

Date of Publication
September 16, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

07 to 13 SEPTEMBER 2026

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>	22
<u>Adversaries in Action</u>	29
<u>Recommendations</u>	35
<u>Threat Advisories</u>	36
<u>Appendix</u>	37
<u>What Next?</u>	39

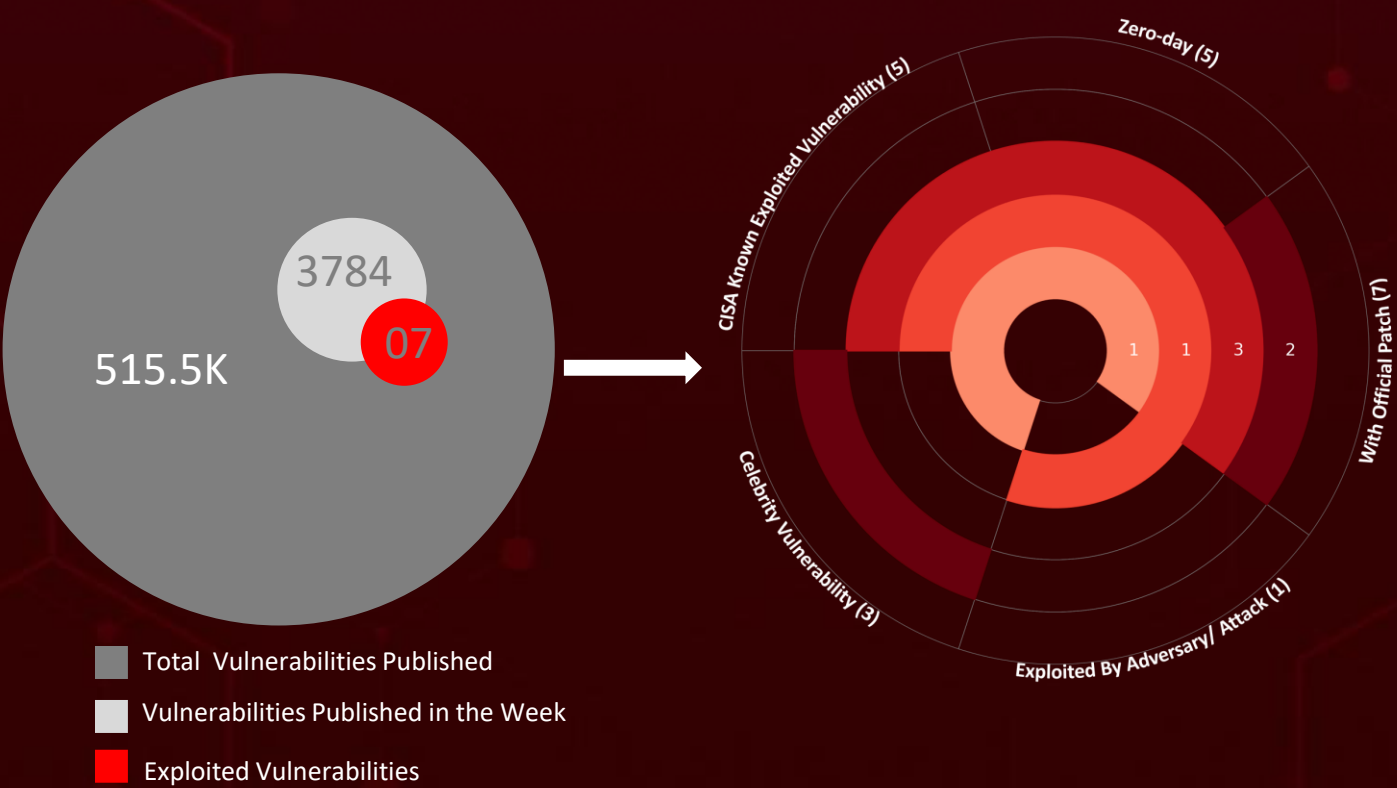
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **14** major attacks were detected, **7** vulnerabilities were actively exploited, and **6** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, **StyleSmuggler (CVE-2026-75650)** leads this cycle. A template-engine flaw in Magento Open Source and Adobe Commerce, exploited in the wild since 4 September 2026, lets unauthenticated attackers hide PHP in a failure report and trigger a failed-payment email that executes it, yielding remote code execution.

That same commercial layer is drawing organized extortion elsewhere. **Panzer**, a new Ransomware-as-a-Service group, went live with its leak site on 5 August 2026 and has already named 20+ victims across 10+ countries, pairing theft with encryption and countdown timers on Tor.

BREEZE COMET threat actor has been active since September 2023; the Brazil-based crew breaches local financial services, fintech, retail, and eCommerce firms to reach internal payment systems and push fraudulent transfers. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

14

Attacks
Executed

7

Vulnerabilities
Exploited

6

Adversaries in
Action

- COBALTSPIN
- REALBREEZE
- MILDFROST
- BOATBEAM
- LIGHTPAINT
- KICKPLATE
- XWORM
- JSCeal
- PEEP
- GRIMWEDGE
- SUPERSTOMP
- LONGTALE
- ShadowPad
- Panzer

- CVE-2026-75650
- CVE-2026-6471
- CVE-2026-85880
- CVE-2026-81963
- CVE-2026-69414
- CVE-2026-86218
- CVE-2026-87491

- BREEZE COMET
- TA412
- UTA0560
- UNK_LateNight
- UNK_DoubleChe
ck
- UNK_QuietRack
et



Insights

N-able N-central

CVE-2026-86218:

Static Code Injection
at Maximum
Severity

CVE-2026-6471: Missing

**Authorization in PostgreSQL Logical
Decoding**

JSCeal: The Fake

TradingView That
Trades Away Your
Crypto

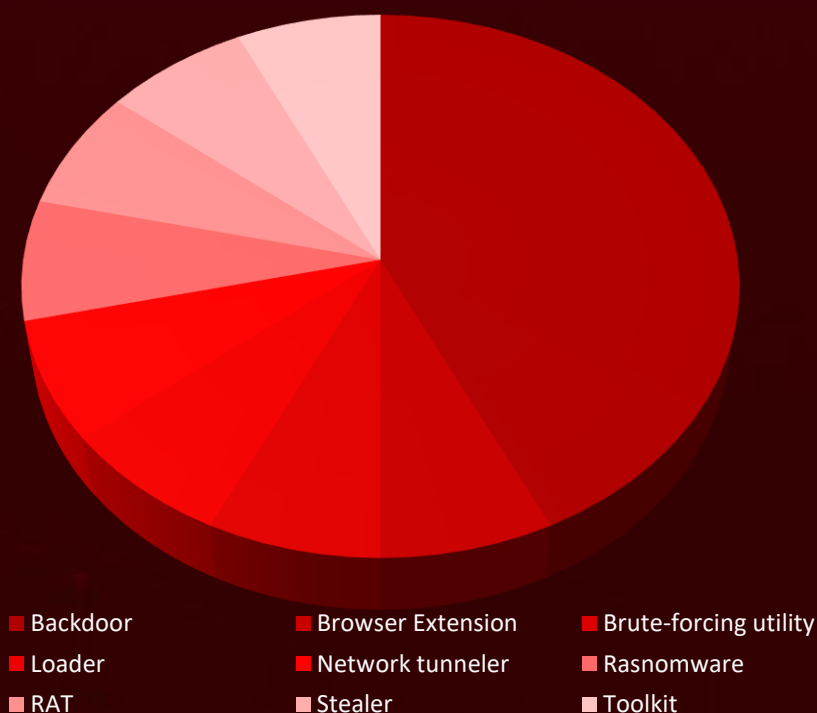
**PEEP: The "Smart Bookmarks"
Extension That Owns Your
Browser**

**Patch Isn't Enough: Hunting the Rust
Implant Behind StyleSmuggler (CVE-
2026-75650)**

BREEZE COMET

Turns Internal
Payment
Systems Into
ATMs

Threat Distribution



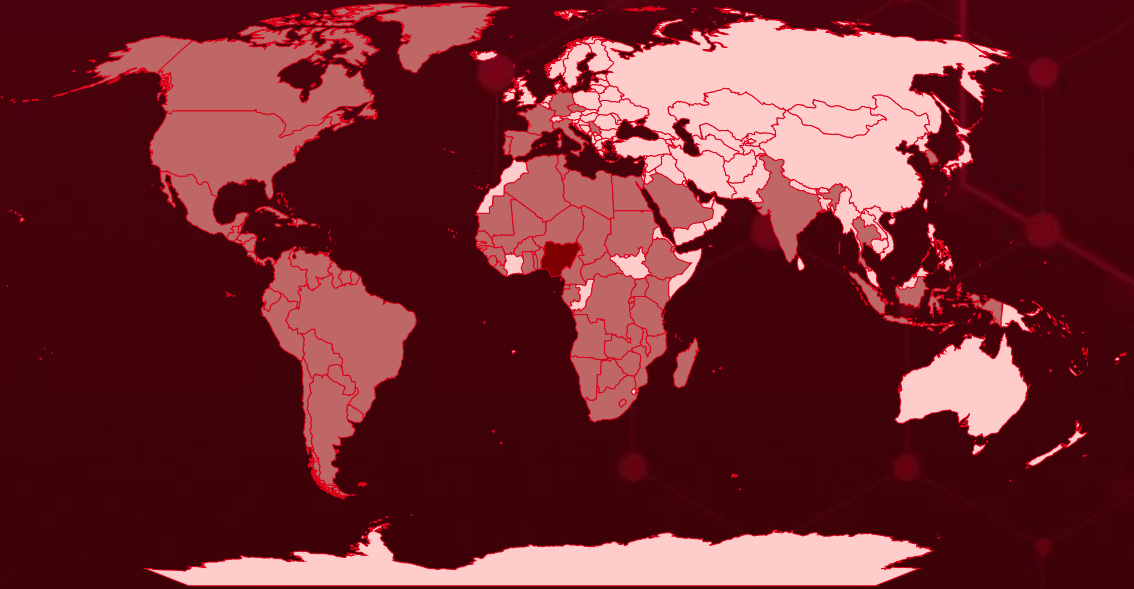


Targeted Countries

Most



Least

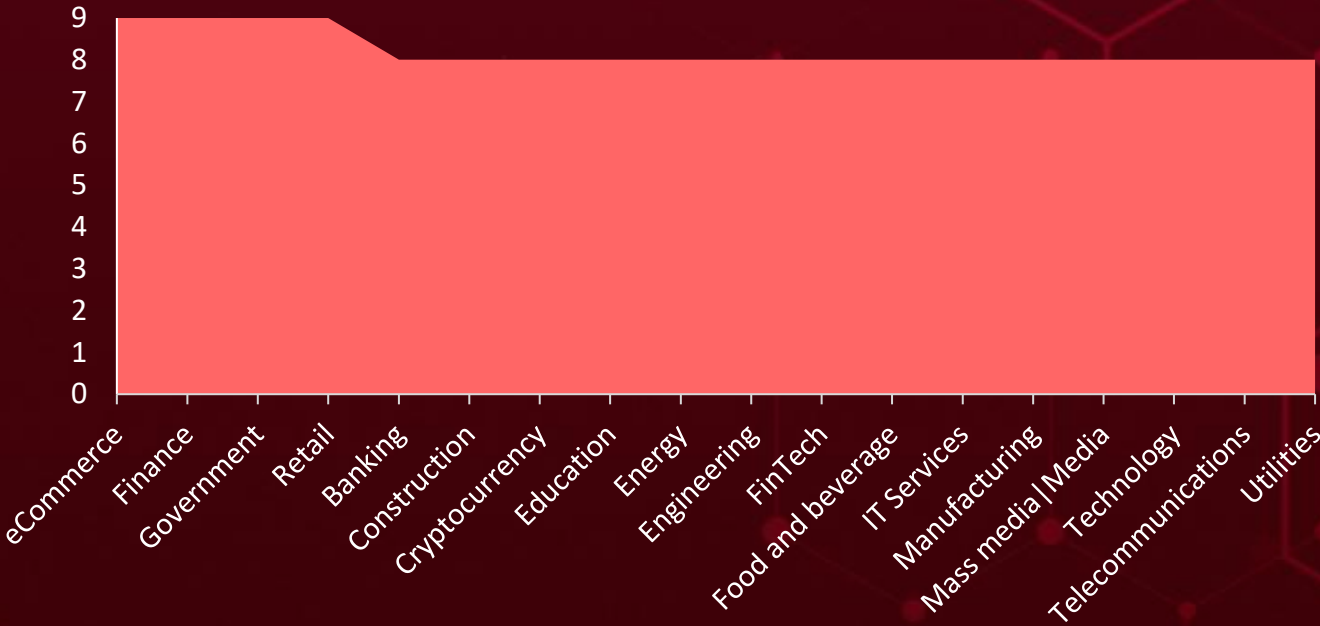


Powered by Bing

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

Countries	Countries	Countries	Countries
Nigeria	Indonesia	Czech Republic	Saudi Arabia
Mexico	Botswana	Kenya	Ghana
United States Virgin Islands	Zambia	Democratic Republic of Congo	Serbia
Senegal	Brazil	Lesotho	Greenland
Angola	Madagascar	Djibouti	Sierra Leone
Liberia	Burkina Faso	Libya	Grenada
Anguilla	Mauritania	Dominica	South Korea
Peru	Burundi	Malawi	Guadeloupe
Antigua and Barbuda	Mozambique	Dominican Republic	Sudan
Suriname	Cameroon	Martinique	Guatemala
Argentina	Panama	Ecuador	Tanzania
Jamaica	Canada	Mauritius	Guinea
Bahamas	Puerto Rico	Egypt	Togo
Mali	Central African Republic	Monaco	Guinea-Bissau
Barbados	Saint Maarten	El Salvador	Tunisia
Nicaragua	Chad	Namibia	Guyana
Belize	Seychelles	Equatorial Guinea	United States
Saint Kitts and Nevis	Chile	Algeria	Haiti
Benin	Spain	Niger	Uruguay
South Africa	Colombia	Ethiopia	Honduras
Bermuda	Thailand	Paraguay	India
Trinidad and Tobago	Comoros	France	Zimbabwe
Bolivia	Uganda	Portugal	Qatar
	Costa Rica	French Guiana	Taiwan
	Venezuela	Rwanda	China
	Cuba	Gabon	
	Italy	Saint Lucia	
		Germany	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	T1005 Data from Local System	T1078 Valid Accounts	T1190 Exploit Public-Facing Application	T1071 Application Layer Protocol
T1027 Obfuscated Files or Information	T1068 Exploitation for Privilege Escalation	T1053 Scheduled Task/Job	T1071.001 Web Protocols	T1657 Financial Theft
T1036 Masquerading	T1588 Obtain Capabilities	T1113 Screen Capture	T1539 Steal Web Session Cookie	T1056 Input Capture
T1574 Hijack Execution Flow	T1059.001 PowerShell	T1583 Acquire Infrastructure	T1059.007 JavaScript	T1556 Modify Authentication Process

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>COBALTSPIN</u>	COBALTSPIN is a Rust-based network tunneler /proxy malware. It establishes a reverse SOCKS5 proxy over WebSocket, relaying traffic between the C2 and internal hosts so the operator can pivot through boundary firewalls without any built-in persistence that might trigger detection.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Network tunneler		Firewall bypass, Lateral movement, Fraudulent transactions	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da2759d27ceec		

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>REALBREEZE</u>	REALBREEZE is a custom LDAP brute-forcing utility (credential-attack tool). BREEZE COMET uses it to hammer directory accounts and obtain valid credentials beyond traditional Active Directory compromise, alongside separate efforts to mine CI/CD environments for hard-coded pipeline credentials, API keys, and highly privileged cloud tokens.	Downloaded from GitHub repositories	-
TYPE		IMPACT	AFFECTED PLATFORM
Brute-forcing utility		Credential compromise, Privilege escalation, Account takeover, directory exposure	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b74441200439a		

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>MILDFROST</u>	MILDFROST is a passive Java JAR backdoor. It hides inside the JVM process space and uses classes such as DnsCommandBeacon.class to establish slow, covert DNS tunnels, serving as a fallback C2 that queries delegated subdomains for instructions and pulls down fresh copies of the actor's C++ executables.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent access, Covert C2, Payload delivery	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	c0db6ddd6222d02ad7490399d33c61ded0076f0037409dc8498924458646d78a		

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>BOATBEAM</u>	BOATBEAM is a Golang backdoor. It stands up a fake IIS HTTPS server on port 443, masquerading as a legitimate web server so backdoor traffic blends with normal HTTPS, and activates its C2 functionality only when a specific session cookie is presented.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Covert C2, Remote Control	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	6d4012e0dd3b56a3e52857734fa0d582cdf3c56f0e5decc8005c882d1d1c6ceb		

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>LIGHTPAINT</u>	LIGHTPAINT is a custom Java-based backdoor. It installs a legitimate VPN such as SoftEther and configures it for automated persistence, then protects that channel by programmatically adding inbound Windows Defender Firewall rules permitting all traffic from the deployed VPN manager and clearing the Windows Networking Vpn Plugin Platform event logs to erase forensic evidence of the connection.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Network Tunneling, Defense Tampering, Evidence Destruction	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-

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>KICKPLATE</u>	KICKPLATE is a custom Nim-based backdoor and loader. It impersonates Windows Update Health Tools to blend in, continuously delivers auxiliary payloads, and enforces host-level persistence by executing commands to control SOCKS5 tunnelers, update registry startup keys, and silently modify Windows services, supplemented by scheduled tasks run via schtasks.exe as SYSTEM and malicious .lnk shortcuts placed in user startup folders.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Payload Delivery, System Tampering	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	f139b4ca15feffb7a6633ec1a431c5c604b397576b56b5c863ae8fe4fa14db4f		

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>XWORM</u>	XWORM is a commodity RAT, widely sold on cybercrime forums, with leaked and cracked builds also circulating. BREEZE COMET deploys it for initial access and an early foothold, configuring it to persist through automated startup shortcut modifications.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote Control, Persistent Access, Credential Theft, Data Exfiltration	-
ASSOCIATED ACTOR			PATCH LINK
BREEZE COMET			-
IOC TYPE	VALUE		
SHA256	51fdd83b3737add7f3832bd0ad0b56863c0a8f7cf9bcc16fd787d1ae4b403ce6, d2aa40cc53b40c6e76ac0677c4a54387b3f27ee94c85d9b2c3a3d66aeef92a66		

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
JSCeal	JSCeal is a credential and cryptocurrency-stealing malware (also tracked as WEEVILPROXY or MeadowLocust) that targets crypto wallets and applications through an unusually stealthy delivery method. Rather than shipping as readable JavaScript, it's distributed as compiled V8 bytecode (.jsc files) and run through a bundled Node.js runtime, meaning the malware never touches disk as human-readable source code. To get there, the attackers first heavily obfuscate the original JavaScript, then compile it into V8's internal bytecode format, a version-specific representation that standard JavaScript deobfuscation tools simply weren't built to handle. This two-step transformation strips away the cues that malware analysts normally rely on, making JSCeal significantly harder to detect, reverse-engineer, and attribute using conventional tooling.	Malicious Facebook and Google ads	-
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Steal Data	Windows, macOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1f5acba97db6d514e4b35ba0601c5269697e8ab3bb99d097db25ec7e74464594		

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
PEEP	PEEP is an emerging Chromium-based post-exploitation toolkit disguised as a "Smart Bookmarks" extension, built on the open-source RedExt framework but heavily extended with its own installer, native host bridge, and command set. Requiring prior admin or code-execution access, it forges Chrome/Edge's Secure Preferences integrity values to inject itself in without triggering Web Store checks or user prompts, then uses a native-messaging bridge to break out of the browser sandbox for host-level command execution and file management. Because it runs inside the trusted, signed browser process, it evades typical detection, turning the browser into a persistent pivot for credential theft, session hijacking, and command execution.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Toolkit		Command Execurion, System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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>GRIMWEDGE</u>	GRIMWEDGE is a lightweight JScript backdoor, coming in at under 250 lines of code, that gives attackers host reconnaissance, file and process management, command execution, and payload delivery capabilities through a set of ten supported commands. Despite its small footprint, it functions as a compact tool, letting an attacker survey a compromised machine, manage files and running processes, execute arbitrary commands, and drop additional payloads, all from a script simple enough to evade tools tuned for more complex malware.	Phishing	CVE-2026-87491
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Command Execurion, System Compromise	Google Chrome
ASSOCIATED ACTOR			PATCH LINK
UTA0560			https://www.google.com/intl/en/chrome/?standalone=1
IOC TYPE	VALUE		
SHA256	69c1603f3f9015beb0097d0a3bb0f17400c314e2eae65a7eceacd3b93ea570dc, 59dc108e22cb856c228bbf8a1ab955fb66f0844a07fe10fa0d9fc3823d2cbbcb		

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>SUPERSTOMP</u>	SUPERSTOMP is a loader built specifically to sneak a malicious Chrome extension onto a victim's machine, ultimately installing LONGTALE, a credential-stealing extension that poses as Google Gemini. It works by tampering with Chrome's Secure Preferences file, a well-known technique, but one that's gotten harder to pull off since Chromium added protections against exactly this kind of tampering: per-preference encrypted hashes in November 2025, followed by a broader "super" hash covering the entire preferences file in June 2026. Even with both of these integrity checks in place, SUPERSTOMP still manages to slip the malicious extension in, showing that the added protections haven't fully closed the door on this attack path.	Phishing	CVE-2026-87491
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional malware	Google Chrome
ASSOCIATED ACTOR			PATCH LINK
TA412			https://www.google.com/intl/en/chrome/?standalone=1
IOC TYPE	VALUE		
SHA256	e2a59432ce2b0d83ded936374a11fca3d3defaf4aab90eb37fca58683eae32c0		

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>LONGTALE</u>	LONGTALE, also tracked as GemStone, is a credential-stealing Chrome extension that disguises itself as Google Gemini to gain a victim's trust. At its core sits a heavily obfuscated JavaScript service worker, background.js, which quietly turns the extension into a browser-surveillance and credential-theft backdoor, monitoring activity and harvesting sensitive data while presenting itself as a legitimate assistant tool.	Phishing	CVE-2026-87491
TYPE		IMPACT	AFFECTED PLATFORM
Browser Extension		Steal Data	Google Chrome
ASSOCIATED ACTOR			PATCH LINK
TA412			https://www.google.com/intl/en/chrome/?standalone=1
IOC TYPE	VALUE		
SHA256	5eb5645511b00e4f4d73125654eeb3a3930fcf09c65685dc7f03f725331492e3		

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
ShadowPad	ShadowPad is a well-known modular backdoor first identified back in 2017, historically spread through supply-chain attacks where legitimate software gets compromised before it ever reaches victims. It's been used both in financially motivated campaigns targeting the gaming industry and in strategic espionage aimed at stealing intellectual property. This particular variant goes out of its way to stay hidden, unhooking 20 network monitoring functions so security tools can't see what it's doing, while it steals saved data from Firefox profiles and sniffs network traffic in the background. It phones home over HTTPS to ms.checcrity[.]com, using its own binary command-and-control protocol and rotating user-agent strings to blend in with normal web traffic.	Phishing	CVE-2026-87491
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Google Chrome
ASSOCIATED ACTOR			PATCH LINK
UNK_LateNight			https://www.google.com/intl/en/chrome/?standalone=1
IOC TYPE	VALUE		
Hostname	ms.checcrity[.]com		

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>Panzer</u>	Panzer is a ransomware-as-a-service double-extortion operation active since August 5, 2026, advertising Windows, Linux, ESXi and FreeBSD encryptors. Claims 20+ victims across 11+ countries.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Rasnomware		Data theft, encryption	Windows, Linux, ESXi, FreeBSD
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
TOR Address	pnzruro7syvwvfx5mpo2fhzi4jftgquynsqf3vy5x3no57yp2iz4nyd[.]onion		

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
<u>CVE-2026-75650</u>	StyleSmuggler	Adobe Commerce and Magento Open Source 2.4.4 - 2.4.9 (2026-aug and earlier), Adobe Commerce on Cloud, Adobe Commerce B2B 1.3.3 - 1.5.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:magento:magento:*:*:*:*:*:open_source:*:*:*:*:*:*:*:*:*:* cpe:2.3:a:adobe:commerce:*:*:*:*:*:*:*:*:*:*	-
Adobe Commerce and Magento Open Source Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1336	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/magento/apsb26-146.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-6471</u>	PostGRESshell	PostgreSQL core server before 18.6, 17.11, 16.15, 15.19, and 14.24	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*	-
PostgreSQL Output Plugin Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.postgresql.org/support/security/CVE-2026-6471/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85880</u>		Windows 10 Version 1809; Windows Server 2019, 2022, 2016, 2012; Windows 10 Version 21H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_10 :*:*:*:*:*:*:*	-
Microsoft Windows Heap- Based Buffer Overflow Vulnerability		cpe:2.3:o:microsoft:windows_se rver:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122, CWE-908	T1068: Exploitation for Privilege Escalation, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-81963</u>		Windows 11 Version 23H2, 24H2, 25H2; Windows Server 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*	-
Microsoft Windows Link Following Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284, CWE-59	T1574: Hijack Execution Flow, T1222: File and Directory Permissions Modification, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-69414</u>	ShieldBreak	Microsoft Malware Protection Engine	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:malware_protection_engine:-:*:*:*:*:*	-
Microsoft Defender Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269, CWE-284	T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69414

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-86218</u>		N-able N-central (Before 2026.3.1.14)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*	-
N-able N-central Static Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-96	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.n-able.com/blog/n-central-security-hotfix-september-5-2026 , https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-87491</u>		Google Chrome versions before 153.0.8010.36 on Windows, macOS, and Linux	TA412, UTA0560, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Google Chromium V8 Out of Bounds Write Vulnerability		cpe:2.3:a:google:chrome:*:*:*:*:*.*.*.*	GRIMWEDGE SUPERSTOMP LONGTALE (aka GemStone) ShadowPad
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.google.com/intl/en/chrome/?s_tandalone=1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>BREEZE</u> <u>COMET (aka</u> <u>UNC5669,</u> <u>PLUMP</u> <u>SPIDER,</u> <u>SHADOW-</u> <u>AETHER-064,</u> <u>CL-CRI-1163)</u>	Brazil	Financial Services, Fintech, Banking Software Providers, Payment Processors, Banks, Retail, Point-Of-Sale, Ecommerce, Exchanges, Government	Brazil, Argentina, Bolivia, Chile, Colombia, Ecuador, French Guiana, Guyana, Peru, Suriname, Uruguay, United States, Mexico, Canada, Guatemala, Haiti, Cuba, Dominican Republic, Honduras, El Salvador, Nicaragua, Costa Rica, Panama, Jamaica, Puerto Rico, Trinidad and Tobago, Belize, Guadeloupe, Bahamas, Martinique, Barbados, Saint Lucia, Grenada, United States Virgin Islands, Antigua and Barbuda, Dominica, Bermuda, Greenland, Saint Kitts and Nevis, Saint Maarten, Anguilla, Nigeria, Paraguay, Venezuela, Ethiopia, Egypt, DR Congo, Tanzania, South Africa, Kenya, Sudan, Uganda, Algeria, Angola, Morocco, Mozambique, Ghana, Madagascar, Cameroon, Niger, Mali, Burkina Faso, Malawi, Zambia, Chad, Senegal, Zimbabwe, Guinea, Benin, Rwanda, Burundi, Tunisia, Togo, Sierra Leone, Libya, Liberia, Central African Republic, Mauritania, Namibia, Gabon, Botswana, Lesotho, Guinea-Bissau, Equatorial Guinea, Mauritius, Djibouti, Comoros, Seychelles
	MOTIVE		
	Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	COBALTPIN, REALBREEZE, MILDFOST, BOATBEAM, LIGHTPAINT, KICKPLATE, XWORM	Windows, Linux, Active Directory, Cloud environments, Kubernetes, CI/CD pipelines, Java Virtual Machine (JVM) process space.

TTPs
TA0043: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0006: Credential Access, TA0007: Discovery, TA0005: Defense Evasion, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1584: Compromise Infrastructure, T1608: Stage Capabilities, T1588: Obtain Capabilities, T1566: Phishing, T1190: Exploit Public-Facing Application, T1200: Hardware Additions, T1219: Remote Access Tools, T1059: Command and Scripting Interpreter, T1204: User Execution, T1610: Deploy Container, T1505: Server Software Component, T1547: Boot or Logon Autostart Execution, T1543: Create or Modify System Process, T1053: Scheduled Task/Job, T1078: Valid Accounts, T1110: Brute Force, T1552: Unsecured Credentials, T1528: Steal Application Access Token, T1087: Account Discovery, T1046: Network Service Discovery, T1083: File and Directory Discovery, T1562: Impair Defenses, T1036: Masquerading, T1070: Indicator Removal, T1620: Reflective Code Loading, T1021: Remote Services, T1119: Automated Collection, T1572: Protocol Tunneling, T1090: Proxy, T1071: Application Layer Protocol, T1568: Dynamic Resolution, T1105: Ingress Tool Transfer, T1567: Exfiltration Over Web Service, T1657: Financial Theft, T1584.004: Server, T1608.001: Upload Malware, T1588.001: Malware, T1588.002: Tool, T1588.007: Artificial Intelligence, T1566.004: Spearphishing Voice, T1219.002: Remote Desktop Software, T1059.001: PowerShell, T1059.004: Unix Shell, T1204.002: Malicious File, T1505.003: Web Shell, T1547.001: Registry Run Keys / Startup Folder, T1543.003: Windows Service, T1053.005: Scheduled Task, T1078.002: Domain Accounts, T1110.003: Password Spraying, T1552.001: Credentials In Files, T1552.007: Container API, T1087.002: Domain Account, T1562.001: Disable or Modify Tools, T1562.004: Disable or Modify System Firewall, T1036.005: Match Legitimate Name or Location, T1070.001: Clear Windows Event Logs, T1070.004: File Deletion, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1090.001: Internal Proxy, T1071.001: Web Protocols, T1071.004: DNS

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>TA412 (aka JungleBamboo, APT31, Violet Typhoon, TIDE CASTLE, Judgment Panda, Zirconium, RedBravo, Bronze Vinewood, Red Keres)</u>	China	Non-governmental organizations, aerospace and defense-industrial firms, mining and physical commodity traders, manufacturing entities, and government and financial-sector entities	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-87491	SUPERSTOMP, LONGTALE (aka GemStone)	Google Chrome
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1588: Obtain Capabilities, T1588.005: Exploits, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1059.003: Windows Command Shell, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1176: Browser Extensions, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1056: Input Capture, T1056.001: Keylogging, T1539: Steal Web Session Cookie, T1082: System Information Discovery, T1057: Process Discovery, T1005: Data from Local System, T1113: Screen Capture, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1573: Encrypted Channel, T1573.001: Symmetric Cryptography, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UTA0560</u>	China	non-governmental organizations (NGOs)	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-87491	GRIMWEDGE	Google Chrome
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1588: Obtain Capabilities, T1588.005: Exploits, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1059.003: Windows Command Shell, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1176: Browser Extensions, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1056: Input Capture, T1056.001: Keylogging, T1539: Steal Web Session Cookie, T1082: System Information Discovery, T1057: Process Discovery, T1005: Data from Local System, T1113: Screen Capture, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1573: Encrypted Channel, T1573.001: Symmetric Cryptography, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNK LateNight	China	aerospace	US
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-87491	ShadowPad	Google Chrome
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1588: Obtain Capabilities, T1588.005: Exploits, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1059.003: Windows Command Shell, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1176: Browser Extensions, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1056: Input Capture, T1056.001: Keylogging, T1539: Steal Web Session Cookie, T1082: System Information Discovery, T1057: Process Discovery, T1005: Data from Local System, T1113: Screen Capture, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1573: Encrypted Channel, T1573.001: Symmetric Cryptography, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNK DoubleCheck	-	manufacturing	Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2026-87491	-	Google Chrome
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1588: Obtain Capabilities, T1588.005: Exploits, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1059.003: Windows Command Shell, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1176: Browser Extensions, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1056: Input Capture, T1056.001: Keylogging, T1539: Steal Web Session Cookie, T1082: System Information Discovery, T1057: Process Discovery, T1005: Data from Local System, T1113: Screen Capture, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1573: Encrypted Channel, T1573.001: Symmetric Cryptography, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNK QuietRack et	China	government, consulting, and financial sector organizations	Singapore , Indonesia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-87491	-	Google Chrome
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1588: Obtain Capabilities, T1588.005: Exploits, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1059.003: Windows Command Shell, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1176: Browser Extensions, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1056: Input Capture, T1056.001: Keylogging, T1539: Steal Web Session Cookie, T1082: System Information Discovery, T1057: Process Discovery, T1005: Data from Local System, T1113: Screen Capture, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1573: Encrypted Channel, T1573.001: Symmetric Cryptography, T1041: Exfiltration Over C2 Channel			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **7 exploited vulnerabilities** and block the indicators related to the threat actors **BREEZE COMET, TA412, UTA0560, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket,** and malware **COBALTSPIN, REALBREEZE, MILDFROST, BOATBEAM, LIGHTPAINT, KICKPLATE, XWORM, JSceal, PEEP, GRIMWEDGE, SUPERSTOMP, LONGTALE, ShadowPad, and Panzer.**

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 **7 exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TA412,** and malware **MILDFROST, KICKPLATE Backdoor, XWorm, JSceal Stealer, COBALTSPIN, and REALBREEZE** in Breach and Attack Simulation(BAS).

Threat Advisories

[BREEZE COMET Turns Brazil's Instant Payment Rails into a Cash-Out Channel](#)

[StyleSmuggler: Adobe Commerce and Magento Zero-Day Exploited](#)

[JSCeal: Crypto Stealer Hidden in V8 Bytecode](#)

[CVE-2026-6471: Twelve-Year-Old PostgreSQL Flaw Grants Full Server Control](#)

[PEEP: The Bookmark Extension That Backdoors Your PC](#)

[Microsoft's September 2026 Patch Tuesday - Priority Fixes](#)

[N-able N-central Pre-Auth RCE Exploited in the Wild \(CVE-2026-86218\)](#)

[Patch-Gap Panic: Chrome V8 Zero-Day Fuels the BlueMoon Espionage Wave](#)

[Panzer: New Cross-Platform RaaS Claims Global Victims in Its First Month](#)

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>COBALTSPIN</u>	SHA256	3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da2759d27ceec
<u>REALBREEZE</u>	SHA256	2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b74441200439a
<u>MILDFROST</u>	SHA256	c0db6ddd6222d02ad7490399d33c61ded0076f0037409dc8498924458646d78a
<u>BOATBEAM</u>	SHA256	6d4012e0dd3b56a3e52857734fa0d582cdf3c56f0e5decc8005c882d1d1c6ceb
<u>KICKPLATE</u>	SHA256	f139b4ca15feffb7a6633ec1a431c5c604b397576b56b5c863ae8fe4fa14db4f
<u>XWORM</u>	SHA256	51fdd83b3737add7f3832bd0ad0b56863c0a8f7cf9bcc16fd787d1ae4b403ce6, d2aa40cc53b40c6e76ac0677c4a54387b3f27ee94c85d9b2c3a3d66aeef92a66, 447e3a131e62bd33b1297739a7b959a92358a97f58554469044636a3c4f244e8
<u>JSCeal</u>	SHA256	1f5acba97db6d514e4b35ba0601c5269697e8ab3bb99d097db25ec7e74464594

Attack Name	TYPE	VALUE
<u>GRIMWEDGE</u>	SHA256	69c1603f3f9015beb0097d0a3bb0f17400c314e2eae65a7eceacd3b93ea570dc, 59dc108e22cb856c228bbf8a1ab955fb66f0844a07fe10fa0d9fc3823d2cbbcb
	Domain	ocr[.]opusaccel[.]top
<u>SUPERSTOMP</u>	SHA256	e2a59432ce2b0d83ded936374a11fca3d3defaf4aab90eb37fca58683eae32c0
<u>LONGTALE</u>	SHA256	5eb5645511b00e4f4d73125654eeb3a3930fcf09c65685dc7f03f725331492e3
	URL	hxxps://xyz0102.gitprogram[.]com/a001
	Hostname	extension-management-portal.centerfjdr658.workers[.]dev, extension-management-portal.kmjukilo-lkjh.workers[.]dev
<u>ShadowPad</u>	Hostname	ms.chechity[.]com
	IPv4	79[.]133[.]56[.]90
	Domain	chechity[.]com
<u>Panzer</u>	TOR Address	pnzruro7syvwvfx5mpo2fhzi4jftgquynsqf3vy5x3no57yp2iz4nyd[.]onion
	Tox ID	8C3D96497A9438794F705C055FC2FD3059F6CF11FF51060EE55ED7F0679CFC7218825BD56CB1

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 demo of HivePro.

REPORT GENERATED ON

September 16, 2026 • 11:00 PM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com