

Date of Publication
June 1, 2026



HiveForce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

MAY 2026

Table Of Contents

<u>Summary</u>	03
<u>Insights</u>	04
<u>Threat Distribution</u>	05
<u>Celebrity Vulnerabilities</u>	06
<u>Vulnerabilities Summary</u>	16
<u>Attacks Summary</u>	21
<u>Adversaries Summary</u>	23
<u>Targeted Products</u>	25
<u>Targeted Countries</u>	28
<u>Targeted Industries</u>	29
<u>Top MITRE ATT&CK TTPs</u>	30
<u>Top Indicators of Compromise (IOCs)</u>	31
<u>Vulnerabilities Exploited</u>	32
<u>Attacks Executed</u>	44
<u>Adversaries in Action</u>	53
<u>MITRE ATT&CK TTPs</u>	61
<u>Top 5 Takeaways</u>	70
<u>Recommendations</u>	71
<u>Appendix</u>	72
<u>Indicators of Compromise (IoCs)</u>	73
<u>What Next?</u>	77

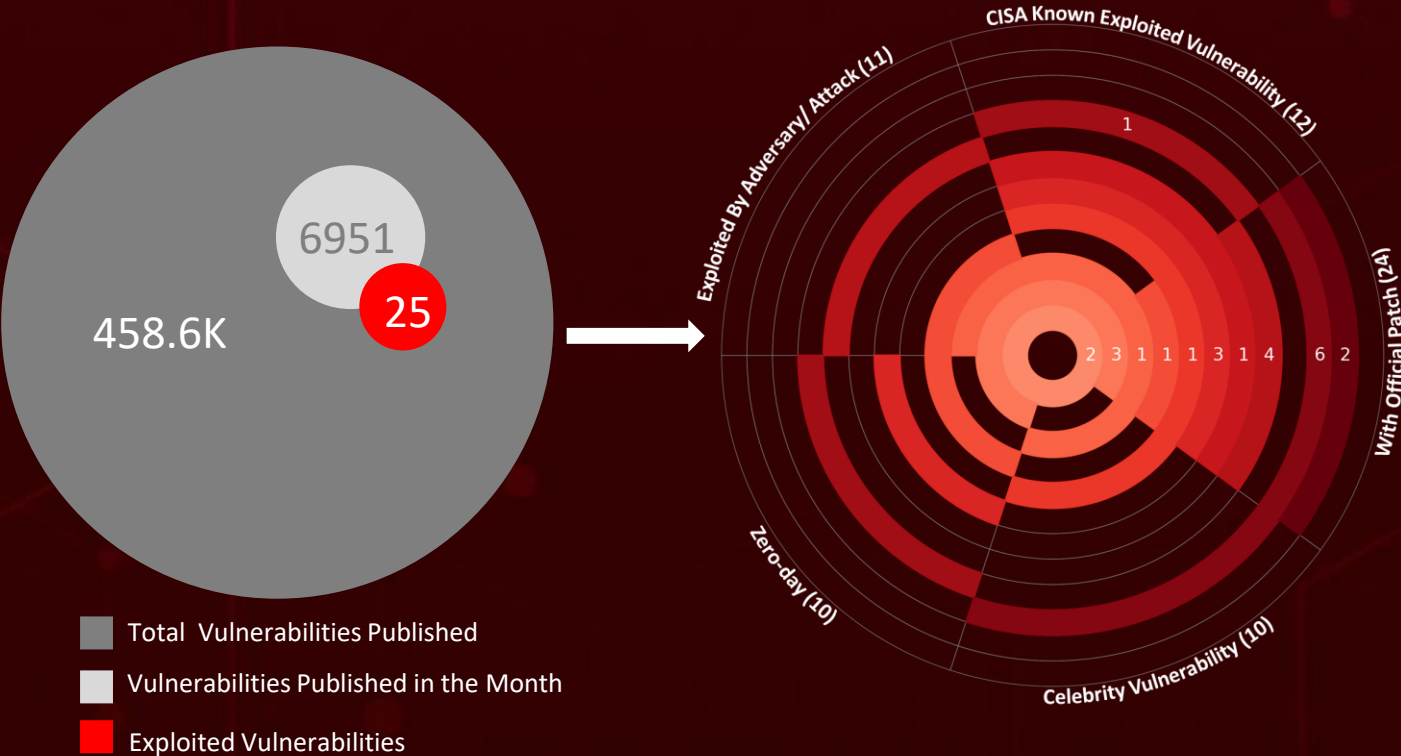
Summary

May reshaped the cybersecurity landscape with active exploitation of **ten** celebrity vulnerabilities and **10** zero-days. The standout threat, **CVE-2026-31431, "Copy Fail"** a critical Linux kernel privilege-escalation flaw in the algif_aead crypto module that lets an unprivileged user gain root via a 732-byte Python exploit, affecting virtually every major Linux distribution shipped since 2017.

Meanwhile, **CVE-2026-0300** PAN-OS Zero-Day, a likely state-sponsored cluster tracked as **CL-STA-1132**, exploited an unauthenticated buffer overflow in the User-ID Authentication Portal since April 9, gaining root on internet-exposed firewalls, injecting shellcode into nginx, deploying EarthWorm and ReverseSocks5 tunnels, enumerating Active Directory, and systematically destroying forensic evidence.

Meanwhile, financially motivated threat groups are becoming increasingly aggressive and innovative. **TeamPCP** intensified its supply chain attacks throughout May 2026, the group allegedly exfiltrated nearly 3,800 internal GitHub repositories through a poisoned VS Code extension and later open-sourced the worm with a \$1,000 underground bounty, rapidly fueling copycat campaigns.

China-linked APT **FamousSparrow** ran a three-wave intrusion against an Azerbaijani oil and gas firm (Dec 2025 - Feb 2026), repeatedly re-exploiting an unpatched Exchange Server via ProxyNotShell to deploy Deed RAT and Terndoor backdoors. The threat curve continues upward, and prioritized defensive adaptation is a mandatory baseline in today's operational environment.



In May 2026, a geopolitical cybersecurity landscape unfolds, revealing **India, the United States, the United Kingdom, Grenada, and Saint Lucia** as the top-targeted countries

Highlighted in **May 2026** is a cyber battleground encompassing the **Cryptocurrency, Financial, Technology, Government, and Healthcare** sectors, designating them as the top industries

84 Malicious Versions, 42 Packages: Inside the TeamPCP @tanstack Compromise

Fox Tempest: Malware-Signing-as-a-Service via Abused Microsoft Artifact Signing

17,000 Subscribers, One Operator, One Jailbroken AI: The **bandcamp** Story

CVE-2026-42945: Critical Heap Overflow in NGINX Under Active Exploitation

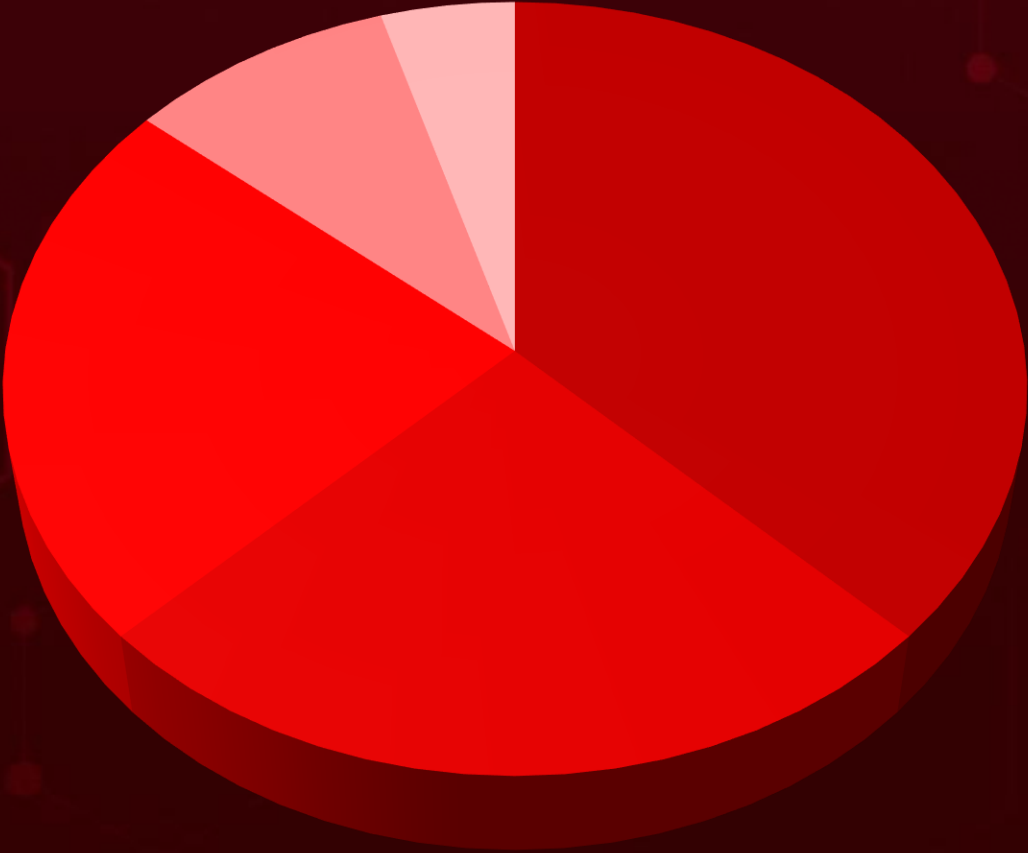
CVE-2026-42897: Actively Exploited OWA Spoofing Flaw in On-Prem Exchange

CVE-2026-20182: A Crafted Handshake Is All It Takes to Root Cisco SD-WAN

Copy Fail (CVE-2026-31431): A Single Kernel Flaw That Turns Containers into Root

CVE-2026-34926: Apex One Flaw Turns Your EDR Into a Malware Distributor

Threat Distribution





Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-31431</u>	Copy Fail	Linux Kernel versions shipped from 2017 through 6.18.21 and 6.19.11; fixed in 6.18.22, 6.19.12, and 7.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-669	T1068: Exploitation for Privilege Escalation, T1059.006 Command and Scripting Interpreter: Python	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=893d22e0135fa394db81df88697fba6032747667

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-43284</u>	Dirty Frag	Linux kernel (xfrm- ESP / Ipsec subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced January 2017 by commit cac2661c53f3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*	-
Linux Kernel xfrm-ESP In-Place Decrypt Page-Cache Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1068 - Exploitation for Privilege Escalation, T1078 - Valid Accounts, T1059 - Command and Scripting Interpreter	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=8253aab4659ca16116b522203c2a6b18dccacea7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-43500</u>	Dirty Frag	Linux kernel (RxRPC subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced June 2023)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel RxRPC In-Place Decrypt Page-Cache Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1068 - Exploitation for Privilege Escalation, T1611 - Escape to Host	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=d45179f8795222ce858770dc619abe51f9d24411

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-55182</u>	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	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:facebook:react:*:*:*:*:* *:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:* node.js:*:* cpe:2.3:a:remix:react_router:*:*:*:*	PCPJack
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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2022-41040</u>	ProxyNotShell	Microsoft Exchange Server	FamousSparrow
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Microsoft Exchange Server Server-Side Request Forgery Vulnerability		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	Deed RAT (aka Snappybee) Terndoor Mofu loader
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1552.005: Cloud Instance Metadata API	https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2022-41082</u>	ProxyNotShell	Microsoft Exchange Server	CL-STA-1132
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	Deed RAT (aka Snappybee) Terndoor Mofu loader
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42945</u>	NGINX Rift	NGINX Plus: R32 – R36 NGINX Open Source: 1.0.0 – 1.30.0, 0.6.27 – 0.9.7 NGINX Instance Manager: 2.16.0 – 2.22.0 F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0 F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*	-
F5 NGINX ngx_http_rewrite_module Heap-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://my.f5.com/manage/s/article/K000161019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-46300</u>	Fragnesia	Linux Kernel (XFRM ESP-in-TCP / `esp4`, `esp6`, `rxrpc` modules) – impacts AlmaLinux 8/9/10, AlmaLinux Kitten 10, Amazon Linux, CloudLinux, Debian, Fedora, Gentoo, openSUSE, Red Hat Enterprise Linux, SUSE, Ubuntu, and OpenShift	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel XFRM ESP-in-TCP Page- Cache Corruption Local Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	Alma Linux , Redhat , Ubuntu , SUSE , Debian , Amazon , Gentoo , Openwall , Kernel

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-31635</u>	DirtyDecrypt	Linux Kernel (6.16; 7.0-rc1 through 7.0-rc7; 6.19 before 6.19.13; 6.16.1 up to but excluding 6.18.23) - requires `CONFIG_RXGK` enabled	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel Local Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-130	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=e2f1a80d8b1ed6a5ae585a399c2b46500bdcc305

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-45185</u>	Dead.Letter	Exim Internet Mailer 4.97 through 4.99.2 (GnuTLS builds only)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:exim:exim:*:*:*:*:*:*	-
Exim Internet Mailer Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter, T1190: Exploit Public- Facing Application, T1203: Exploitation for Client Execution, T1082: System Information Discovery	https://exim.org/static/doc/security/EXIM-Security-2026-05-01.1/

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-31431	Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability	Linux Kernel			
CVE-2026-22679	Weaver (Fanwei) E-cology Remote Code Execution Vulnerability	Weaver (Fanwei) E-cology			
CVE-2026-0300	Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability	Palo Alto Networks PAN-OS (PA-Series, VM-Series)			
CVE-2026-40982	VMware Spring Cloud Config Server Path Traversal Vulnerability	VMware Spring Cloud Config Server			
CVE-2026-6973	Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability	Ivanti EPMM			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-43284	Linux Kernel xfrm-ESP In-Place Decrypt Page-Cache Write Vulnerability	Linux kernel (xfrm-ESP / Ipsec subsystem) kernel			
CVE-2026-43500	Linux Kernel RxRPC In-Place Decrypt Page-Cache Write Vulnerability	Linux kernel (RxRPC subsystem)			
CVE-2025-29927	Next.js Middleware Bypass Vulnerability	Next.js versions			
CVE-2025-55182	Meta React Server Components Remote Code Execution Vulnerability	react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack			
CVE-2026-1357	WordPress WPVivid Backup & Migration Unauthenticated Arbitrary File Upload Vulnerability	WordPress WPVivid Backup & Migration			
CVE-2025-9501	WordPress W3 Total Cache Command Injection Vulnerability	WordPress W3 Total Cache plugin			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-48703	CWP Control Web Panel OS Command Injection Vulnerability	CWP (aka Control Web Panel or CentOS Web Panel)			
CVE-2026-45321	TanStack Router npm Packages Embedded Malicious Code Vulnerability	TanStack Router npm Packages			
CVE-2026-20182	Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN			
CVE-2022-41040	Microsoft Exchange Server Server-Side Request Forgery Vulnerability	Microsoft Exchange Server			
CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server			
CVE-2026-42897	Microsoft Exchange Server Cross-Site Scripting Vulnerability	Microsoft Exchange Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-42945	F5 NGINX ngx_http_rewrite_module Heap-Based Buffer Overflow Vulnerability	NGINX Plus: R32 – R36NGINX			
CVE-2026-46300	Linux Kernel XFRM ESP-in-TCP Page-Cache Corruption Local Privilege Escalation Vulnerability	Linux Kernel			
CVE-2026-31635	Linux Kernel Local Privilege Escalation Vulnerability	Linux Kernel			
CVE-2026-45185	Exim Internet Mailer Use-After-Free Vulnerability	Exim Internet Mailer			
CVE-2026-48172	LiteSpeed User-End cPanel Plugin Privilege Escalation Vulnerability	LiteSpeed User-End cPanel Plugin			
CVE-2026-9082	Drupal Core SQL Injection Vulnerability	Drupal / Drupal Core			
CVE-2026-5426	Digital Knowledge KnowledgeDeliver Remote Code Execution Vulnerability	Digital Knowledge KnowledgeDeliver			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-34926	Apex One Server Directory Traversal Vulnerability	Trend Micro Apex One (On-Premise)			

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
ValleyRAT	Backdoor	-	Windows	-	Phishing
ABCDoor	Backdoor	-	Windows	-	Phishing
RustSL	Loader	-	Windows	-	Phishing
EarthWorm	Tunneling tool	CVE-2026-0300	Palo Alto Networks PAN-OS		-
ReverseSocks5	Tunneling tool	CVE-2026-0300	Palo Alto Networks PAN-OS		-
TCLBANKER	Banking Trojan	-	Windows	-	Trojanized MSI Installer
Quasar Linux	RAT	-	npm, PyPI, GitHub, AWS, Docker, Kubernetes, Git, HashiCorp Vault, Terraform	-	-
PCPJack	Framework	CVE-2025-29927 CVE-2025-55182 CVE-2026-1357 CVE-2025-9501 CVE-2025-48703	Docker, Kubernetes, Redis, MongoDB, RayML, Next.js, React, WordPress (WPVivid Backup, W3 Total Cache), CentOS Web Panel (CWP)		Dropper
Mini Shai-Hulud	Worm	CVE-2026-45321	TanStack Router npm Packages		Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Deed RAT	Modular Backdoor	CVE-2022-41040 CVE-2022-41082	Windows		Exploiting Vulnerabilities
Terndoor	Backdoor	CVE-2022-41040 CVE-2022-41082	Windows		Exploiting Vulnerabilities
Mofu Loader	Loader	CVE-2022-41040 CVE-2022-41082	Windows		Exploiting Vulnerabilities
SHub Reaper	Infostealer	-	macOS	-	Social Engineering
StellarMonster	RAT	-	Telegram, Truth Social, Windows, WordPress	-	Phishing
BLUEBEAM	Web shell	CVE-2026-5426	Digital Knowledge KnowledgeDeliver		Exploiting Vulnerability

Adversaries Summary

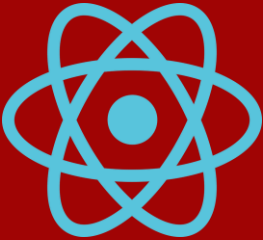
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Silver Fox	Information theft and espionage	China	-	ValleyRAT, ABCDoor, RustSL	Windows
CL-STA-1132	Espionage	-	CVE-2026-0300	EarthWorm, ReverseSocks5	Palo Alto Networks PAN-OS
TeamPCP	Espionage, Sabotage, Disruption, Financial Gains	-	CVE-2026-45321	Mini Shai-Hulud Worm	TanStack Router npm Packages
UAT-8616	Information theft and Espionage	-	CVE-2026-20182	-	Cisco Catalyst SD-WAN Controller / Manager
FamousSparrow	Information Theft, Espionage	China	CVE-2022-41040 CVE-2022-41082	Malware: Deed RAT (aka Snappybee), Terndoor, Mofu loader	Microsoft Exchange Server
Storm-2949	Information Theft and Espionage	-	-	-	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Fox Tempest	Financial Gains	-	-	-	AnyDesk, Microsoft Teams, PuTTY, Webex (impersonated as lures)
bandcampro	Financial Gains, Information Theft and Espionage	Russia	-	StellarMonster	Telegram, Truth Social, Windows, WordPress



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	Linux Kernel versions shipped from 2017 through 6.18.21 and 6.19.11; fixed in 6.18.22, 6.19.12, and 7.0), Linux kernel (xfrm-ESP / Ipsec subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced January 2017 by commit cac2661c53f3), Linux kernel (RxRPC subsystem) kernel versions 4.10 through 7.0 (vulnerable code introduced June 2023), Linux Kernel (XFRM ESP-in-TCP / `esp4`, `esp6`, `rxrpc` modules) – impacts, Linux Kernel (6.16; 7.0-rc1 through 7.0-rc7; 6.19 before 6.19.13; 6.16.1 up to but excluding 6.18.23) - requires `CONFIG_RXGK` enabled
	Application	Weaver (Fanwei) E-cology 10.0 versions prior to 20260312
	Operating System	Palo Alto Networks PAN-OS (PA-Series, VM-Series) Versions 10.2.x, 11.1.x, 11.2.x, 12.1.x
	Application	VMware Spring Cloud Config Server 3.1.0 through 3.1.13; 4.1.0 through 4.1.9; 4.2.0 through 4.2.6; 4.3.0 through 4.3.2; 5.0.0 through 5.0.2; and older unsupported versions

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Enterprise Management Platform	Ivanti EPMM (Before 12.6.1.1, 12.7.0.1, 12.8.0.1)
	Software libraries	Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0, Next.js versions: 14.3.0- canary.77+, 15.x, 16.x (before 16.0.7)
	Software libraries	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 React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc
	Software	WordPress WPVivid Backup & Migration, WordPress W3 Total Cache plugin before 2.8.13
	Application	CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205
	Application	TanStack Router npm Packages
	Network Device	Cisco Catalyst SD-WAN before 20.9.9.1, before 20.12.7.1, before 20.12.7.1, before 20.12.5.4, 20.12.6.2, 20.12.7.1, before 20.15.5.2, before 20.15.5.2, before 20.15.4.4, 20.15.5.2, before 20.18.2.2, before 20.18.2.2, before 26.1.1.1
	Mail & Collaboration Server	Microsoft Exchange Server 2016 (all update levels), Microsoft Exchange Server 2019 (all update levels), Microsoft Exchange Server Subscription Edition (all update levels)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Load Balancer / Web Server / API Gateway	NGINX Plus: R32 – R36 NGINX Open Source: 1.0.0 – 1.30.0, 0.6.27 – 0.9.7
	Management & Monitoring Tool	NGINX Instance Manager: 2.16.0 – 2.22.0F5
	Kubernetes Ingress Controller	NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2
	Security Software Products	WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2
	Mail Transfer Agent (MTA) software	Exim Internet Mailer 4.97 through 4.99.2 (GnuTLS builds only)
	cPanel Plugin	LiteSpeed User-End cPanel Plugin (versions 2.3 through 2.4.4, i.e. before 2.4.5)
	Content Management System (CMS)	Drupal core: from 8.9.0 before 10.4.10, from 10.5.0 before 10.5.10, from 10.6.0 before 10.6.9, from 11.0.0 before 11.1.10, from 11.2.0 before 11.2.12, from 11.3.0 before 11.3.10.
	Software	Digital Knowledge KnowledgeDeliver (Before February 24, 2026)
	Endpoint security software	Trend Micro Apex One 2019 (On-Premise) - Server and Agent builds below 17079

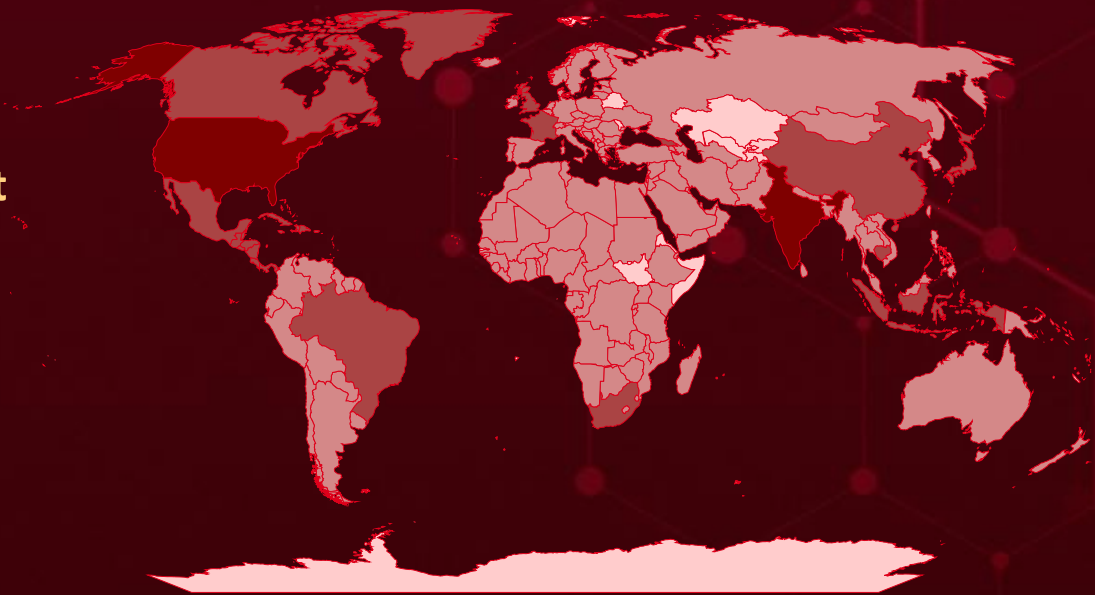


Targeted Countries

Most



Least



Powered by Bing

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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	India		British Virgin Islands		El Salvador		Tokelau		Faroe Islands
	United States		Greenland		Trinidad and Tobago		Denmark		Monaco
	United Kingdom		Cambodia		France		Montenegro		Fiji
	Grenada		Guadeloupe		Georgia		Djibouti		Morocco
	Saint Lucia		Canada		United States Virgin Islands		Netherland Antilles		Finland
	Anguilla		Haiti		Scotland		Belgium		Nauru
	Honduras		Cayman Islands		Niger		Northern Cyprus		Argentina
	Antigua and Barbuda		Indonesia		Ukraine		American Samoa		New Zealand
	Nicaragua		China		Bahrain		Paraguay		French Guiana
	Aruba		Japan		Portugal		Ecuador		North Korea
	Turks and Caicos Islands		Costa Rica		Croatia		Romania		Gabon
	Bahamas		Martinique		Switzerland		Egypt		Norway
	Guatemala		Cuba		Bangladesh		Chile		Bhutan
	Barbados		Montserrat		Myanmar		Benin		Cape Verde
	Jamaica		Curacao		Algeria		Sierra Leone		Germany
	Belize		Panama		Pakistan		Equatorial Guinea		Philippines
	Mexico		Dominica		Cyprus		Sudan		Ghana
	Bermuda		Saint Kitts and Nevis		Saint Eustatius		Estonia		Qatar
	Puerto Rico		Dominican Republic		Czech Republic		Thailand		Gibraltar
	Brazil		Saint Vincent and the Grenadines		Angola		Ethiopia		Rwanda
	South Africa				Democratic Republic of Congo		Turkey		Greece
									Chad
									Bolivia

Targeted Industries

Most



Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1036

Masquerading

T1068

Exploitation for Privilege Escalation

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1071.001

Web Protocols

T1082

System Information Discovery

T1036.005

Match Legitimate Name or Location

T1027

Obfuscated Files or Information

T1552

Unsecured Credentials

T1041

Exfiltration Over C2 Channel

T1078

Valid Accounts

T1204

User Execution

T1059.006

Python

T1059.001

PowerShell

T1552.001

Credentials In Files

T1204.002

Malicious File

T1543

Create or Modify System Process

T1566

Phishing

T1005

Data from Local System

T1059.004

Unix Shell

T1611

Escape to Host

T1567

Exfiltration Over Web Service



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>ABCDoor</u>	IPv4:Port	45[.]118[.]133[.]203[:]5000
	Domains	abc[.]fetish-friends[.]com, abc[.]3mkoreald[.]com, abc[.]sudsmama[.]com, abc[.]woopami[.]com, abc[.]ilptour[.]com, abc[.]petitechanson[.]com, abc[.]doublemobile[.]com
	MD5	04194F8DDD0518FD8005F0E87AE96335, F15A67899CFE4DECFF76D4CD1677C254, 11705121F64FA36F1E9D7E59867B0724, 13669B8F2BD0AF53A3FE9AC0490499E5, 5B998A5BC5AD1C550564294034D4A62C, C50C980D3F4B7ED970F083B0D37A6A6A, DE8F0008B15F2404F721F76FAC34456A, 9BF9F635019494C4B70FB0A7C0FB53E4, A543B96B0938DE798DD4F683DD92A94A, FA08B243F12E31940B8B4B82D3498804
<u>EarthWorm</u>	URL	hxxp[:]//146[.]70[.]100[.]69[:]8000/php_sess
	SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63 dcd84f97a584
<u>ReverseSocks5</u>	URL	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/do wnload/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz
<u>Quasar Linux</u>	MD5	70f70743f287a837d17c56933152a8a6
	SHA1	b0f2c668cbdd63a871c90592b6c93e931115872e
	SHA256	ea1d34b21b739a6bbf89b3f7e67978005cf7f3eda612cefc7eac 1c8ead7c5545
<u>PCPJack</u>	Domain	cdn[.]cloudfront-js[.]com
	SHA256	b1d8149e5c7b6312f40c220e89b1913762f9aa416ff491540b3 b7b7040260eb5
<u>Mini Shai-Hulud</u>	SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b9 0f2fa8601266c, e7347d90653efc565f03733a95e9209d78f9cfa81e31ff2b2dd9 d48d75a4b8b1



Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-22679</u>		Weaver (Fanwei) E-cology 10.0 versions prior to 20260312	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:weaver:e-cology:*:*:*:*:*:*	-
Weaver (Fanwei) E-cology Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.001: Command and Scripting Interpreter: PowerShell, T1105: Ingress Tool Transfer, T1036: Masquerading	https://www.weaver.com.cn/cs/securityDownload.html#

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-40982</u>		VMware Spring Cloud Config Server 3.1.0 through 3.1.13; 4.1.0 through 4.1.9; 4.2.0 through 4.2.6; 4.3.0 through 4.3.2; 5.0.0 through 5.0.2; and older unsupported versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:spring_cloud_config:*:*:*:*:*:*	-
VMware Spring Cloud Config Server Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery, T1005: Data from Local System	https://github.com/spring-cloud/spring-cloud-config/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-6973</u>		Ivanti EPMM (Before 12.6.1.1, 12.7.0.1, 12.8.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:endpoint_manager_mobile:*.~.*.*.*.*.*.*	-
Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1078: Valid Accounts, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-29927</u>		Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vercel:next.js:-.*.*.*.*.*.*.*	PCPJack
Next.js Middleware 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
<u>CVE-2026-1357</u>		WordPress WPVivid Backup & Migration	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wpvivid:wpvivid_backup_plugin:*:*:*:*:wordpress:*:*	PCPJack
WordPress WPVivid Backup & Migration Unauthenticated Arbitrary File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190 - Exploit Public-Facing Application, T1505 - Server Software Component, T1505.003 - Web Shell	https://wordpress.org/plugins/wpvivid-backuprestore/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-9501</u>		WordPress W3 Total Cache plugin before 2.8.13	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:boldgrid:w3_total_cache:*:*:*:*:wordpress:*:*	PCPJack
WordPress W3 Total Cache Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190 - Exploit Public-Facing Application, T1059 - Command and Scripting Interpreter	https://wordpress.org/plugins/w3-total-cache/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-48703</u>		CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*	PCPJack
CWP Control Web Panel OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://control-webpanel.com/changelog

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-45321</u>		TanStack Router npm Packages	TeamPCP
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:tanstack:tanstack\ /arktype-adapter:*:*:*:*:*:*	Mini Shai-Hulud Worm
TanStack Router npm Packages Embedded Malicious Code Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1583 - Acquire Infrastructure, T1583.001 - Domains, T1587 - Develop Capabilities, T1587.001 - Malware	https://github.com/TanStack/router/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-0300</u>		Palo Alto Networks PAN-OS (PA-Series, VM-Series) Versions 10.2.x, 11.1.x, 11.2.x, 12.1.x	CL-STA-1132
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*	EarthWorm, ReverseSocks5
Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1090: Proxy, T1070: Indicator Removal	https://security.paloalto.com/CVE-2026-0300

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-20182</u>		Cisco Catalyst SD-WAN before 20.9.9.1, before 20.12.7.1, before 20.12.7.1, before 20.12.5.4, 20.12.6.2, 20.12.7.1, before 20.15.5.2, before 20.15.5.2, before 20.15.4.4, 20.15.5.2, before 20.18.2.2, before 20.18.2.2, before 26.1.1.1	UAT-8616
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190 - Exploit Public-Facing Application, T1059 - Command and Scripting Interpreter, T1098 - Account Manipulation, T1098.004 - SSH Authorized Keys, T1068 - Exploitation for Privilege Escalation, T1588 - Obtain Capabilities, T1588.006 - Vulnerabilities	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-sdwan-rpa2-v69WY2SW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42897</u>		Microsoft Exchange Server 2016 (all update levels), Microsoft Exchange Server 2019 (all update levels), Microsoft Exchange Server Subscription Edition (all update levels)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:2016:-:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:* :* cpe:2.3:a:microsoft:exchange_server:-:*:*:*:subscription:*:*:*	-
Microsoft Exchange Server Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.007: JavaScript	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-48172</u>		LiteSpeed User-End cPanel Plugin (versions 2.3 through 2.4.4, i.e. before 2.4.5)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:litespeedtech:user-end_cpanel_plugin:*:*:*:*:cpanel.*:*	-
LiteSpeed User-End cPanel Plugin Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-266	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.litespeedtech.com/products/litespeed-web-server/control-panel-support/release-log

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-9082</u>		Drupal core: from 8.9.0 before 10.4.10, from 10.5.0 before 10.5.10, from 10.6.0 before 10.6.9, from 11.0.0 before 11.1.10, from 11.2.0 before 11.2.12, from 11.3.0 before 11.3.10.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:drupal:drupal:*:*:*:*:*:*	-
Drupal Core SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1213: Data from Information Repositories, T1505.003 Server Software Component: Web Shell	https://www.drupal.org/sa-core-2026-004

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-5426</u>		Digital Knowledge KnowledgeDeliver (Before February 24, 2026)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Digital Knowledge KnowledgeDeliver Remote Code Execution Vulnerability		cpe:2.3:a:digital-knowledge:knowledgedeliver:*:*:*.*.*.*.*.*	BLUEBEAM (sks Godzilla), Cobalt Strike BEACON
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-321, CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003 Server Software Component: Web Shell, T1027: Obfuscated Files or Information	https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2026/MNDT-2026-0009.md

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-34926</u>		Trend Micro Apex One 2019 (On-Premise) - Server and Agent builds below 17079	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trendmicro:apex_one:*.~.*.*:on-premises:windows:*.*	-
Apex One Server Directory Traversal Vulnerability		cpe:2.3:a:trendmicro:apex_one:*.~.*.*:saas:windows:*.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1078: Valid Accounts, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://success.trendmicro.com/en-US/solution/KA-0023430

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>ValleyRAT</u>	ValleyRat is a sophisticated multi-stage Remote Access Trojan attributed to the China-based Silver Fox APT group, targeting Chinese-speaking users and now expanding globally. It uses staged shellcode loading, multiple UAC bypasses, and AV/Defender disabling to remain stealthy. Once installed, it grants attackers full remote control with keylogging, screen capture, and arbitrary plugin deployment.	Phishing	-
		IMPACT	AFFECTED PRODUCT
		Espionage, full system compromise	Windows
			PATCH LINK
TYPE			
Backdoor			
ASSOCIATED ACTOR			
Silver Fox			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>ABCDoor</u>	ABCDoor is a previously undocumented Python-based backdoor used by the Silver Fox group since at least December 2024, delivered as a custom ValleyRAT plugin. It communicates with C2 servers over HTTPS using a distinctive "abc" subdomain pattern. Capabilities include persistence, screenshot capture, remote mouse/keyboard control, file system operations, and clipboard exfiltration.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Remote control, data exfiltration	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
Silver Fox			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>RustSL</u>	RustSL is a modified Rust-based shellcode loader derived from a public GitHub project, weaponized by Silver Fox for stealthy payload delivery. It uses custom modules for steganography-based unpacking and country-based geofencing before executing payloads. Establishes "Phantom Persistence" and serves as the initial stage for dropping ValleyRAT while evading antivirus detection.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Stealthy payload delivery, AV bypass	Windows
Loader			PATCH LINK
ASSOCIATED ACTOR			
Silver Fox			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TCLBANKER</u>	TCLBANKER is a banking trojan delivered via trojanized Logitech Logi AI Prompt Builder MSI installers bundled inside ZIP files. It uses DLL side-loading to execute a malicious loader that deploys two .NET Reactor-protected modules: a banking trojan using WPF-based fraud overlays and WebSocket C2, and a worm module that self-propagates via WhatsApp session hijacking and Outlook COM-automated phishing emails.	Trojanized MSI Installer	-
		IMPACT	AFFECTED PLATFORM
TYPE		Malware self-propagation, Supply chain contamination, System compromise and resource hijacking	Windows
Banking Trojan			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Quasar Linux</u>	Quasar Linux (QLNX) is a sophisticated Linux malware targeting developer workstations and DevOps environments. It employs the memfd_create syscall to load itself into memory, re-execute from the in-memory image, and delete the original binary from disk to erase its on-disk footprint. The malware uses the MFD_RE environment variable to prevent re-execution loops and includes fallback mechanisms for systems lacking memfd_create support via /proc/self/fd.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Persistence establishment, Sandbox/monitoring bypass	npm, PyPI, GitHub, AWS, Docker, Kubernetes, Git, HashiCorp Vault, Terraform
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PCPJack	PCPJack is a modular credential theft framework that worms across exposed cloud infrastructure, harvesting credentials from cloud, container, developer, productivity, and financial services. The toolset actively evicts and replaces artifacts associated with the TeamPCP threat actor before establishing its own persistence and exfiltrating stolen data through attacker-controlled Telegram channels. Unlike typical cloud-focused malware, PCPJack does not deploy cryptominers, suggesting monetization through credential theft, fraud, spam, extortion, or resale of stolen access.	Dropper	CVE-2025-29927 CVE-2025-55182 CVE-2026-1357 CVE-2025-9501 CVE-2025-48703
TYPE		IMPACT	AFFECTED PRODUCT
Framework		Credential Loss, Infrastructure Compromise, Data Exfiltration	Docker, Kubernetes, Redis, MongoDB, RayML, Next.js, React, WordPress (WPVivid Backup, W3 Total Cache), CentOS Web Panel (CWP)
ASSOCIATED ACTOR			PATCH LINK
-			https://github.com/vercel/next.js/releases , https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r , https://wordpress.org/plugins/wpvivid-backuprestore/ , https://wordpress.org/plugins/w3-total-cache/ , http://centos-webpanel.com/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Mini Shai-Hulud</u>	Mini Shai-Hulud is a self-propagating supply chain worm that compromises npm and PyPI packages to steal credentials from developer machines and CI/CD runners. The malware uses stolen credentials to automatically publish additional malicious package versions, enabling worm-like propagation across the software supply chain. Payloads are heavily obfuscated and execute during package installation.	Exploiting Vulnerability	CVE-2026-45321
		IMPACT	AFFECTED PRODUCT
TYPE		Credential Theft, Destructive Capabilities	TanStack Router npm Packages
Worm			PATCH LINK
ASSOCIATED ACTOR			https://github.com/TanStack/router/releases
TeamPCP			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>EarthWorm</u>	EarthWorm is an open-source network tunneling utility frequently abused by adversaries for post-exploitation pivoting, including by APT groups like UAT-5918. It provides SOCKS5 proxy and port-forwarding features with forward, reverse, and multi-transfer modes across Windows, Linux, and macOS. Enables attackers to traverse segmented networks and reach internal assets shielded by firewalls.	Exploiting Vulnerability	CVE-2026-0300
		IMPACT	AFFECTED PRODUCT
TYPE		Covert tunneling, lateral movement	Palo Alto Networks PAN-OS
Tunneling tool			PATCH LINK
ASSOCIATED ACTOR			https://security.paloaltonetworks.com/CVE-2026-0300
CL-STA-1132			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ReverseSocks5	ReverseSocks5 is an open-source networking tool used to bypass firewalls or NAT by establishing an outbound connection from a target machine to a controller, rather than the other way around. Once the connection is established, it creates a SOCKS5 proxy tunnel that allows the controller to route traffic into the target's internal network. Used in the recent PAN-OS firewall zero-day campaign attributed to a suspected Chinese state actor, alongside Cavalry Werewolf operations.	Exploiting Vulnerability	CVE-2026-0300
		IMPACT	AFFECTED PRODUCT
TYPE		Firewall bypass, internal pivoting	Palo Alto Networks PAN-OS
Tunneling tool			PATCH LINK
ASSOCIATED ACTOR			https://security.paloaltonetworks.com/CVE-2026-0300
CL-STA-1132			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Deed RAT	Deed RAT is a modular backdoor uses multi-stage AES-CBC/RC4-encrypted payloads and LZNT1/Deflate compression. The malware patches Windows API to trigger execution during the host application's natural control flow, evading sandbox analysis. Plugins provide command execution, process injection, network communication, and persistence. Lateral movement occurs via RDP and Impacket SMB utilities. HTTPS C2 exfiltration via masqueraded security vendor domains.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
		IMPACT	AFFECTED PRODUCT
TYPE		Initial Access, Persistence, Credential & Data Theft	Windows
Modular Backdoor			PATCH LINKS
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082
FamousSparrow			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Terndoor</u>	Terndoor is a kernel-mode backed deployed as a redundant persistence mechanism. Delivered via Mofu shellcode loader using DLL sideloading, Terndoor stages a Windows kernel driver to achieve system-level persistence and evasion. The malware uses LZNT1 compression, RC4 encryption with hardcoded keys, and one-byte XOR string obfuscation. Payloads target msdt.exe for process injection and establish C2 via service creation.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
		IMPACT	AFFECTED PRODUCT
TYPE		Kernel & Driver Persistence, Evasion & Detection Bypass	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082
FamousSparrow			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mofu Loader</u>	Mofu Loader is a position-independent shellcode loader used to deliver kernel-mode and userland payloads. The loader uses NOP+CALL prologue for PIC execution, subtract-XOR-add (SXA) transformation for decryption, and LZNT1 compression. Payloads are prefixed with 12-byte headers containing seed and size values; MZ/PE headers are stripped to evade signature detection. Execution occurs entirely in memory with no disk footprint, making it ideal for covert payload staging in multi-stage intrusions.	Exploiting Vulnerabilities	CVE-2022-41040 CVE-2022-41082
		IMPACT	AFFECTED PRODUCT
TYPE		Fileless Execution, Lateral Movement, & Persistence	Windows
Loader			PATCH LINKS
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082
FamousSparrow			

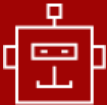
NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SHub Reaper</u>	SHub Reaper is a new macOS infostealer variant that spoofs Apple, Google, and Microsoft in a single attack chain. It shifts execution from Terminal to AppleScript in Script Editor to bypass macOS Tahoe 26.4 paste protections, then harvests browser credentials, Keychain, and crypto wallets while planting a persistent LaunchAgent backdoor.	Fake WeChat/Miro installer downloads	-
		IMPACT	AFFECTED PRODUCT
TYPE		Credential theft, crypto wallet compromise	macOS
Infostealer			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>StellarMonster</u>	StellarMonster is a trojanized fake "self-custody" crypto wallet (StellarMonSetup.exe) distributed by a Russian-speaking solo actor who scaled operations with jailbroken Gemini API keys. The installer covertly deploys GoToResolve for persistent remote access, while a fake "import wallet" screen harvests victims' seed phrases to drain wallets across multiple blockchains.	Fake crypto wallet download	-
		IMPACT	AFFECTED PRODUCT
TYPE		Remote access, crypto wallet drainage	Telegram, Truth Social, Windows, WordPress
RAT			PATCH LINK
ASSOCIATED ACTOR			
bandcampro			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>BLUEBEAM</u>	BLUEBEAM (aka Godzilla) is a .NET-based in-memory web shell deployed via the CVE-2026-5426 ASP.NET ViewState deserialization zero-day in KnowledgeDeliver LMS (Mandiant, May 2026). Running entirely inside the IIS w3wp.exe process with encrypted HTTP POST C2, it leaves no on-disk artifacts and was used to tamper with site JavaScript to stage Cobalt Strike BEACON.	Exploiting vulnerabilities	CVE-2026-5426
		IMPACT	AFFECTED PRODUCT
TYPE		Remote code execution, persistence	Digital Knowledge KnowledgeDeliver
Web shell			PATCH LINK
ASSOCIATED ACTOR			
-			https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2026/MNDT-2026-0009.md

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Silver Fox (aka Void Arachne)</u>	China	Industrial, Consulting, Retail, Transportation	India, Russia, Indonesia, South Africa, Cambodia, Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	ValleyRAT, ABCDoor, RustSL	Windows
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1566: Phishing, T1566.001: Spearphishing Attachment, T1566.002: Spearphishing Link, T1204: User Execution , T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1059.007: JavaScript, T1059.006: Python, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1053: Scheduled Task/Job , T1053.005: Scheduled Task, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1497: Virtualization/Sandbox Evasion , T1497.001: System Checks, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1036.008: Masquerade File Type, T1140: Deobfuscate/Decode Files or Information, T1622: Debugger Evasion, T1016: System Network Configuration Discovery, T1016.001: Internet Connection Discovery, T1082: System Information Discovery Collection, T1115: Clipboard Data, T1113: Screen Capture, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1105: Ingress Tool Transfer, T1571: Non-Standard Port Exfiltration , T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 CL-STA-1132	-	-	-
	MOTIVE		
	Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2026-0300	EarthWorm, ReverseSocks5	Palo Alto Networks PAN-OS
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1548: Abuse Elevation Control Mechanism , T1548.001: Setuid and Setgid Defense Evasion , T1070: Indicator Removal T1070.004: File Deletion, T1003: OS Credential Dumping Discovery , T1018: Remote System Discovery, T1090: Proxy, T1572: Protocol Tunneling , T1588: Obtain Capabilities , T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UAT-8616</u>	-	-	-
	MOTIVE		
	Information theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2026-20182	-	Cisco Catalyst SD-WAN Controller / Manager
TTPs			
TA0001: Initial Access, T1190: Exploit Public-Facing Application Execution, T1059: Command and Scripting Interpreter , TA0002: Persistence, T1098: Account Manipulation, T1098.004: SSH Authorized Keys, TA0004: Privilege Escalation, T1068: Exploitation for Privilege Escalation, TA0042: Resource Development, T1588: Obtain Capabilities, T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>FamousSparrow</u> (aka <u>UNC2286</u>, <u>GhostEmperor</u>, <u>RedMike</u>, <u>Operator Panda</u>, <u>Earth Estries</u>, <u>Salt Typhoon</u>)	China	Oil and Gas, Energy	Armenia, Azerbaijan, Georgia
	MOTIVE		
	Information Theft, Espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	TARGETED CVE		
	CVE-2022-41040 CVE-2022-41082	Malware: Deed RAT (aka Snappybee), Terndoor, Mofu loader	Microsoft Exchange Server
TTPs			
TA0001: Initial Access, T1190: Exploit Public-Facing Application, TA0003: Persistence, T1505: Server Software Component, T1543: Create or Modify System Process, T1547: Boot or Logon Autostart Execution, T1505.003: Web Shell, T1543.003: Windows Service, T1547.001: Registry Run Keys / Startup Folder, TA0002: Execution, T1569: System Services, T1059: Command and Scripting Interpreter, T1569.002: Service Execution, T1059.001: PowerShell, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1140: Deobfuscate/Decode Files or Information, T1562: Impair Defenses, T1027: Obfuscated Files or Information, T1055: Process Injection, T1014: Rootkit, T1036: Masquerading, T1574.002: DLL Side-Loading, T1036.005: Match Legitimate Resource Name or Location, TA0006: Credential Access, T1078: Valid Accounts, T1078.002: Domain Accounts, TA0007: Discovery, T1016: System Network Configuration Discovery, TA0008: Lateral Movement, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, TA0024: Resource Development, T1583: Acquire Infrastructure, T1583.001: Domains, TA0011: Command and Control, T1071: Application Layer Protocol, T1573: Encrypted Channel, T1071.001: Web Protocols, T1573.002: Asymmetric Cryptography			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-2949	-	Worldwide	All
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0007: Discovery; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1566: Phishing; T1566.003: Spearphishing via Service; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1098: Account Manipulation; T1098.005: Device Registration; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1070: Indicator Removal; T1070.001: Clear Windows Event Logs; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1530: Data from Cloud Storage; T1087: Account Discovery; T1087.004: Cloud Account; T1580: Cloud Infrastructure Discovery; T1528: Steal Application Access Token; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1021: Remote Services; T1021.007: Cloud Services Dashboard; T1219: Remote Access Software; T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>TeamPCP (aka PCPcat, ShellForce, DeadCatx3, CipherForce, Persy PCP, UNC6780)</u>	-	Software Development, AI/ML, Cloud Computing, CI/CD Pipelines, Data Analytics/Visualization, Enterprise Automation, Source Code Hosting Platforms	Worldwide
	MOTIVE		
	Espionage, Sabotage, Disruption, Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2026-45321	Mini Shai-Hulud Worm	TanStack Router npm Packages
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1078: Valid Accounts; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1106: Native API; T1176: Browser Extensions; T1543: Create or Modify System Process; T1543.001: Launch Agent; T1543.002: Systemd Service; T1546: Event Triggered Execution; T1027: Obfuscated Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1070: Indicator Removal; T1070.006: Timestomp; T1656: Impersonation; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.004: Private Keys; T1555: Credentials from Password Stores; T1555: Credentials from Password Stores; T1555.005: Password Managers; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1526: Cloud Service Discovery; T1083: File and Directory Discovery; T1005: Data from Local System; T1213: Data from Information Repositories; T1213.003: Code Repositories; T1072: Software Deployment Tools; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1132: Data Encoding; T1567: Exfiltration Over Web Service; T1567.001: Exfiltration to Code Repository; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1485: Data Destruction; T1204: User Execution; T1204.002: Malicious File; T1059.006: Python; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.005: Cloud Instance Metadata API			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Fox Tempest	-	Healthcare, Education, Government, Financial Services	United States, France, India, China
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	AnyDesk, Microsoft Teams, PuTTY, Webex (impersonated as lures)
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0006: Credential Access; TA0011: Command and Control; TA0040: Impact; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1583.008: Malvertising; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.003: Cloud Accounts; T1586: Compromise Accounts; T1587: Develop Capabilities; T1587.002: Code Signing Certificates; T1608: Stage Capabilities; T1608.006: SEO Poisoning; T1189: Drive-by Compromise; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1136: Create Account; T1136.001: Local Account; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 bandcamppro	Russia	Cryptocurrency Holders, Small and Medium Businesses (Weapons Retailers, Legal Offices, Medical Practices, Commercial Sites), Financial Services (Impersonated)	North America
	MOTIVE		
	Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	StellarMonster	Telegram, Truth Social, Windows, WordPress
TTPs			
TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.003: Virtual Private Server, T1583.004: Server, T1585: Establish Accounts, T1585.001: Social Media Accounts, T1585.002: Email Accounts, T1588: Obtain Capabilities, T1588.001: Malware, T1588.002: Tool, T1586: Compromise Accounts, TA0001: Initial Access, T1566: Phishing, TA0002: Execution, T1204: User Execution, T1204.002: Malicious File, TA0005: Defense Evasion, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1656: Impersonation, TA0006: Credential Access, T1110: Brute Force, T1110.001: Password Guessing, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1555: Credentials from Password Stores, TA0007: Discovery, T1592: Gather Victim Host Information, TA0009: Collection, T1115: Clipboard Data, T1005: Data from Local System, TA0011: Command and Control, T1219: Remote Access Software, T1090: Proxy, T1071: Application Layer Protocol, TA0040: Impact, T1657: Financial Theft			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
		T1195.002: Compromise Software Supply Chain
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.006: Python
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	

Tactic	Technique	Sub-technique
TA0002: Execution	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
	T1610: Deploy Container	
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
		T1098.005: Device Registration
	T1136: Create Account	T1136.001: Local Account
		T1136.003: Cloud Account
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder

Tactic	Technique	Sub-technique
TA0003: Persistence	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
		T1098.005: Device Registration
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
	T1611: Escape to Host	
TA0005: Defense Evasion	T1014: Rootkit	

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.003: Rename System Utilities
		T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.002: Clear Linux or Mac System Logs
		T1070.004: File Deletion
		T1070.006: Timestamp
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1140: Deobfuscate/Decode Files or Information	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
	T1222: File and Directory Permissions Modification	T1222.001: Windows File and Directory Permissions Modification
		T1222.002: Linux and Mac File and Directory Permissions Modification
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass

Tactic	Technique		Sub-technique
TA0005: Defense Evasion	T1553: Subvert Trust Controls		T1553.002: Code Signing
			T1553.006: Code Signing Policy Modification
	T1556: Modify Authentication Process		T1556.003: Pluggable Authentication Modules
	T1562: Impair Defenses		T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts		T1564.002: Hidden Users
	T1574: Hijack Execution Flow		T1574.002: DLL Side-Loading
			T1574.006: Dynamic Linker Hijacking
	T1610: Deploy Container		
	T1620: Reflective Code Loading		
	T1622: Debugger Evasion		
T1656: Impersonation			
TA0006: Credential Access	T1003: OS Credential Dumping		
	T1056: Input Capture		T1056.001: Keylogging
			T1056.002: GUI Input Capture
			T1056.003: Web Portal Capture
	T1110: Brute Force		T1110.001: Password Guessing
	T1528: Steal Application Access Token		
	T1539: Steal Web Session Cookie		
	T1552: Unsecured Credentials		T1552.001: Credentials In Files
			T1552.004: Private Keys
			T1552.005: Cloud Instance Metadata API

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1552: Unsecured Credentials	T1552.007: Container API
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
TA0007: Discovery	T1010: Application Window Discovery	
	T1016: System Network Configuration Discovery	T1016.001: Internet Connection Discovery
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1526: Cloud Service Discovery	
	T1580: Cloud Infrastructure Discovery	
	T1613: Container and Resource Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery

Tactic	Technique	Sub-technique
TA0007: Discovery	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
	T1072: Software Deployment Tools	
	T1210: Exploitation of Remote Services	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.001: Local Email Collection
		T1114.002: Remote Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1213: Data from Information Repositories	T1213.003: Code Repositories
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository
TA0011: Command and Control	T1001: Data Obfuscation	

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.003: Mail Protocols
	T1090: Proxy	T1090.001: Internal Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
	T1529: System Shutdown/Reboot	
	T1565: Data Manipulation	T1565.001: Stored Data Manipulation
		T1565.003: Runtime Data Manipulation
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains

Tactic	Technique	Sub-technique
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
		T1583.004: Server
		T1583.006: Web Services
		T1583.008 : Malvertising
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1585: Establish Accounts	
	T1586: Compromise Accounts	T1586.001: Social Media Accounts
		T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.003: Code Signing Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.006: SEO Poisoning
TA0043: Reconnaissance	T1592: Gather Victim Host Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment

Top 5 Takeaways

#1

In May 2026, **10 zero-day vulnerabilities** surfaced, led by the “**Ten Celebrity Vulnerabilities**,” including **Copy Fail**, **Dirty Frag**, **React2Shell**, **ProxyNotShell**, **NGINX Rift**, **Fragnesia**, **DirtyDecrypt**, and **Dead.Letter**. These zero-days were found across products from Palo Alto, Ivanti, CWP, Cisco, Microsoft, LiteSpeed, Digital Knowledge, and Trend Micro.

#2

Newly identified malware active in **May** included a broad mix of **Backdoors**, **RATs**, and **Loaders**. Key discoveries were **ValleyRAT**, **ABCDoor**, **Terndoor**, **RustSL**, **Mofu Loader**, **Quasar Linux**, and **StellarMonster**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

#3

Cyberattacks concentrated heavily on **India**, **the United States**, **the United Kingdom**, **Grenada**, and **Saint Lucia**, which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4

Cryptocurrency, **Financial**, **Technology**, **Government**, and **Healthcare** sectors absorbed the bulk of targeted activity, with ransomware operations, data theft, and espionage campaigns driving operational disruption. Attackers continued refining techniques and expanding pressure across these industries.

#5

Activity during the period was dominated by **CL-STA-1132**, **TeamPCP**, **FamousSparrow**, **Storm-2949**, and **Fox Tempest**, all well-resourced groups known for sustained, high-impact operations. Their campaigns shaped a threat landscape defined by disciplined tradecraft, rapid exploitation cycles, and a clear focus on high-value targets across public and private sectors.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **25 significant vulnerabilities** and block the indicators related to the **8 active threat actors**, **15 active malware**, and **202 potential MITRE TTPs**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **25 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors**, **active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

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 malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Social engineering: is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

Supply chain attack: Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

Eavesdropping: Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities

CVE - Common Vulnerabilities and Exposures

CPE - Common Platform Enumeration

CWE - Common Weakness Enumeration

✕ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>ValleyRAT</u>	IPv4	108[.]187[.]37[.]85, 108[.]187[.]42[.]63, 207[.]56[.]138[.]28
	MD5	4A5195A38A458CDD2C1B5AB13AF3B393, E66BAE6E8621DB2A835FA6721C3E5BBE
<u>ABCDDoor</u>	IPv4:Port	45[.]118[.]133[.]203[:]:5000
	Domains	abc[.]fetish-friends[.]com, abc[.]3mkorealtd[.]com, abc[.]sudsmama[.]com, abc[.]woopami[.]com, abc[.]ilptour[.]com, abc[.]petitechanson[.]com, abc[.]doublemobile[.]com
	MD5	04194F8DDD0518FD8005F0E87AE96335, F15A67899CFE4DECF76D4CD1677C254, 11705121F64FA36F1E9D7E59867B0724, 13669B8F2BD0AF53A3FE9AC0490499E5, 5B998A5BC5AD1C550564294034D4A62C, C50C980D3F4B7ED970F083B0D37A6A6A, DE8F0008B15F2404F721F76FAC34456A, 9BF9F635019494C4B70FB0A7C0FB53E4, A543B96B0938DE798DD4F683DD92A94A, FA08B243F12E31940B8B4B82D3498804
<u>RustSL</u>	MD5	039E93B98EF5E329F8666A424237AE73, B6DF7C59756AB655CA752B8A1B20CFFA, 5390E8BF7131CAAAA98A5DD63E27B2BC, 44299A368000AE1EE9E9E584377B8757

Attack Name	TYPE	VALUE
<u>RustSL</u>	MD5	E5E8EF65B4D265BD5FB77FE165131C2F, 3279307508F3E5FB3A2420DEC645F583, 1020497BEF56F4181AEFB7A0A9873FB4, B23D302B7F23453C98C11CA7B2E4616E, A234850DFDFD7EE128F648F9750DD2C4, 4FC5EC1DE89CE3FCDD3E70DB4A9C39D1, A0D1223CA4327AA5F7674BDA8779323F, 70AE9CA2A285DA9005A8ACB32DD31ACE, DD0114FFACC6610B5A4A1CB0E79624CC, 891DE2FF486A1824F2DB01C1BDF1D2E9, B0E06925DB5416DFC90BABF46402CD6F, AD39A5790B79178D02AC739099B8E1F4, D1D78CD1436991ADB9C005CC7C6B5B98, 2C5A1DD4CB53287FE0ED14E0B7B7B1B7, E6362A81991323E198A463A8CE255533, CB3D86E3EC2736EE1C883706FCA172F8, A083C546DC66B0F2A5E0E2E68032F62C, 70016DDBCB8543BDB06E0F8C509EE980, 8FC911CA37F9F451A213B967F016F1F8, 202A5BCB87C34993318CFA3FA0C7ECB0, 06130DC648621E93ACB9EFB9FABB9651, F7037CC9A5659D5A1F68E88582242375, 8AC5BEE89436B29F9817E434507FEF55, 5ED84B2099E220D645934E1FD552AE3A, 27A3C439308F5C4956D77E23E1AAD1A9, 53B68CA8D7A54C15700CF9500AE4A4E2, 1D1F71936DB05F67765F442FEB95F3FD, 3C6AEC25EBB2D51E1F16C2EEF181C82A, 7F27818E4244310A645984CCC41EA818, A75713F0310E74FFD24D91E5731C4D31, 4FC8C78516A8C2130286429686E200ED, 3417B9CF7ACB22FAE9E24603D4DE1194, 933F1CB8ED2CED5D0DD2877C5EA374E8, B5CA812843570DCF8E7F35CACAB36D4A
<u>EarthWorm</u>	URL	hxxp[:]//146[.]70[.]100[.]69[:.]8000/php_sess
	SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dc d84f97a584

Attack Name	TYPE	VALUE
<u>ReverseSocks5</u>	URL	hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz
<u>TCLBANKER</u>	SHA256	701d51b7be8b034c860bf97847bd59a87dca8481c4625328813746964995b626, 8a174aa70a4396547045aef6c69eb0259bae1706880f4375af71085eeb537059, 668f932433a24bbae89d60b24eee4a24808fc741f62c5a3043bb7c9152342f40
	Domains	campanha1-api[.]ef971a42[.]workers[.]dev, mxtestacionamentos[.]com
<u>Quasar Linux</u>	MD5	70f70743f287a837d17c56933152a8a6
	SHA1	b0f2c668cbdd63a871c90592b6c93e931115872e
	SHA256	ea1d34b21b739a6bbf89b3f7e67978005cf7f3eda612cefc7eac1c8ead7c5545
<u>PCPJack</u>	Domain	cdn[.]cloudfront-js[.]com
	SHA256	b1d8149e5c7b6312f40c220e89b1913762f9aa416ff491540b3b7b7040260eb5
<u>Mini Shai-Hulud</u>	SHA256	ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c, e7347d90653efc565f03733a95e9209d78f9cfa81e31ff2b2dd9d48d75a4b8b1
<u>Deed RAT</u>	SHA256	25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b
<u>Terndoor</u>	SHA256	711d9427ee43bc2186b9124f31cba2db5f54ec9a0d56dc2948e1a4377bada289
<u>SHub Reaper</u>	Filepath	~/Library/Application Support/Google/GoogleUpdate.app/Contents/MacOS/GoogleUpdate, ~/Library/LaunchAgents/com.google.keystone.agent.plist, /tmp/shub_log.zip, /tmp/shub_split.sh, /tmp/shub_mzip_*.zip, /tmp/.c.sh, /tmp/*_asar.zip

Attack Name	TYPE	VALUE
<u>StellarMonster</u>	SHA256	981036cec38c6fd9796fc64a102100b97983f56b3482cc3e1f1610e14a1fae58
<u>BLUEBEAM</u>	SHA256	7c1f99dca8e5a7897892f9d224a6495023a2cfd2671697d229d355978c415ed2

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 Demo of HivePro.

REPORT GENERATED ON

June 01, 2026 • 11:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com