data leak, exposing session tokens and sensitive memory without authentication.

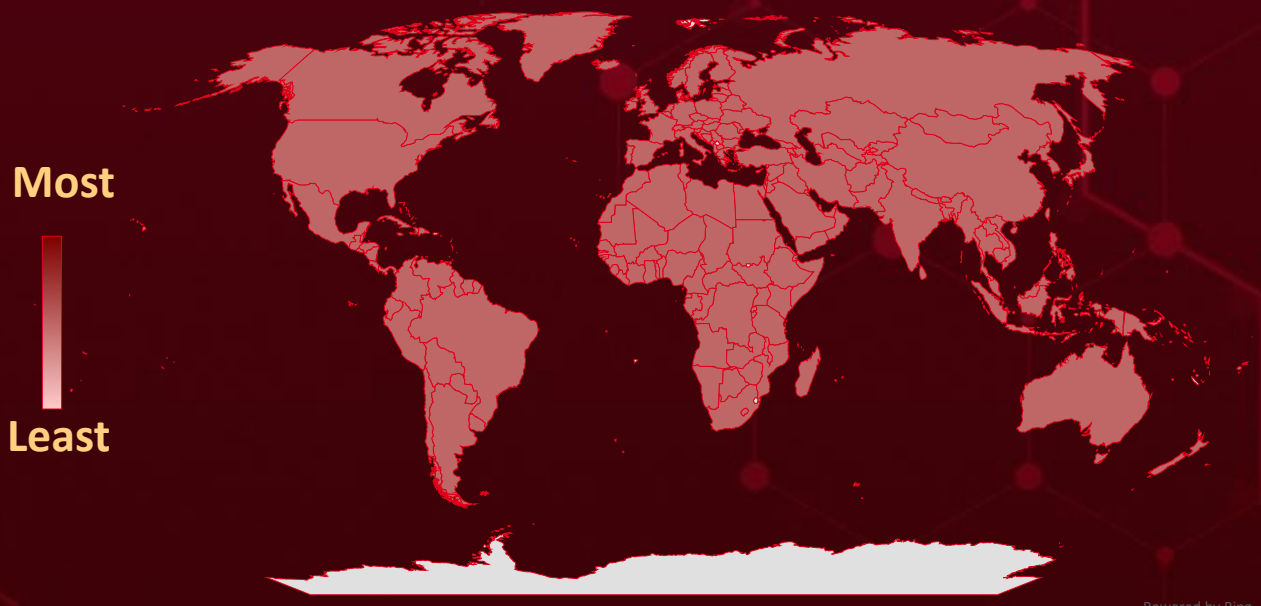
Google races to patch **CVE-2026-5281**, a Chrome zero-day in the WebGPU Dawn component, already exploited in the wild via a use-after-free flaw.

A single poisoned dependency can silently compromise the entire software **supply chain**, turning trusted code into a stealthy, large-scale attack vector.

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
Israel	Netherlands	Italy	Uganda
Jordan	Finland	Poland	Burma
Qatar	Russia	Laos	Eritrea
Bahrain	France	Romania	Honduras
Kuwait	Sweden	Latvia	French Guiana
Cyprus	Germany	San Marino	Burundi
United Arab Emirates	United States	Brunei	Burkina Faso
Iraq	Greece	Serbia	Cabo Verde
Lebanon	Norway	Liechtenstein	Vanuatu
Saudi Arabia	Holy See	Slovakia	Azerbaijan
Ukraine	Portugal	Vietnam	Bangladesh
Syria	Hungary	Spain	Cameroon
Albania	Cambodia	Luxembourg	Saint Lucia
Oman	Iceland	Canada	Belize
Belgium	Slovenia	Malaysia	Seychelles
Switzerland	India	Thailand	Central African Republic
Egypt	Croatia	Malta	South Korea
Turkey	Indonesia	Denmark	Chad
Iran	Dominican Republic	Mauritius	Bahamas
Yemen	Bosnia and Herzegovina	United Kingdom	Angola
Austria	Montenegro	Moldova	Tunisia
Philippines	Andorra	Belarus	Chile
Timor-Leste	North Macedonia	Monaco	Guinea
Singapore	Ireland	Lithuania	Jamaica
Estonia	Bulgaria	Panama	

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1082** System Information Discovery	**T1195.002** Compromise Software Supply Chain	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1547.001 Registry Run Keys / Startup Folder	**T1036.005** Match Legitimate Resource Name or Location	**T1083** File and Directory Discovery	**T1588** Obtain Capabilities	**T1195** Supply Chain Compromise
T1195.001 Compromise Software Dependencies and Development Tools	**T1059.006** Python	**T1547** Boot or Logon Autostart Execution	**T1071** Application Layer Protocol	**T1552** Unsecured Credentials
T1071.001 Web Protocols	**T1588.006** Vulnerabilities	**T1543.002** Systemd Service	**T1485** Data Destruction	**T1560.001** Archive via Utility

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
WAVESHAPER.V2	WAVESHAPER.V2 (aka ZshBucket RAT) is a cross-platform backdoor primarily developed in C++ to target macOS systems, where it is used to gather system information, enumerate directories, and execute additional payloads. It relies on command-line arguments to obtain its command-and-control (C2) server details, enabling flexible deployment across compromised environments. Across all versions, the malware maintains consistent communication patterns, beaconing to its C2 server over port 8000 at regular 60-second intervals using Base64-encoded JSON data, along with a hard-coded User-Agent string to standardize its network traffic and evade detection.	Supply Chain	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data theft, Execute commands, File System Enumeration	Axios npm package
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC1069			
IOC TYPE	**VALUE**		
SHA256	92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a, 617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101		

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
SILKBELL	SILKBELL is a stealthy loader that adapts its behavior based on the victim's operating system, dynamically delivering platform-specific payloads at runtime. To obscure its intent, it employs a custom obfuscation scheme combining XOR and Base64 encoding to hide critical elements such as the command-and-control (C2) URL and OS-specific execution commands.	Supply Chain	-
		IMPACT	AFFECTED PRODUCT
TYPE		Drops additional payloads	Axios npm package
Dropper			PATCH LINK
ASSOCIATED ACTOR			-
UNC1069			
IOC TYPE	VALUE		
SHA256	e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Vect ransomware	Vect is a Ransomware-as-a-Service (RaaS) operation that surfaced in late December 2025 to early January 2026, rapidly positioning itself as a polished and professional threat actor. Unlike many ransomware groups that rely on repurposed or leaked builders, Vect stands out for deploying custom-developed malware written in C++, giving it greater control over functionality and evasion techniques. This tailored approach enables the group to support multi-platform targeting, reflecting a more advanced and adaptable ransomware framework designed for modern enterprise environments.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Comprise, Encrypt Data	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
TeamPCP			
IOC TYPE	VALUE		
IPv4	158[.]94[.]210[.]11		

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-2026-3055	✗	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler Out-of-Bounds Read Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1190: Exploit Public-Facing Application; T1212: Exploitation for Credential Access	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-5281	✗ ZERO-DAY	Google Chrome (Before 146.0.7680.178)	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Dawn Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-by Compromise; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-33634	✗ ZERO-DAY	Aquasecurity setup-trivy Version before 0.2.6, aquasecurity trivy-action Before 0.35.0, Aquasecurity Trivy version before 0.69.3	TeamPCP
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:aquasec:setup-trivy:*:*:*:*:*:*:*:* cpe:2.3:a:aquasec:trivy:0.69.4:*:*:*:*:go:*:* cpe:2.3:a:aquasec:trivy_action:*:*:*:*:*:*:*:* cpe:2.3:a:litellm:litellm:*:*:*:*:*:*:*:* cpe:2.3:a:telnyx:telnyx:*:*:*:*:python:*:*	-
Aquasecurity Trivy Embedded Malicious Code Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-506	T1059: Command and Scripting Interpreter	https://github.com/aquasecurity/trivy/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-29927		Next.js version 1.11.4 and prior to versions 12.3.5, 13.5.9, 14.2.25, and 15.2.3	TeamPCP
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:*	-
Vercel Next.js Middleware Authorization Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863 CWE-285	T1059: Command and Scripting Interpreter	https://github.com/vercel/next.js/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55182	React2Shell	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	TeamPCP
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:* cpe:2.3:a:remix:react_router:*:*:*	-
React2Shell (Meta React Server Components Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter	https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
TeamPCP (aka PCPcat, ShellForce, DeadCatx3, CipherForce, Persy_PCP, UNC6780)	-	All	Worldwide (Primary focus on Iran)
	MOTIVE		
	Espionage, Sabotage, Disruption, Financial Gains		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-33634 CVE-2025-29927 CVE-2025-55182	Vect ransomware	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1059.006: Python; T1204.002: Malicious File; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1053: Scheduled Task/Job; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1611: Escape to Host; T1027: Obfuscated Files or Information; T1027.001: Binary Padding; T1027.003: Steganography; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1528: Steal Application Access Token; T1528: Steal Application Access Token T1552: Unsecured Credentials; T1552.005: Cloud Instance Metadata API; T1552.004: Private Keys; T1003: OS Credential Dumping; T1082: System Information Discovery; T1083: File and Directory Discovery; T1021: Remote Services; T1021.004: SSH; T1610: Deploy Container; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1102: Web Service; T1102.001: Dead Drop Resolver; T1572: Protocol Tunnelling; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1485: Data Destruction; T1496: Resource Hijacking; T1486: Data Encrypted for Impact

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC1069 (aka BlueNorOff, APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71, Alluring Pisces, Selective Pisces, G0082, CryptoCore, CageyChameleon)	North Korea **MOTIVE** Financial crime	All	Worldwide
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	WAVESHAPER.V2 (aka ZshBucket RAT), SILKBELL	Axios npm package (versions 1.14.1 and 0.30.4), Node.js environments, CI/CD pipelines

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA006: Credential Access; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.001: PowerShell; T1059.002: AppleScript; T1059.006: Python; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1070: Indicator Removal; T1070.004: File Deletion; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1027: Obfuscated Files or Information; T1620: Reflective Code Loading; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1552: Unsecured Credentials; T1552.001: Credentials In Files

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **TeamPCP, UNC1069,** and malware **WAVESHAPER.V2, SILKBELL,** and **Vect ransomware.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **TeamPCP, UNC1069,** and malware **WAVESHAPER.V2, SILKBELL,** and **Vect ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2026-3055: Silent Memory Leak in NetScaler Actively Exploited

CVE-2026-5281: Chrome Dawn Flaw Sparks In-the-Wild Zero-Day Attacks

Axios npm Supply Chain Attack: What You Need to Know

TeamPCP's Automated Supply Chain: From Trivy to LiteLLM in a Multi-Ecosystem Breach

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)

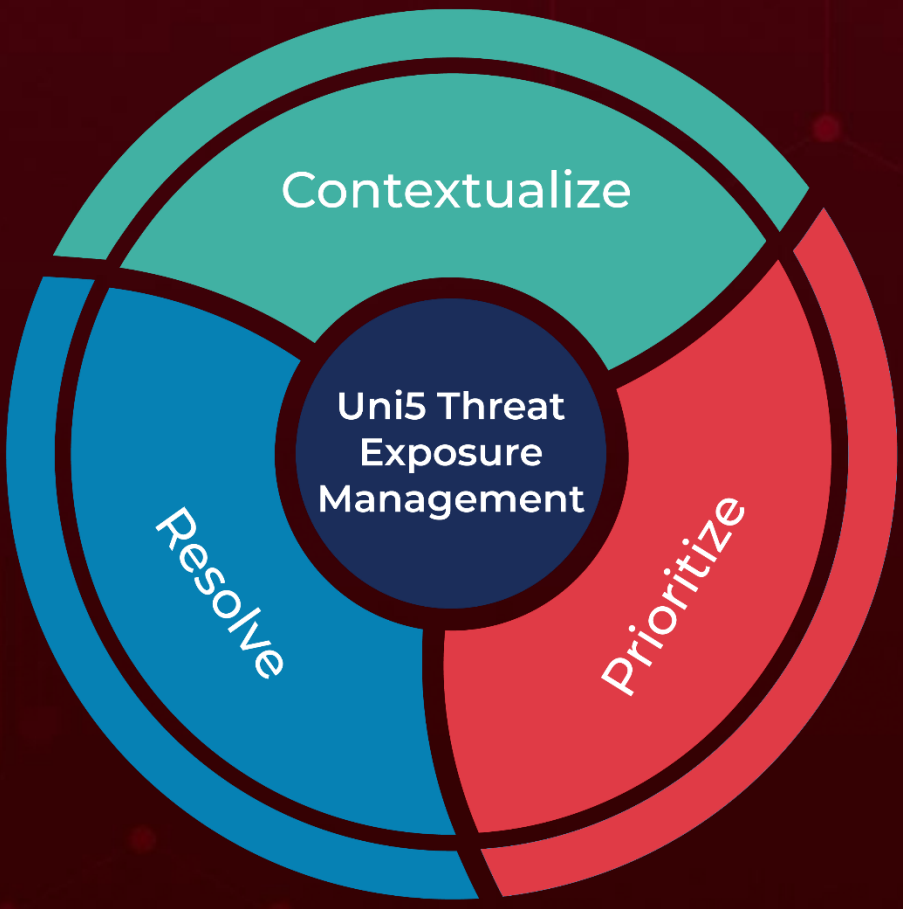
Attack Name	TYPE	VALUE
WAVESHAPER.V2	SHA256	92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a, 617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101, ed8560c1ac7ceb6983ba995124d5917dc1a00288912387a6389296637d5f815c, fcb81618bb15edfdedfb638b4c08a2af9cac9ecfa551af135a8402bf980375cf
SILKBELL	SHA256	e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09
Vect ransomware	IPv4	158[.]94[.]210[.]11
	SHA256	8ee4ec425bc0d8db050d13bbff98f483fff020050d49f40c5055ca2b9f6b1c4d

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

April 6, 2026 . 09:00 AM

More at www.hivepro.com