

Date of Publication
August 10, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

03 to 09 AUGUST 2026

Table Of Contents

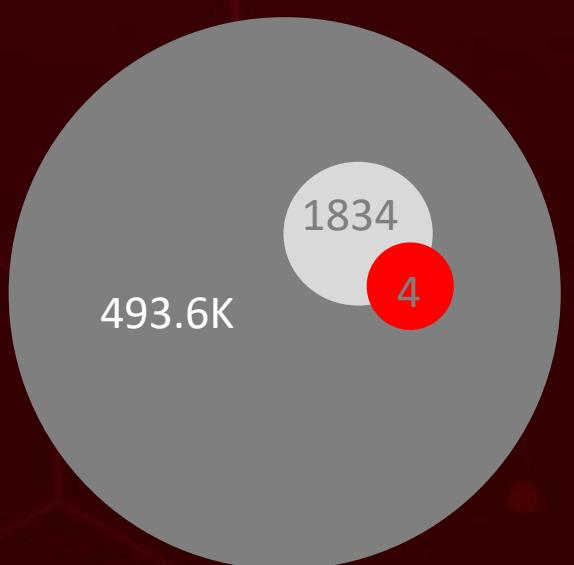
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	18
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	25

Summary

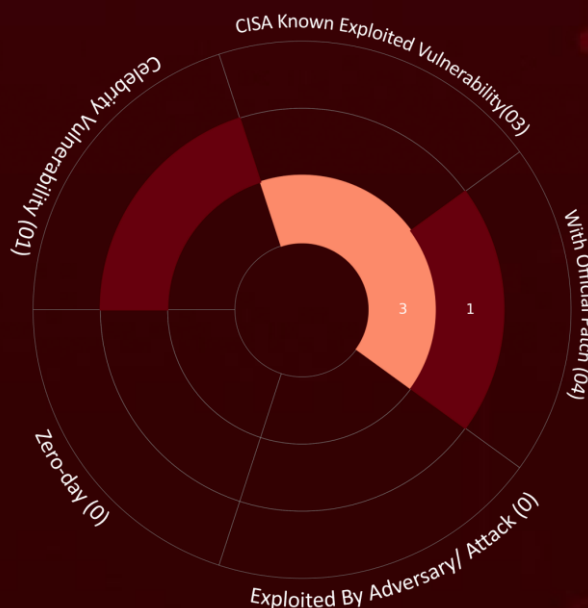
HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **six** major attacks were detected, **four** vulnerabilities were actively exploited, and **one** threat actor group was closely monitored,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

Among the most significant developments, attackers are actively exploiting **CVE-2026-63077**, a critical (CVSS 9.8) unauthenticated RCE flaw in JetBrains TeamCity On-Premises that bypasses authentication to run arbitrary commands with server privileges, exposing credentials and CI/CD pipelines. In parallel, **CVE-2026-18577**, an authentication bypass in N-able N-central, is being exploited to seize full administrative control of the RMM console and pivot into managed endpoints, including domain controllers.

Meanwhile, **ChainDrop**, a self-propagating Shai-Hulud npm worm, poisoned the keyv package family within hours, compromising over two billion monthly installs to steal developer and cloud credentials. Researchers also tracked **Mirage Kitten (aka UNC1549)**, an Iranian state-backed group deploying the NightLedger backdoor and custom tunnelers against defense and government targets across the Middle East, Africa, and South Asia. Together, these incidents reinforce the need for timely patching, continuous monitoring, and layered security defenses.



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



High Level Statistics

6

Attacks
Executed

4

Vulnerabilities
Exploited

1

Adversaries in
Action

- [NightLedger](#)
- [BridgeHead](#)
- [ArcBridge](#)
- [ChainDrop](#)
- [FDMP](#)
- [XCSSET](#)

- [CVE-2026-18577](#)
- [CVE-2026-18556](#)
- [CVE-2026-66066](#)
- [CVE-2026-63077](#)

- [Mirage Kitten](#)



Insights

CVE-2026-63077,

a critical unauthenticated RCE in JetBrains TeamCity On-Premises, is under active exploitation to hijack build servers and expose CI/CD credentials.

A **macOS ClickFix campaign** used fake CAPTCHA prompts to install a Go-based stealer that drains cryptocurrency wallets a fraction at a time to evade notice.

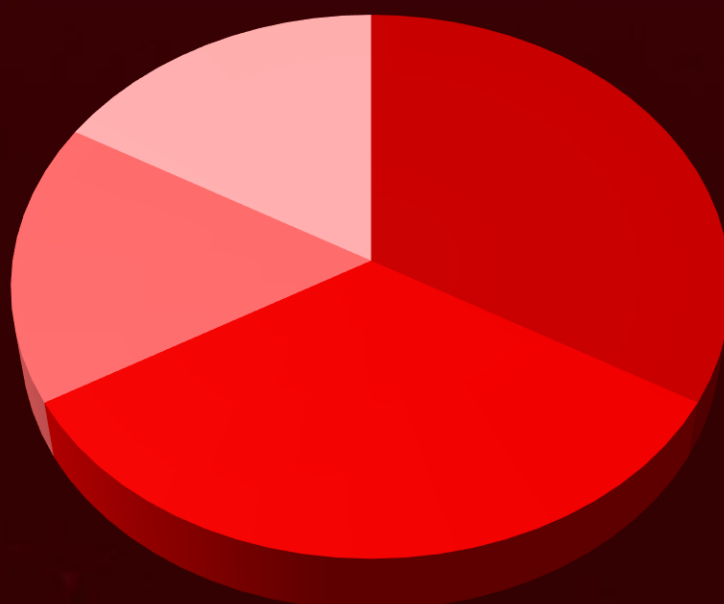
XCSSET returned in a stealthier v40 build that blocks macOS security updates while spreading through poisoned Xcode projects.

ChainDrop, a self-propagating Shai-Hulud npm worm, poisoned the keyv package family within hours, weaponizing over two billion monthly installs to steal developer and cloud credentials.

Mirage Kitten (UNC1549), an Iranian state-backed group, deployed the NightLedger backdoor and custom tunnelers against defense and government targets across the Middle East, Africa, and South Asia.

CVE-2026-18577 is being exploited to bypass authentication in N-able N-central, giving attackers full admin control and a pivot into managed domain controllers.

Threat Distribution



■ Backdoor

■ Tunneling tool

■ Modular

■ Worm

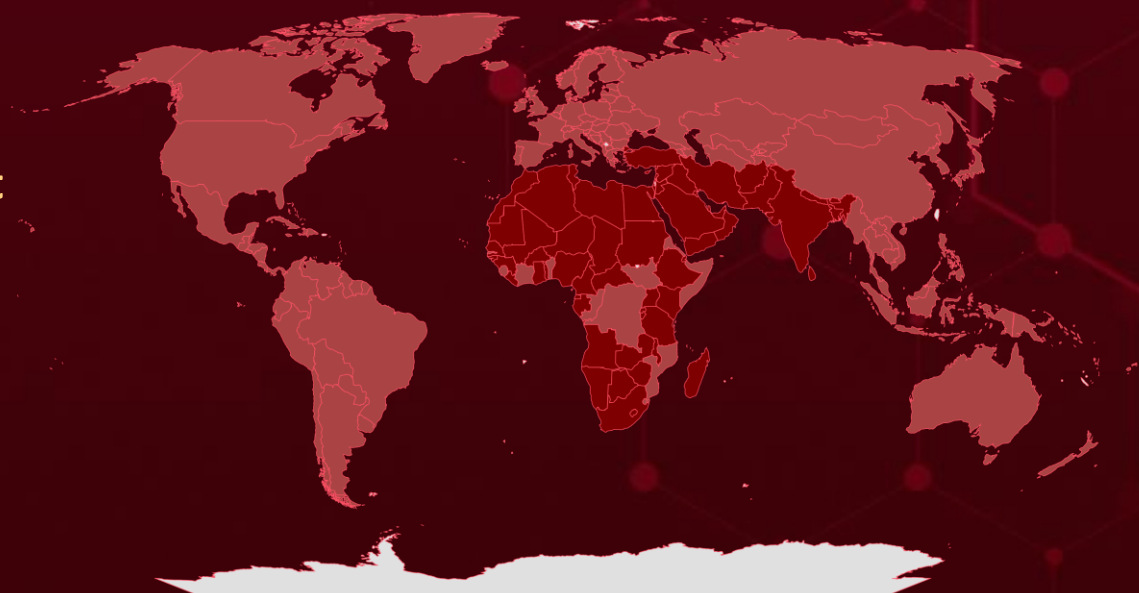


Targeted Countries

Most



Least

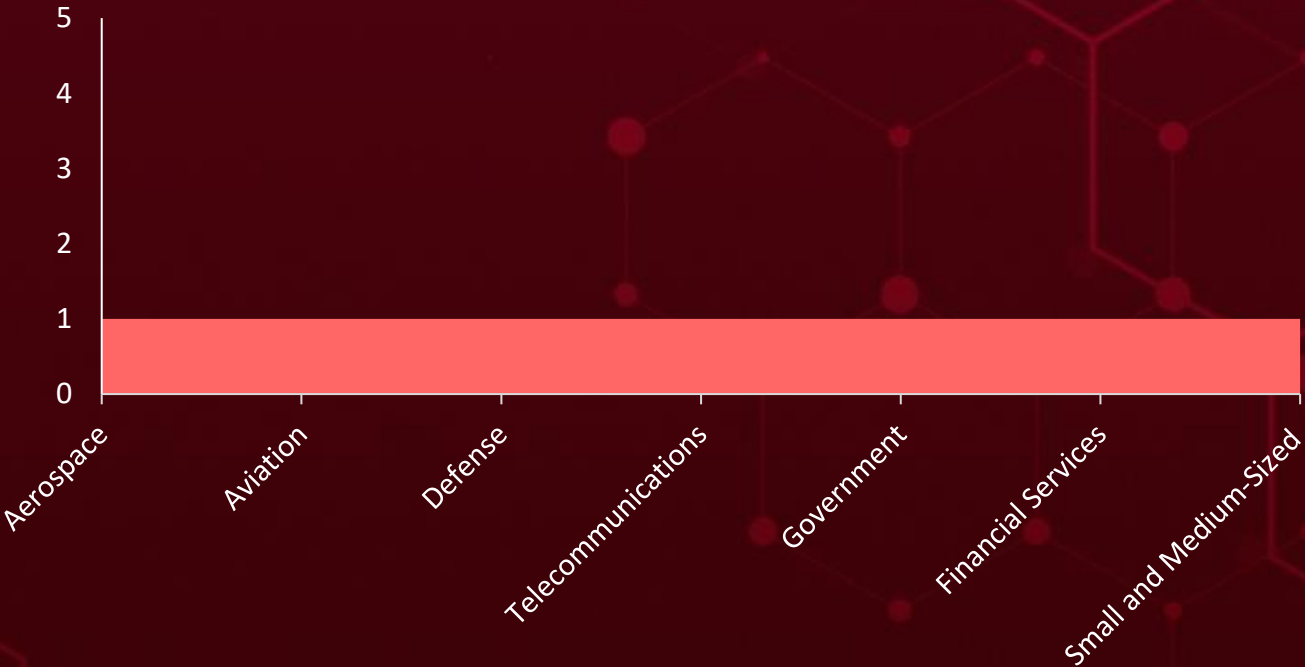


Powered by Bing

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

Countries	Countries	Countries	Countries
Zimbabwe	Sudan	Iraq	Germany
Rwanda	Comoros	Sri Lanka	St. Vincent & Grenadines
Morocco	Tunisia	Israel	Benin
Algeria	Cyprus	Syria	Turkmenistan
Tanzania	Yemen	Jordan	Greece
Angola	Djibouti	Togo	French Guiana
Maldives	Libya	Kenya	Greenland
Bahrain	Egypt	Turkey	Peru
Nigeria	Malawi	Kuwait	Grenada
Bangladesh	Equatorial Guinea	United Arab Emirates	Saint Kitts & Nevis
South Africa	Mali	Lebanon	Guatemala
Bhutan	Ethiopia	Zambia	Dominica
Uganda	Mauritius	Afghanistan	Albania
Botswana	Gabon	Liberia	South Korea
Madagascar	Namibia	Lesotho	Bolivia
Burkina Faso	Ghana	Uzbekistan	Sweden
Mauritania	Niger	Slovenia	Guyana
Burundi	Guinea	Czech Republic	Tonga
Nepal	Oman	Belize	Haiti
Cameroon	Guinea-Bissau	El Salvador	Belgium
Pakistan	Qatar	Gambia	Holy See
Central African Republic	India	Palau	Fiji
Senegal	Saudi Arabia	Georgia	Honduras
Chad	Iran	Sao Tome & Principe	Norway
	Seychelles		

Targeted Industries



TOP MITRE ATT&CK TTPs

<u>T1059</u> Command and Scripting Interpreter	<u>T1036</u> Masquerading	<u>T1005</u> Data from Local System	<u>T1071</u> Application Layer Protocol	<u>T1027</u> Obfuscated Files or Information
<u>T1071.001</u> Web Protocols	<u>T1195</u> Supply Chain Compromise	<u>T1036.005</u> Match Legitimate Name or Location	<u>T1082</u> System Information Discovery	<u>T1552</u> Unsecured Credentials
<u>T1190</u> Exploit Public-Facing Application	<u>T1083</u> File and Directory Discovery	<u>T1041</u> Exfiltration Over C2 Channel	<u>T1555</u> Credentials from Password Stores	<u>T1033</u> System Owner/User Discovery
<u>T1195.002</u> Compromise Software Supply Chain	<u>T1059.007</u> JavaScript	<u>T1574</u> Hijack Execution Flow	<u>T1204</u> User Execution	<u>T1057</u> Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
NightLedger	NightLedger is a previously undocumented Windows backdoor. It masquerades as SspiCli.dll and is designed for DLL search-order hijacking against the legitimate AppVShNotify.exe, abusing the fact that RPCRT4.dll can delay-load SspiCli.dll during authenticated RPC calls, while forwarding expected exports to the real DLL. A UUID-style mutex enforces a single running instance. Functionally, it adds screenshot capture and collection of NetSetup.log on top of TWOSTROKE's core command set.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
SHA256	24771d0a69e442b9493ab1406e0253be1acd31d83f593177fd736f7f6d629ed9		

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>BridgeHead</u>	BridgeHead is a custom WebSocket-based tunneling tool, observed as a side-loaded DLL unbcl.dll under %LocalAppData%\Microsoft\VisualStudio on an Egyptian host, and libwinpthread-1.dll inside a univpn directory in a Pakistan-based environment. Before activating, it dynamically resolves GetUserNamedA from advapi32.dll, lowercases the current Windows username, and checks it for a hardcoded substring; if the match fails, it exits evidence of prior internal reconnaissance silently, per-target tailoring of each binary, and an anti-sandbox guard.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Tunneling tool		Network pivoting, Traffic relay, Perimeter bypass	Windows
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
SHA256	d80c6f338ecf4997d5dfce92bde9303578982fa6d20e49d3538a269d7f7a048d, 78e1d5640936f65071dba0e99abfe85b61a7b1156bfca266edb55585cecf0a3		

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
ArcBridge	ArcBridge is a custom WebSocket tunneling tool, first identified in April 2026 in activity against victims in the Middle East. On execution it creates the mutex to enforce single-instance execution the UUID-style naming convention matching the NightLedger backdoor and reinforcing common authorship.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Tunneling tool		Network pivoting, Traffic relay, Perimeter bypass	Windows
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-
IOC TYPE	VALUE		
SHA256	0258c24048532e2c6dcd20f15162406e71f9e78763fb256772e4b9c336339fe2, f714881161b8249ceb480da57d9f5ed461157d8ccc6080588af7c6a9a9428f6d		

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
ChainDrop	ChainDrop is a self-propagating Shai-Hulud npm worm that harvests developer and cloud credentials via a malicious preinstall hook, then reuses stolen tokens to republish itself across additional packages and repositories. Exfiltrated data is RSA-encrypted and routed through an Ethereum smart contract (EtherHiding) for C2 rotation.	Malicious npm preinstall hook	-
TYPE		IMPACT	AFFECTED PLATFORM
worm		Credential theft, supply chain compromise	npm keyv/cacheable ecosystem
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2caa93012b350668		

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>FDMTP</u>	FDMTP is a backdoor malware that lets attackers secretly control an infected Windows computer. It first checks the victim's device to make sure it's a real target, then quietly reports back details like the computer's username, installed antivirus, and network info to the attacker's server. From there, it can download more malicious tools, stay hidden using scheduled tasks and registry tricks, and give the attacker ongoing access to spy on or further compromise the system.	Through a compromised version of QuickFox	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	795594ad5e6f2868cc4d8ed12dabf4f3999a1477c6b250527c5ede9a98528fb9		

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>XCSSET</u>	Modular macOS malware family that infects Xcode projects and executes when the project is compiled, active since August 2020. The latest version is v40, tracked from mid-April 2026 across two waves, adding polymorphic payloads, fileless persistence, a Chrome backdoor, and a Telegram trojanizer.	Supply chain compromise (Xcode projects)	-
TYPE		IMPACT	AFFECTED PLATFORM
Modular		Information theft, Defenses disabled	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	ac3467a04eeb552d92651af1187bdc795100ea77a7a1ac755b4681c654b54692, d11a549e6bc913c78673f4e142e577f372311404766be8a3153792de9f00f6c1		

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-2026-18577</u>		N-able N-central (Before 2026.3.1.7)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*	-
N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1057: Process Discovery	https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-18556</u>		N-able N-central (Before 2026.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*	-
N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-66066</u>	KindaRails2Shell	Ruby on Rails Active Storage, all versions before 7.2.3.2; version 8.0 and later, before 8.0.5.1; and version 8.1 and later, before 8.1.3.1.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rubyonrails:rails:- .*.*.*.*.*.*	-
Ruby on Rails Active Storage Arbitrary File Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1188	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1083: File and Directory Discovery, T1005: Data from Local System	https://github.com/rails/rails/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-63077</u>		JetBrains TeamCity On-Premises (all versions before 2025.11.7 and before 2026.1.3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*	-
JetBrains TeamCity Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1195: Supply Chain Compromise, T1059: Command and Scripting Interpreter	https://www.jetbrains.com/teamcity/download/other/



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Mirage Kitten</u> (aka <u>UNC1549</u>, <u>TA455</u>, <u>Smoke</u> <u>Sandstorm</u>, <u>Bohrium</u>, <u>DEV-0056</u>, <u>Yellow</u> <u>Dev 13</u>, <u>Subtle</u> <u>Snail</u>, <u>Nimbus</u> <u>Manticore</u>, <u>Screening</u> <u>Serpens</u>, <u>GalaxyGato</u>)	Iran	Aerospace, Aviation, Defense, Telecommunications , Government, Financial Services, Small and Medium-Sized Business	Cameroon, Sudan, Iran, Iraq, Seychelles, Ghana, India, Turkey, Comoros, Central African Republic, Yemen, Guinea, Madagascar, Equatorial Guinea, Saudi Arabia, Malawi, Kuwait, Bhutan, Sri Lanka, United Arab Emirates, Palestine, Liberia, Bangladesh, Mauritania, Oman, Morocco, Lesotho, Tanzania, Bahrain, Angola, Syria, Mali, Nepal, Mauritius, Guinea-Bissau, Senegal, South Africa, Cyprus, Gabon, Algeria, Burundi, Egypt, Libya, Pakistan, Qatar, Nigeria, Togo, Lebanon, Botswana, Israel, Uganda, Zambia, Maldives, Namibia, Ethiopia, Afghanistan, Chad, Ivory Coast, La Reunion, Cape Verde, Jordan, Tunisia, Niger, Rwanda, Kenya, Djibouti, Akrotiri and Dhekelia, Burkina Faso, Democratic Republic of Congo, Zimbabwe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	NightLedger, BridgeHead, ArcBridge	Windows
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0007: Discovery, TA0009: Collection, TA0010: Exfiltration, TA0011: Command and Control, T1583: Acquire Infrastructure, T1566: Phishing, T1204: User Execution, T1129: Shared Modules, T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow, T1497: Virtualization/Sandbox Evasion, T1027: Obfuscated/Encoded Files or Information, T1036: Masquerading, T1082: System Information Discovery, T1083: File and Directory Discovery, T1057: Process Discovery, T1113: Screen Capture, T1005: Data from Local System, T1583.001: Domains, T1583.006: Web Services, T1566.002: Spearphishing Link, T1204.002: Malicious File, T1574.002: DLL, T1497.001: System Checks, T1036.005: Match Legitimate Resource Name or Location, T1071: Application Layer Protocol, T1572: Protocol Tunneling, T1090: Proxy, T1105: Ingress Tool Transfer, T1041: Exfiltration Over C2 Channel, T1071.001: Web Protocols			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actor **Mirage Kitten**, and malware **NightLedger**, **BridgeHead**, **ArcBridge**, **XCSSET**, **ChainDrop**, and **FDMTF**.

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 **four exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Mirage Kitten**, and malware **NightLedger**, **XCSSET**, **ChainDrop**, and **FDMTF** in Breach and Attack Simulation(BAS).

Threat Advisories

[N-able Confirms Active Exploitation of N-central Authentication Bypass Flaw](#)

[Mirage Kitten Marks New Territory Across the Middle East and Africa](#)

[ChainDrop: Shai-Hulud npm Supply Chain Worm Compromises keyv Ecosystem](#)

[A Fake Update, a Real Threat: The FDMTP Backdoor's Supply Chain Run](#)

[XCSSET v40 Locks macOS Out of Its Own Security Updates](#)

[Fake CAPTCHA, Real Theft: macOS ClickFix Drains Crypto Wallets](#)

[Unsafe by Default: KindaRails2Shell Exposes Ruby on Rails to File Read and RCE](#)

[CVE-2026-63077: Critical TeamCity On-Premises RCE Under Active Exploitation](#)

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>NightLedger</u>	SHA256	24771d0a69e442b9493ab1406e0253be1acd31d83f593177fd736f7f6d629ed9
	MD5	A239E655709A2518DD0B7BDBED163679
<u>BridgeHead</u>	SHA256	d80c6f338ecf4997d5dfce92bde9303578982fa6d20e49d3538a269d7f7a048d, 78e1d5640936f65071dba0e99abfe85b61a7b1156bfca266edb55585cecf0a3, f0c0357b12b5e6125bf97f6806f91e9183cac133600b2d9c46a7a0a2da997754
	MD5	5FA15EF96808EA82F0A6176F0BB4B386, 42F847597109DA2A220391BB09D00676, AFB1C1583606599C7272CFB33CC6F498
<u>ArcBridge</u>	SHA256	0258c24048532e2c6dcd20f15162406e71f9e78763fb256772e4b9c336339fe2

Attack Name	TYPE	VALUE
<u>ArcBridge</u>	SHA256	f714881161b8249ceb480da57d9f5ed461157d8ccc6080588af7c6a9a9428f6d, 87fa75eaa5d538826570ac7d4f0bcf58879183bac90c068f1b7477883296c416, e0e98bde358a6cf02c36a794021dfd921a7f55c5c7a0a4cd241e9568ed4a4016, 2592f40a2ee9dde24eb966c5b0b1afe7ddbc8e80aee4662e68295ad1608a79ee
	MD5	6038D42AF0AFFD1FB263F470C0956F6B, AE628EFA305387B633DCE82F9364875B, F7D36CC5904A53252D2BB3D21615134F, C90F0EFADBF322E5EB1C4103A38C30E6, D09B14A2FE01C7363ECC56F5D046162C
<u>XCSSET</u>	SHA256	ac3467a04eeb552d92651af1187bdc795100ea77a7a1ac755b4681c654b54692, d11a549e6bc913c78673f4e142e577f372311404766be8a3153792de9f00f6c1, 172eb05a2f72cb89e38be3ac91fd13929ee536073d1fe576bc8b8d8d6ec6c262, a238ed8a801e48300169afae7d27b5e49a946661ed91fab4f792e99243fbc28d
	Domains	accapple[.]ru, adschecks[.]ru, adschecks.ru, adsmobi[.]ru, adsmorein[.]in, adsmoreme[.]in, amdcnd[.]ru, amzndev[.]in, amzndev[.]ru, amznprod[.]in

Attack Name	TYPE	VALUE
<u>XCSSET</u>	Domains	applecdn[.]ru, appledisk[.]ru, appledns[.]ru, applehosts[.]ru, appletime[.]in, bulksec[.]ru, cdnamz[.]in, cdnamz[.]ru, cdnapple[.]in, cdnatapple[.]ru, cdnroute[.]ru, checkcdn[.]ru, chromeads[.]ru, cnmag[.]ru, devnetaps[.]ru, dnsapple[.]ru, dnsrelays[.]ru, explorecdn[.]ru, fiddlejoy[.]ru, figmacat[.]ru, figmanets[.]in, funchats[.]ru, gironetcdn[.]ru, goalmate[.]ru, googlenets[.]ru, greencn[.]ru, icloudsnet[.]ru, imails[.]ru, legalads[.]in, littleads[.]in, littledns[.]ru, maganet[.]ru, mindelgate[.]ru

Attack Name	TYPE	VALUE
<u>XCSSET</u>	Domain s	netapsdev[.]ru, netcdnads[.]in, netcdnamz[.]ru, netcdndev[.]in, netcorps[.]ru, netsprot[.]in, netsproto[.]in, networkads[.]in, rigacdn[.]in, rigmajoy[.]in, rigmanet[.]ru, rigmanets[.]in, sahusuzuki[.]in, stuffdns[.]in, testjoys[.]ru, timewebnet[.]in, vigmanet[.]ru, whitead[.]in, whiteads[.]ru, windcdn[.]ru, windsecure[.]ru
<u>ChainDrop</u>	SHA256	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2caa93012b, 350668, fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda806e56, 84b1eb, 9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367cfc2509c, f1bcc
<u>FDMTTP</u>	SHA256	795594ad5e6f2868cc4d8ed12dabf4f3999a1477c6b250527c5ede9a98 528fb9

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

August 10, 2026 • 09:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com