

Date of Publication
October 1, 2026



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

SEPTEMBER 2026

Table Of Contents

[Summary](#)..... 03

[Insights](#)..... 04

[Threat Distribution](#)..... 05

[Celebrity Vulnerabilities](#)..... 06

[Vulnerabilities Summary](#)..... 09

[Attacks Summary](#)..... 15

[Adversaries Summary](#)..... 18

[Targeted Products](#)..... 21

[Targeted Countries](#)..... 26

[Targeted Industries](#)..... 27

[Top MITRE ATT&CK TTPs](#)..... 28

[Top Indicators of Compromise \(IOCs\)](#)..... 29

[Vulnerabilities Exploited](#)..... 32

[Attacks Executed](#)..... 65

[Adversaries in Action](#)..... 93

[MITRE ATT&CK TTPs](#)..... 107

[Top 5 Takeaways](#)..... 117

[Recommendations](#)..... 118

[Appendix](#)..... 119

[Indicators of Compromise \(IoCs\)](#)..... 120

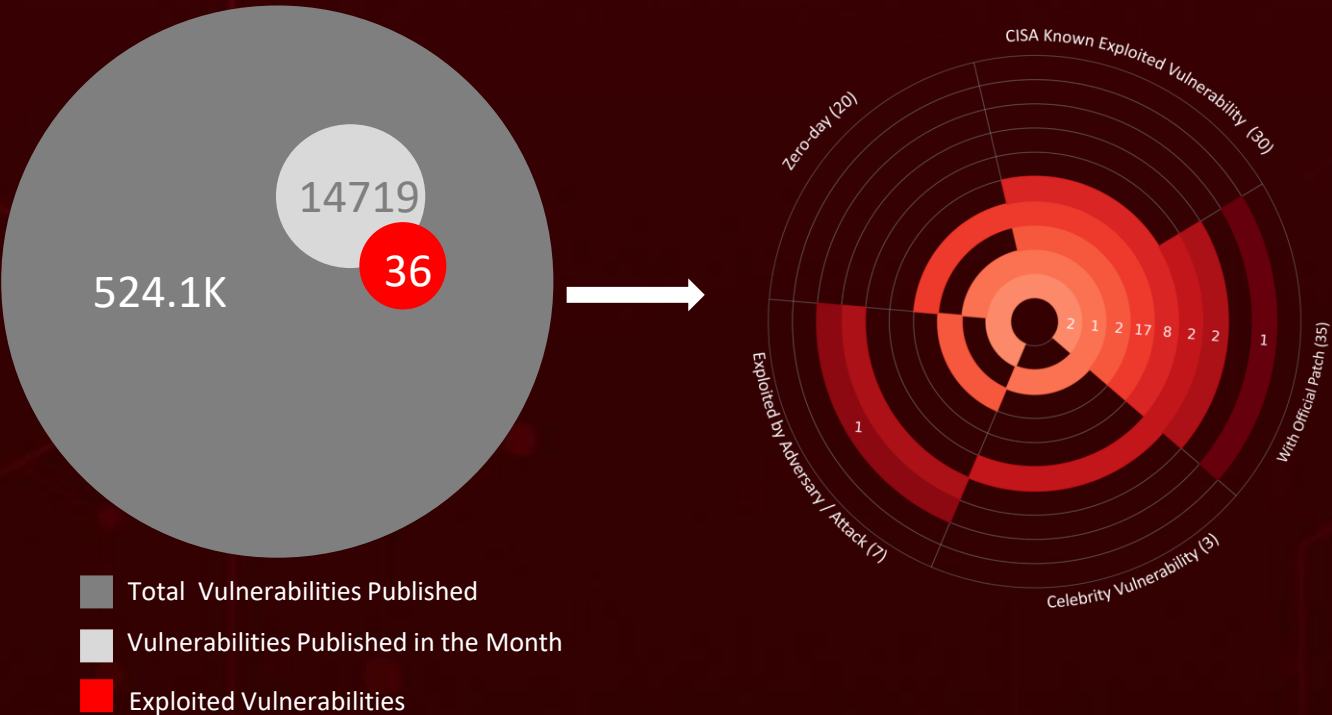
[What Next?](#)..... 126

Summary

September reshaped the cybersecurity landscape, with **20** zero-day vulnerabilities actively exploited. One of the most notable threats came from **ShinyHunters** (UNC6240), which renewed its mass exploitation of a critical Oracle PeopleSoft PeopleTools flaw, **CVE-2026-35273**. The attackers bypass WAF rules by URL-encoding a single character in the PSEMHUB path, letting them reach systems that were never patched. Once inside, they deploy web shells, the **SIDEEYE** backdoor, Neo-reGeorg tunnels, and MeshAgent. Victims span higher education, healthcare, government, and other sectors worldwide, and the goal is data theft and extortion. Organizations should patch immediately and should not rely on WAF rules alone.

Additionally, Google also patched **CVE-2026-87491**, an out-of-bounds write flaw in the V8 JavaScript and WebAssembly engine used by Chrome and other Chromium-based browsers. The fix reached the Chromium source tree weeks before the stable Chrome release, which gave attackers a patch-gap window to weaponize the flaw. The attacks are tied to a shared exploit kit called **BlueMoon**, which chains this flaw with a second V8 flaw (CVE-2026-85046) and a Windows kernel privilege escalation flaw (CVE-2026-85880) to compromise a computer with a single click. BlueMoon was first seen on August 28, 2026, and was used by multiple China-aligned actors. The attacks have delivered the **GRIMWEDGE** JScript backdoor, the **SUPERSTOMP** loader, the **ShadowPad** backdoor, and Rust-based loaders.

Moreover, **NeedyMantis** is a modular backdoor used by the China-based actor **Storm-3069** to keep long-term access to networks it has already breached. Its targets include telecommunications, education, healthcare, nonprofit, and government organizations. It is delivered through DLL sideloading inside bundles of legitimate software such as Poedit, curl, Vim, and TightVNC. With risks like these growing, strong defensive measures are more important than ever.



In September 2026, a geopolitical cybersecurity landscape unfolds, revealing **Germany, Mexico, United Arab Emirates, South Africa, and Canada** as the top-targeted countries

Highlighted in **September 2026** is a cyber battleground encompassing the **Government, Finance, Education, Technology, and Retail** sectors, designating them as the top industries

ShinyHunters is running a renewed mass campaign, so attackers are scanning for unpatched **PeopleTools** systems right now

NetScaler handles VPN, remote access, load balancing, and authentication, so **CVE-2026-88771** or **CVE-2026-88772** hands an attacker the keys to the perimeter

PAYLOAD

Ransomware skipped the encryptor entirely in one intrusion, so a ransomware defense built only to catch encryption would have seen nothing.

CVE-2026-87491 is the seventh **Chrome** zero-day of 2026 exploited in the wild, so **Chrome** emergency updates are becoming routine.

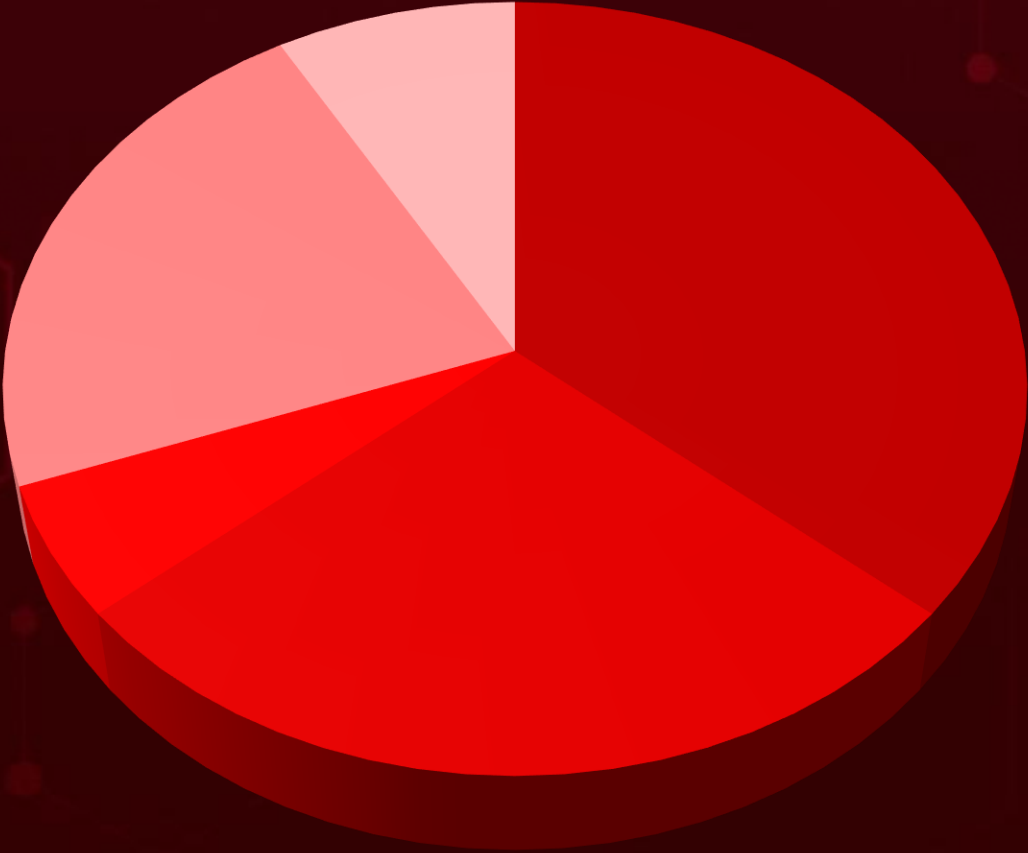
StyleSmuggler (CVE-2026-75650) scores a perfect CVSS 10.0, so this is about as bad as a vulnerability gets.

Mirage Kitten is using fake recruiters to deliver **NodeRabbit** and **PollCat**, so the job offer in your inbox may be the attack.

NeedyMantis is how **Storm-3069** signs a long-term lease, so the real risk is how long it stays, not how it got in.

CVE-2026-86950 lives in **CoreGraphics**, the part of Apple's software that draws images and documents, so almost everything on an iPhone, iPad, or Mac touches it.

Threat Distribution



- Malware Attacks
- Social Engineering
- Denial-of-Service Attack
- Injection Attacks
- Password Attack



Celebrity Vulnerabilities

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

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

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-72529	TrueConf Server Missing Authentication for Critical Function Vulnerability	TrueConf server			
CVE-2026-72530	TrueConf Server Code Injection Vulnerability	TrueConf server			
CVE-2026-82078	PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability	PaperCut NG and PaperCut MF			
CVE-2026-81578	PaperCut NG and PaperCut MF Authentication Bypass Vulnerability	PaperCut NG and PaperCut MF			
CVE-2026-83548	SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability	SonicWall SMA 1000			
CVE-2026-83549	SonicWall SMA1000 Appliances OS Command Injection Vulnerability	SonicWall SMA 1000			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-32475	WordPress Elementor Pro Unauthenticated Arbitrary File Upload Vulnerability	WordPress Elementor Pro			
CVE-2026-85046	Google Chrome V8 Type Confusion Vulnerability	Google Chrome			
CVE-2026-75650	Adobe Commerce and Magento Open Source Remote Code Execution Vulnerability	Adobe Commerce and Magento			
CVE-2026-6471	PostgreSQL Output Plugin Missing Authorization Vulnerability	PostgreSQL			
CVE-2026-85880	Microsoft Windows Heap-Based Buffer Overflow Vulnerability	Microsoft Windows			
CVE-2026-81963	Microsoft Windows Link Following Vulnerability	Microsoft Windows			
CVE-2026-69414	Microsoft Defender Elevation of Privilege Vulnerability	Microsoft Malware Protection Engine			
CVE-2026-86218	N-able N-central Static Code Injection Vulnerability	N-able N-central			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-87491	Google Chromium V8 Out of Bounds Write Vulnerability	Google Chrome			
CVE-2026-85706	GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability	GitLab CE/EE			
CVE-2026-76461	Cisco Secure Email Gateway SQL Injection Vulnerability	Cisco Secure Email Gateway (AsyncOS)			
CVE-2026-87886	Acronis Backup Incorrect Default Permissions Vulnerability	Acronis Backup			
CVE-2026-84869	ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability	ConnectWise ScreenConnect			
CVE-2026-76460	Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability	Cisco ISE & ISE-PIC			
CVE-2026-42016	JFrog Artifactory Incorrect Authorization Vulnerability	JFrog Artifactory			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-42018	JFrog Artifactory Improper Authentication Vulnerability	JFrog Artifactory			
CVE-2026-82329	JFrog Artifactory Improper Authentication Vulnerability	JFrog Artifactory			
CVE-2026-7273	Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability	Zyxel GS1900 Series Switches			
CVE-2026-93616	Check Point Multiple Products Path Traversal Vulnerability	Check Point Security Management, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent			
CVE-2026-85102	Check Point Multiple Products Improper Certificate Validation Vulnerability	Check Point Security Gateway, Spark Firewall Centrally Managed, Spark Firewall Locally Managed			
CVE-2026-94127	F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability	F5 BIG-IP APM			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-93952	Arista VeloCloud Orchestrator Improper Input Validation Vulnerability	Arista VeloCloud Orchestrator (VCO)			
CVE-2026-87902	WordPress Unauthenticated Path Traversal Vulnerability	WordPress			
CVE-2023-52271	Topaz Antifraud Improper Access Control Vulnerability	Topaz Antifraud			
CVE-2025-61155	Hotta Studio GameDriverX64 Improper Access Control Vulnerability	Tower of Fantasy (Gamedriverx64.sys driver)			
CVE-2025-1055	K7 Computing K7 Security Anti-Malware Missing Authorization Vulnerability	K7 Security (K7RKScan.sys driver)			
CVE-2026-88771	Citrix NetScaler Improper Input Validation Vulnerability	Citrix NetScaler ADC & NetScaler Gateway			
CVE-2026-88772	Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	Citrix NetScaler ADC & NetScaler Gateway			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-86950	Apple Multiple Products Out-of-Bounds Write Vulnerability	Apple iOS and iPadOS, Apple macOS Tahoe, Apple macOS Sequoia			
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	Oracle PeopleSoft Enterprise PeopleTools			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
NodeRabbit	RAT	-	Windows, Linux, macOS	-	Trojanized coding-challenge archives
PollCat	RAT	-	Windows, Linux, macOS	-	Trojanized React coding challenge
Retrograde/MiniFast	Backdoor	-	Windows	-	-
COBALTSPIN	Network tunneler	-	-	-	-
REALBREEZE	Brute-forcing utility	-	-	-	Downloaded from GitHub repositories
MILDFROST	Backdoor	-	-	-	-
BOATBEAM	Backdoor	-	-	-	-
LIGHTPAINT	Backdoor	-	-	-	-
KICKPLATE	Backdoor	-	-	-	-
XWORM	RAT	-	-	-	Phishing
JSceal	Stealer	-	Windows, macOS	-	Malicious Facebook and Google ads
PEEP	Toolkit	-	-	-	-
GRIMWEDGE	Backdoor	CVE-2026-87491	Google Chrome		Phishing
SUPERSTOMP	Loader	CVE-2026-87491	Google Chrome		Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LONGTALE	Browser Extension	CVE-2026-87491	Google Chrome		Phishing
ShadowPad	Backdoor	CVE-2026-87491	Google Chrome		Phishing
Panzer	Ransomware	-	Windows, Linux, ESXi, FreeBSD	-	-
AppleSeed (KGH_SPY)	Backdoor	-	Windows	-	Spear-phishing emails
HappyDoor	Backdoor	-	Windows	-	Spear-phishing emails
HelloDoor	Backdoor	-	Windows	-	Spear-phishing emails
httpMalice	Backdoor	-	Windows	-	Spear-phishing emails
httpTroy	Backdoor	-	Windows	-	Spear-phishing
MemLoad	Loader	-	Windows	-	Spear-phishing attachment
HTTPSpy	RAT	-	Windows	-	Spear-phishing attachments
AsyncRAT	RAT	-	Windows	-	Spear-phishing
StormousX	Ransomware	-	-	-	phishing
XMRig	Cryptominer	CVE-2026-84869	ConnectWise ScreenConnect		social engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PAYLOAD Ransomware	Ransomware	-	Microsoft Active Directory (Group Policy), Fortinet FortiGate SSL VPN, VMware ESXi	-	Malicious GPO
DragonForce Ransomware	Ransomware	CVE-2023-52271, CVE-2025-61155, CVE-2025-1055	Microsoft Windows		DLL sideloading, BYOVD
SIDEEYE	Multi-stage backdoor	CVE-2026-35273	Oracle PeopleSoft PeopleTools		Trojanized Ple64.exe installer
NeedyMantis	Modular	-	Windows	-	DLL sideloading

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Mirage Kitten	Information theft and espionage	Iran	-	NodeRabbit, PollCat, Retrograde/MiniFast	Windows
BREEZE COMET	Financial Gain	Brazil	-	COBALTSPIN, REALBREEZE, MILDFOST, BOATBEAM, LIGHTPAINT, KICKPLATE, XWORM	Windows, Linux, Active Directory, Cloud environments, Kubernetes, CI/CD pipelines, Java Virtual Machine (JVM) process space.
TA412	Information theft and espionage	China	CVE-2026-87491	SUPERSTOMP, LONGTALE (aka GemStone)	Google Chrome
UTA0560	Information theft and espionage	China	CVE-2026-87491	GRIMWEDGE	Google Chrome
UNK_LateNight	Information theft and espionage	China	CVE-2026-87491	ShadowPad	Google Chrome
UNK_DoubleCheck	Information theft and espionage	-	CVE-2026-87491	-	Google Chrome

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNK_QuietRacket	Information theft and espionage	China	CVE-2026-87491	-	Google Chrome
Kimsuky	Espionage, Financial Gains	North Korea	CVE-2017-11882 CVE-2018-0802 CVE-2019-0708 CVE-2019-1405 CVE-2020-0787 CVE-2024-1709 CVE-2025-48703	AppleSeed (KGH_SPY), AlphaSeed, HappyDoor, PebbleDash, HelloDoor, httpMalice, httpTroy, MemLoad, HTTPSpy, AsyncRAT, BabyShark, GoldDragon, KLogEXE, Troll Stealer, Gomir, NavRAT, NikiHTTP, NikiTeaR, ComeBacker, DRATzarus, FastFire, FastSpy, FlowerPower, RandomQuery, Yorekey, Grease, TRANSLATEX, QuasarRAT, Gh0st RAT, KimJongRAT, CSPY Downloader, BITTERSWEET, VENOMBITE, xRAT, MailFetch.py, Reger Dropper, Pidoc Dropper	GitHub, Pastebin, Dropbox, Slack, Cloudflare Quick Tunnels, Visual Studio, Microsoft 365, Okta

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Stormous	Financial gain	-	-	Stormous X	-
Meowciety403	Financial Gains, Information Theft	-	-	-	-
ShinyHunters	Financial gain	-	CVE-2026-35273	SIDEEYE	Oracle PeopleSoft
Storm-3069	Information Theft, Espionage	China	-	NeedyMantis	-



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Server	TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier
	application software	All versions of PaperCut NG and PaperCut MF
	Network Security Appliance	SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform-hotfix) and older versions
	Plugin	WordPress Elementor Pro (Before 4.2.2)
	Content Management System (CMS)	WordPress WordPress Core (4.7.0 – 7.1.1)
	Browser	Google Chrome (Before 152.0.7977.82 Linux; Before 152.0.7977.82/.83 Windows, macOS)
	Browser	Google Chrome versions before 153.0.8010.36 on Windows, macOS, and Linux
	e-commerce platform software	Adobe Commerce and Magento Open Source 2.4.4 - 2.4.9 (2026-aug and earlier), Adobe Commerce on Cloud, Adobe Commerce B2B 1.3.3 - 1.5.3
	Relational Database Management System	PostgreSQL core server before 18.6, 17.11, 16.15, 15.19, and 14.24

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	Windows 10 Version 1809; Windows Server 2019, 2022, 2016, 2012; Windows 10 Version 21H2, Windows 11 Version 23H2, 24H2, 25H2; Windows Server 2025
	antimalware scanning engine	Microsoft Malware Protection Engine
	Remote Monitoring and Management (RMM) platform	N-able N-central (Before 2026.3.1.14)
	DevOps / DevSecOps platform	GitLab CE/EE self-managed (18.7 before 19.1.8; 19.2 before 19.2.6; 19.3 before 19.3.2)
	Email Security Gateway	Cisco Secure Email Gateway (AsyncOS): 15.5 and earlier (before 15.5.5-014), 16.0 (before 16.0.4-302), 16.5 (before 16.5.0-780)
	Network Access Control (NAC) / Identity and Access Management Appliance	Cisco ISE & ISE-PIC (Releases 3.0 through 3.5, before the first fixed release)
	Backup and Recovery Software	Acronis Backup plugin for cPanel & WHM (Before 1.9.3.1021); Acronis Backup extension for Plesk (Before 1.8.11.638)
	Remote Support Software	ConnectWise ScreenConnect client version before 26.6.5
	Repository Manager	JFrog Artifactory Self-Hosted Before 7.133.11
	Repository Manager	JFrog Artifactory Self-Hosted Before: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.8

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Repository Manager	JFrog Artifactory Self-Hosted 7.111.4 to: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.37; 7.161.0 to 7.161.19
	Network Infrastructure	Zyxel GS1900-8 (Before 2.90(AAHH.2)C0), GS1900-8HP (Before 2.90(AAHI.2)C0), GS1900-10HP (Before 2.90(AAZI.2)C0), GS1900-16 (Before 2.90(AAHJ.2)C0), GS1900-24 (Before 2.90(AAHL.2)C0), GS1900-24E (Before 2.90(AAHK.2)C0), GS1900-24EP (Before 2.90(ABTO.2)C0), GS1900-24HPv2 (Before 2.90(ABTP.2)C0), GS1900-48 (Before 2.90(AAHN.2)C0), GS1900-48HPv2 (Before 2.90(ABTQ.2)C0)
	Network Security Management Platform	Check Point Security Management, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent (R82.20; R82.10 with Jumbo Hotfix Take 44 or lower; R82 with Take 126 or lower; R81.20 with Take 166 or lower; R81.10 with Take 190 or lower, EoS; R80, R80.10, R80.20, R80.30, R80.40, R81, all EoS)
	Network Security Management Platform	Check Point Security Gateway, Spark Firewall Centrally Managed, Spark Firewall Locally Managed (R81, EoS; R81.10, EoS; R81.10.x; R81.20; R82; R82.00.x; R82.10)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Access Management / Remote Access and Zero Trust Gateway	F5 BIG-IP APM (17.1.0 - 17.1.3, 17.5.0 - 17.5.1, 21.1.0)
	Orchestration Platform	Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.16, 6.1.x through 6.1.3.7, 6.4.x before 6.4.2.8, 7.0.x through 7.0.0.2)
	Endpoint Security Software	Topaz Antifraud (wsftprm.sys driver)
	Gaming Software	Tower of Fantasy (Gamedriverx64.sys driver)
	Endpoint Security Software	K7 Security (K7RKScan.sys driver)
	Secure Remote Access Gateway	Citrix NetScaler ADC & NetScaler Gateway (14.1 before 14.1-73.37; 13.1 before 13.1-64.23; 14.1-FIPS before 14.1-73.37 FIPS; 13.1-FIPS & 13.1-NDcPP before 13.1-37.279)
	Secure Remote Access Gateway	Citrix NetScaler ADC & NetScaler Gateway (ADC: before 14.1-73.37, before 13.1-64.23, before 14.1-73.37 FIPS, and before 13.1.37.279 FIPS and NDcPP; Gateway: before 14.1-73.37 and before 13.1-64.23)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	Apple iOS and iPadOS (Before 26.7.1), Apple macOS Tahoe (Before 26.7.1), Apple macOS Sequoia (Before 15.8.1)
	Enterprise Application Platform	Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)

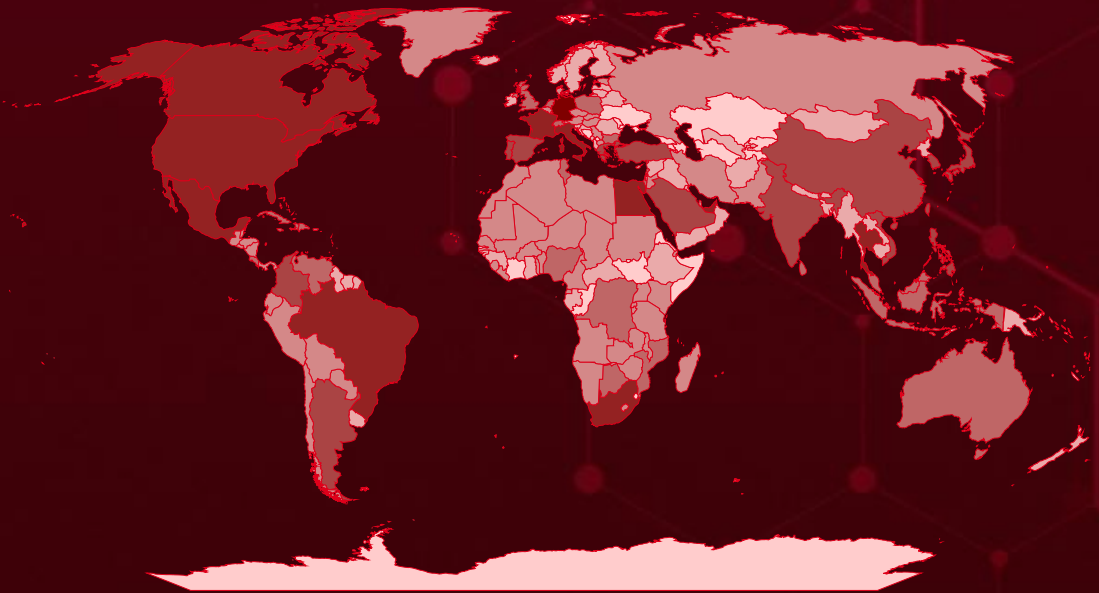


Targeted Countries

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
	Germany		Saudi Arabia		United Kingdom		Iran		Albania
	Mexico		China		Australia		Peru		Cayman Islands
	United Arab Emirates		Greece		Venezuela		Belize		Cambodia
	South Africa		Vietnam		Haiti		Burkina Faso		Maldives
	Canada		Japan		Costa Rica		Benin		Lithuania
	United States		Israel		Lebanon		Russia		Guinea
	Egypt		Dominican Republic		Chad		Bermuda		Yemen
	Singapore		Democratic Republic of Congo		Qatar		Saint Kitts and Nevis		Guinea-Bissau
	France		Mozambique		Niger		Jordan		Cape Verde
	Brazil		Sri Lanka		Czech Republic		Saint Maarten		Guyana
	Thailand		Netherlands		Serbia		Kenya		Curacao
	Italy		Tunisia		Denmark		Senegal		Fiji
	South Korea		Nigeria		Zambia		Lesotho		Uruguay
	Turkey		Malaysia		Djibouti		Seychelles		Monaco
	Taiwan		Bulgaria		Paraguay		Liberia		Romania
	Colombia		Indonesia		Dominica		Slovakia		Mongolia
	India		Poland		Saint Lucia		Libya		Bangladesh
	Philippines		Switzerland		Austria		Anguilla		Montenegro
	Spain		Bahrain		Cameroon		Madagascar		Laos
	Portugal				Ecuador		Tanzania		Montserrat
	Argentina				Pakistan		Mauritius		Suriname
	Saudi Arabia				Estonia		Morocco		Aruba
					Angola				

Targeted Industries

Most



Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1027

Obfuscated Files or Information

T1005

Data from Local System

T1071

Application Layer Protocol

T1078

Valid Accounts

T1105

Ingress Tool Transfer

T1566

Phishing

T1068

Exploitation for Privilege Escalation

T1071.001

Web Protocols

T1059.00

3
Windows Command Shell

T1083

File and Directory Discovery

T1036

Masquerading

T1041

Exfiltration Over C2 Channel

T1657

Financial Theft

T1583

Acquire Infrastructure

T1021

Remote Services

T1082

System Information Discovery

T1053

Scheduled Task/Job

T1562

Impair Defenses

T1036.005

Match Legitimate Name or Location

T1204.002

Malicious File

T1070

Indicator Removal



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>NodeRabbit</u>	Domains	naturalapplication[.]azurewebsites[.]net, retaildemo[.]azurewebsites[.]net, tubitak[.]azurewebsites[.]net, rgbteller[.]azurewebsites[.]net, wslwebui[.]azurewebsites[.]net, plugplay[.]azurewebsites[.]net, crossdwm[.]azurewebsites[.]net, wdisystem[.]azurewebsites[.]net, wslmenus[.]azurewebsites[.]net, dnshnsdev[.]azurewebsites[.]net, hpjumpsrv[.]azurewebsites[.]net, storview[.]azurewebsites[.]net, healthcomfsdpower[.]com, visitfinancedentists[.]com, kyrasey-f8hfixa5cqamh7fk[.]westeurope-01[.]azurewebsites[.]net, greenyjsbfd[.]azurewebsites[.]net, helptellerbls[.]azurewebsites[.]net, timedrv[.]azurewebsites[.]net, userwellgtfs[.]azurewebsites[.]net, hecowime-aqdphyd4bbdef6es[.]westeurope-01[.]azurewebsites[.]net, msmanagementgrp[.]com, msmanagementgrpmedia[.]com
<u>PollCat</u>	URL	hxxps[:]//lifespotify[.]com/api/users/b879746e-fed9-4211-a6da-4d8223681267/otp/validate
	Filenames	RankChallenge-react-6uJSX3-main.zip, requireObject.js
	Domains	gamebarapp[.]azurewebsites[.]net, gamebarappinformation[.]azurewebsites[.]net, sahi-finance[.]com, lifespotify[.]com
<u>Retrograde/Mini Fast</u>	MD5	810F8E3B88EB05F710C09552941D6F56
	SHA256	0db36a04d304ad96f9e6f97b531934594cd95a5cea9ff2c9af249201089dc864

Attack Name	TYPE	VALUE
<u>GRIMWEDGE</u>	SHA256	69c1603f3f9015beb0097d0a3bb0f17400c314e2eae65a7ecea cd3b93ea570dc, 59dc108e22cb856c228bbf8a1ab955fb66f0844a07fe10fa0d9f c3823d2cbbcb
	Domain	ocr[.]opusaccel[.]top
<u>SUPERSTOMP</u>	SHA256	e2a59432ce2b0d83ded936374a11fca3d3defaf4aab90eb37fc a58683eae32c0
<u>LONGTALE</u>	SHA256	5eb5645511b00e4f4d73125654eeb3a3930fcf09c65685dc7f0 3f725331492e3
	URL	hxxps://xyz0102.gitprogram[.]com/a001
	Hostname	extension-management-portal.centerfjdr658.workers[.]dev, extension-management-portal.kmjukilo-lkjh.workers[.]dev
<u>ShadowPad</u>	Hostname	ms.chechity[.]com
	IPv4	79[.]133[.]56[.]90
	Domain	chechity[.]com
<u>PAYLOAD</u> <u>Ransomware</u>	SHA256	1CA67AF90400EE6CBBBD42175293274A0F5DC05315096CB2E 214E4BFE12FFB71F
	MD5	E0FD8FF6D39E4C11BDAF860C35FD8DC0, 0108656A3E1ADE6CA4F21B084F5E1208, BEA5E267F24D7DA59F6821BFFDBFF293
	TOR Address	payload6eualw6kni6v2lqn7ovjcl76ojx25z5unsyvqo3lbqy3bo5 qd[.]onion, payloadynyvabjacbun4uwhmxc7yvdzorycslnleguxjn7glahsv qd[.]onion, payloadrz5yw227brtbvdqpnlhq3rdcdekdn3rgucbcdeawq2v6 vuyd[.]onion
<u>DragonForce</u> <u>Ransomware</u>	SHA256	e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb3 77ff16eb96b22, a4eb9be98d00c961ad8c3329ee80690c1eec98d4c8fa8dd91c 371d9ecc451581
	SHA1	55acb53f348c9f6b89343dc8d96522aa75e4cfdb
	MD5	bd47ae24b03e5ba0f1ab2e95e7acb989
	File Path	C:\Users\Public\log.log
	TOR Address	3pktcrbcmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7r yqd[.]onion, z3wqggtxft7id3ibr7sriyv5gjof5fwg76slewnzwwakjuf3nlhukdid [.]onion
	TOX ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD9 1ADEA6BA55F4A856D90A65E99D20

Attack Name	TYPE	VALUE
<u>SIDEEYE</u>	SHA256	3ba215692665513abfffd4e815c5c45f2d41e5dcc4283a2a3b740930c5c417c3
	IPv4	162[.]219[.]30[.]165
<u>NeedyMantis</u>	SHA256	e842dd7642c8e04b5ec20b6393848a9c904e4832930950c16664fe7800ba382e, 9cb68f986043a576e19d32184c583b7d8f571c7219d8dc0065dced1c13f077ef, c82520eb03c084226be4eafbff46f56dca0aa8804a2a7f23a085a96afe71ef77



Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-72529</u>		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:*	PhantomCore, PhantomGraph
TrueConf Server Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-306	T1059:Command and Scripting Interpreter	https://trueconf.com/blog/update/trueconf-server-security-updates-june-2026 , https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-72530</u>		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:*	PhantomCore, PhantomGraph
TrueConf Server Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059:Command and Scripting Interpreter	https://trueconf.com/blog/update/trueconf-server-security-updates-june-2026 , https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-82078</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng:*.~*.~*.~*.~*.~*.~*, cpe:2.3:a:papercut:papercut_mf:*.~*.~*.~*.~*.~*.~*	-
PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-470	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter, T1070:Indicator Removal	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-81578</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng:*.~.*.*.*.*.*.*,* cpe:2.3:a:papercut:papercut_mf:*.~.*.*.*.*.*.*.*	-
PaperCut NG and PaperCut MF Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190:Exploit Public-Facing Application, T1562:Impair Defenses	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-83548</u>		SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform- hotfix) and older versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918, CWE-441	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-83549</u>		SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform- hotfix) and older versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-32475</u>		WordPress Elementor Pro (Before 4.2.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:elementor:elementor_pro:*:*:*:*:*	-
WordPress Elementor Pro Unauthenticated Arbitrary File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/plugins/elementor/

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

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85706</u>		GitLab CE/EE self-managed (18.7 before 19.1.8; 19.2 before 19.2.6; 19.3 before 19.3.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:**, cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*.*	-
GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1005: Data from Local System	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-76461</u>		Cisco Secure Email Gateway (AsyncOS): 15.5 and earlier (before 15.5.5- 014), 16.0 (before 16.0.4-302), 16.5 (before 16.5.0-780)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Cisco Secure Email Gateway SQL Injection Vulnerability		cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*,* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:*:*:*:*:*:*:*,* cpe:2.3:h:cisco:secure_email_gateway:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-87886</u>		Acronis Backup plugin for cPanel & WHM (Before 1.9.3.1021); Acronis Backup extension for Plesk (Before 1.8.11.638)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:acronis:backup_plugin_for_cpanel_and_whm:*:*:*:*:*:*:**, cpe:2.3:a:acronis:backup_extension_for_plesk:*:*:*:*:*:*:*	-
Acronis Backup Incorrect Default Permissions Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-276	T1068: Exploitation for Privilege Escalation	https://security-advisory.acronis.com/updates/UPD-2609-3d72-20a7 , https://security-advisory.acronis.com/updates/UPD-2609-efb0-50b2 , https://security-advisory.acronis.com/advisories/SEC-10986

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-84869</u>		ConnectWise ScreenConnect client version before 26.6.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*	XMRig cryptominer
ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269, CWE-862	T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism	https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42016</u>		JFrog Artifactory Self-Hosted Before 7.133.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	-
JFrog Artifactory Incorrect Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1583: Acquire Infrastructure, T1587: Develop Capabilities, T1528: Steal Application Access Token, T1190: Exploit Public-Facing Application	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42018</u>		JFrog Artifactory Self-Hosted Before: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	-
JFrog Artifactory Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1562: Impair Defenses	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-82329</u>		JFrog Artifactory Self-Hosted 7.111.4 to: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.37; 7.161.0 to 7.161.19	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	-
JFrog Artifactory Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1562: Impair Defenses	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-7273</u>		Zyxel GS1900-8 (Before 2.90(AAHH.2)C0), GS1900-8HP (Before 2.90(AAHI.2)C0), GS1900-10HP (Before 2.90(AAZI.2)C0), GS1900-16 (Before 2.90(AAHJ.2)C0), GS1900-24 (Before 2.90(AAHL.2)C0), GS1900-24E (Before 2.90(AAHK.2)C0), GS1900-24EP (Before 2.90(ABTO.2)C0), GS1900-24HPv2 (Before 2.90(ABTP.2)C0), GS1900-48 (Before 2.90(AAHN.2)C0), GS1900-48HPv2 (Before 2.90(ABTQ.2)C0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:gs1900-8_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-8hp_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-10hp_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-16_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-24_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-24e_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-24ep_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-24hpv2_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-48_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:gs1900-48hpv2_firmware:*:*:*:*:*:*	-
Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-93616</u>		Check Point Security Management, Multi-Domain Security Management Server, Log Server, Multi- Domain Log Server, SmartEvent (R82.20; R82.10 with Jumbo Hotfix Take 44 or lower; R82 with Take 126 or lower; R81.20 with Take 166 or lower; R81.10 with Take 190 or lower, EoS; R80, R80.10, R80.20, R80.30, R80.40, R81, all EoS)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:checkpoint:security_management:*:*:*:*:*:*	-
Check Point Multiple Products Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.checkpoint.com/results/sk/sk1000171/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85102</u>		Check Point Security Gateway, Spark Firewall Centrally Managed, Spark Firewall Locally Managed (R81, EoS; R81.10, EoS; R81.10.x; R81.20; R82; R82.00.x; R82.10)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:checkpoint:security_gateway:*.~.*.*.*.*.*.*	-
Check Point Multiple Products Improper Certificate Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-295	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.checkpoint.com/results/sk/sk1000117

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-94127</u>		F5 BIG-IP APM (17.1.0 - 17.1.3, 17.5.0 - 17.5.1, 21.1.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*	-
F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://my.f5.com/magazine/s/article/K000162605

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-93952</u>		Arista VeloCloud Orchestrator (VCO) On- Prem (5.2.x before 5.2.3.16, 6.1.x through 6.1.3.7, 6.4.x before 6.4.2.8, 7.0.x through 7.0.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*.*	-
Arista VeloCloud Orchestrator Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-87902</u>		WordPress WordPress Core (4.7.0 – 7.1.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress:*.~*~*~*~*~*~*	-
WordPress Unauthenticated Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-98	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/download/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-52271</u>		Topaz Antifraud (wsftprm.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:topazevolution:antifraud:*:*:*:*:*:*	DragonForce Ransomware
Topaz Antifraud Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1068: Exploitation for Privilege Escalation	Update to the latest version above 2.0.0.0.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-61155</u>		Tower of Fantasy (Gamedriverx64.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:hotta_studio:gamedriverx64.sys:*:*:*:*:*:*	DragonForce Ransomware
Hotta Studio GameDriverX64 Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1068: Exploitation for Privilege Escalation	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-1055</u>		K7 Security (K7RKScan.sys driver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	-	DragonForce Ransomware
K7 Computing K7 Security Anti-Malware Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-862	T1068: Exploitation for Privilege Escalation	K7 Security Anti-Malware (K7RKScan.sys) - Fixed in version 23.0.0.10 or later.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-88771</u>		Citrix NetScaler ADC & NetScaler Gateway (14.1 before 14.1-73.37; 13.1 before 13.1-64.23; 14.1- FIPS before 14.1-73.37 FIPS; 13.1-FIPS & 13.1- NDcPP before 13.1- 37.279)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* *	-
Citrix NetScaler Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-88772</u>		Citrix NetScaler ADC & NetScaler Gateway (ADC: before 14.1-73.37, before 13.1-64.23, before 14.1-73.37 FIPS, and before 13.1.37.279 FIPS and NDcPP; Gateway: before 14.1- 73.37 and before 13.1- 64.23)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* *	-
Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1499: Endpoint Denial of Service	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-35273</u>		Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)	ShinyHunters
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:peoplesoft,_enterprise_peopletools:*:*,:*:*:*:*:*	SIDEEYE backdoor
Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>NodeRabbit</u>	A cross-platform Node.js RAT and Mirage Kitten's first Node.js implant, running on Windows, Linux, and macOS. Launched by a trojanized npm package, it persists by masquerading as legitimate updaters and encrypts C2 traffic with AES-256-GCM. Across three variants it supports up to 23 commands.	Trojanized coding-challenge archives	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote access, data exfiltration	Windows, Linux, macOS
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-

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
PollCat	A cross-platform RAT written in obfuscated JavaScript, delivered via an OTP-gated React coding challenge. It runs independently of the lure, registers with its C2, and profiles the host against 24 security-vendor directories. It declares 22 commands and persists via scheduled tasks, cron, or LaunchAgents.	Trojanized React coding challenge	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote access, host profiling	Windows, Linux, macOS
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Retrograde/MiniFast	A native Windows DLL backdoor previously attributed to Mirage Kitten, used here as PollCat's attribution comparator. It shares an identical C2 handshake, host registration, polling logic, and beacon timing, but implements functional UAC elevation and scheduled-task persistence.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, privilege escalation	Windows
ASSOCIATED ACTOR			PATCH LINK
Mirage Kitten			-

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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

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
Panzer	Panzer is a ransomware-as-a-service double-extortion operation active since August 5, 2026, advertising Windows, Linux, ESXi and FreeBSD encryptors. Claims 20+ victims across 11+ countries.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data theft, encryption	Windows, Linux, ESXi, FreeBSD
ASSOCIATED ACTOR			PATCH LINK
-			-

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AppleSeed (KGH_SPY)	AppleSeed is Kimsuky's flagship espionage implant, first seen in 2019 and still active through version 2.1, with the KGH_SPY suite tracked as a closely related modular toolset from the same actor. KGH_SPY as a modular spyware suite giving the operators reconnaissance, keylogging, information-stealing and backdoor functions. The AppleSeed family ships in two forms: a Dropper variant that pulls down further malware and runs C2 commands, and a Spy variant that harvests documents, screenshots, keystrokes and USB drive listings.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Remote execution, Keystroke logging	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
HappyDoor	HappyDoor is a backdoor, with the name taken from the "happy" string found in its export DLL name and debug data. It is a DLL that stores its configuration, including C2 addresses and encryption keys, in registry paths designed to look like legitimate software, and it communicates using a custom fixed-length packet structure with several authentication fields.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Remote execution, Screen capture, File exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
HelloDoor	HelloDoor is a DLL-based backdoor and is Kimsuky's first known malware written in Rust, a language the group rarely uses. Its C2 is hosted on TryCloudflare, a temporary Cloudflare tunneling service that requires no account or setup, which makes the infrastructure behind it hard to trace. On execution it fingerprints the host using the MAC address, computer name and a fixed string, hashes that into a unique ID, and binds to local port 5555 or 5554 depending on whether its token is elevated.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Autorun tampering, Host fingerprinting, Local port-binding, Process termination	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
httpMalice	httpMalice is a backdoor, surfacing no later than December 2025. It profiles the host with Windows commands run under code page 949, indicating Korean-language (EUC-KR) targets, and its command set covers file transfer, directory archiving and upload, screen capture, in-memory payload loading, hibernation and self-removal.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent backdoor, Service creation, Remote execution	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
httpTroy	httpTroy is the final-stage backdoor in a Kimsuky three-part chain. Its role is long-term access and data exfiltration. It marks infected hosts by writing eight random bytes to an Alternate Data Stream, depending on whether it holds an elevated token. It is heavily obfuscated: API calls are hidden behind custom hashing and strings are scrambled with XOR and SIMD operations, with both reconstructed at runtime rather than reused, which frustrates static analysis.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote execution, Reverse shell, File transfer, Persistent Access	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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>MemLoad</u>	MemLoad is a loader; its purpose is twofold: to keep the real backdoor off disk to evade detection and vet the target before committing the payload, using anti-VM checks and basic reconnaissance.	Spear-phishing attachment	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Payload delivery, Memory injection, Scheduled-task persistence, Privilege check	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
HTTPSpy	HttpSpy is a remote access trojan seen in use around April 2026 against South Korean military and enterprise targets. The newer variant abandons the old single-binary design for a three-stage chain with the final RAT decrypted and executed entirely in memory. Its command set covers shell execution, file upload in chunks and download, screen capture, secure file wiping, timestomping, DLL injection into a chosen process, execution in a specified terminal session, TCP connectivity testing, live config updates and full self-uninstall.	Spear-phishing attachments	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote execution, File exfiltration, File download	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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
AsyncRAT	AsyncRAT is a widely available open-source .NET remote access trojan, not custom Kimsuky tooling; the group adopts it alongside other commodity RATs. In Kimsuky's hands, it appears most prominently in the campaign tracks as Operation GitPower, where encrypted AsyncRAT payloads are staged in Git repositories disguised as image files, with GitHub serving as both the distribution point and the C2 channel so traffic blends into trusted developer infrastructure.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote control, Keystroke logging, Screen capture, Credential theft	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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>StormousX</u>	StormousX is the ransomware program the Stormous group has marketed under its own brand since 2023 and later offered alongside GhostLocker through the STMX_GhostLocker affiliate service. It is advertised as a file-encrypting payload supporting the group's double-extortion operations, with victims listed across multiple regions.	phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data theft and public leak	-
ASSOCIATED ACTOR			PATCH LINK
Stormous			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XMRig</u>	XMRig is an open-source, cross-platform Monero (XMR) cryptocurrency miner that is legitimate software but is one of the most widely abused tools in illicit cryptojacking, as attackers embed it in malware chains to hijack victim CPU resources for mining.	social engineering	CVE-2026-84869
TYPE		IMPACT	AFFECTED PLATFORM
Cryptominer		Resource hijacking, persistent access	ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
-			https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

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>PAYLOAD Ransomware</u>	PAYLOAD is a ransomware instead of deploying an encryptor on Windows systems, it turns Active Directory Group Policy into a weapon. The attackers got in through a FortiGate SSL VPN using stolen credentials, gained domain admin-level control, and linked a malicious GPO named "PAYLOAD" at the domain root.	Malicious GPO	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Wallpaper hijack, Admin lockout, Data exfiltration	Microsoft Active Directory (Group Policy), Fortinet FortiGate SSL VPN, VMware ESXi
ASSOCIATED ACTOR			PATCH LINK
-			-

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DragonForce Ransomware	DragonForce, now operating as a ransomware cartel, has deployed Backdoor.Turn, a Go-based backdoor that hides command-and-control inside legitimate Microsoft Teams TURN-relay traffic. It pairs this with multi-driver BYOVD exploitation to terminate security tools at kernel level. Its 32-bit Windows locker then encrypts local files and reachable SMB shares using ChaCha8 and RSA-4096.	DLL sideloading, BYOVD	CVE-2023-52271 CVE-2025-61155 CVE-2025-1055
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, extortion	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SIDEEYE</u>	A multi-stage C++ backdoor delivered in-memory on compromised Windows PeopleSoft servers, capable of stealing browser and desktop-application credentials, file/process management, interactive reverse shell, and reverse-proxy tunneling.	Trojanized Ple64.exe installer	CVE-2026-35273
TYPE		IMPACT	AFFECTED PLATFORM
Multi-stage backdoor		Credential theft, remote control	Oracle PeopleSoft PeopleTools
ASSOCIATED ACTOR			PATCH LINK
ShinyHunters			https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

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>NeedyMantis</u>	NeedyMantis is a modular, post-compromise backdoor used by the China-based threat actor Storm-3069 to keep hidden, long-term access to networks it has already broken into. It is delivered through : the attackers place a trusted program such as Poedit, curl, Vim, or TightVNC next to a malicious DLL and an encrypted archive, so the trusted program loads the malware without raising suspicion. They then spread the same bundle to other machines with the Impacket toolkit.	DLL sideloading	-
TYPE		IMPACT	AFFECTED PLATFORM
Modular		Persistent Access, System Reconnaissance, Defense Evasion, Remote Control	Windows
ASSOCIATED ACTOR			PATCH LINK
Storm-3069			-

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

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-</u> <u>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, FinTech	Middle East and Africa
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	TARGETED CVE		
	-	NodeRabbit, PollCat, Retrograde/MiniFast	Windows, linux and mac
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			

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

TTPs

TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0006: Credential Access, TA0007: Discovery, TA0005: Defense Evasion, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1584: Compromise Infrastructure, T1608: Stage Capabilities, T1588: Obtain Capabilities, T1566: Phishing, T1190: Exploit Public-Facing Application, T1200: Hardware Additions, T1219: Remote Access Tools, T1059: Command and Scripting Interpreter, T1204: User Execution, T1610: Deploy Container, T1505: Server Software Component, T1547: Boot or Logon Autostart Execution, T1543: Create or Modify System Process, T1053: Scheduled Task/Job, T1078: Valid Accounts, T1110: Brute Force, T1552: Unsecured Credentials, T1528: Steal Application Access Token, T1087: Account Discovery, T1046: Network Service Discovery, T1083: File and Directory Discovery, T1562: Impair Defenses, T1036: Masquerading, T1070: Indicator Removal, T1620: Reflective Code Loading, T1021: Remote Services, T1119: Automated Collection, T1572: Protocol Tunneling, T1090: Proxy, T1071: Application Layer Protocol, T1568: Dynamic Resolution, T1105: Ingress Tool Transfer, T1567: Exfiltration Over Web Service, T1657: Financial Theft, T1584.004: Server, T1608.001: Upload Malware, T1588.001: Malware, T1588.002: Tool, T1588.007: Artificial Intelligence, T1566.004: Spearphishing Voice, T1219.002: Remote Desktop Software, T1059.001: PowerShell, T1059.004: Unix Shell, T1204.002: Malicious File, T1505.003: Web Shell, T1547.001: Registry Run Keys / Startup Folder, T1543.003: Windows Service, T1053.005: Scheduled Task, T1078.002: Domain Accounts, T1110.003: Password Spraying, T1552.001: Credentials In Files, T1552.007: Container API, T1087.002: Domain Account, T1562.001: Disable or Modify Tools, T1562.004: Disable or Modify System Firewall, T1036.005: Match Legitimate Name or Location, T1070.001: Clear Windows Event Logs, T1070.004: File Deletion, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1090.001: Internal Proxy, T1071.001: Web Protocols, T1071.004: DNS

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

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

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

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

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Kimsuky (aka APT43, Thallium, Velvet Chollima, Black Banshee, Emerald Sleet, Ruby Sleet, Sparkling Pisces, Springtail, TA427, TA406, Earth Kumiho, PatheticSlug, ARCHIPELAGO, SharpTongue, ITG16, Greendinosa, RGB-D5, Cerium)</u>	North Korea	Government, Public Administration, Defense, Think Tanks, Policy Research Institutes, Academia, Universities, NGOs, Human Rights Organizations, Media, Healthcare, Machinery, Energy, Nuclear Power Operations, Manufacturing, Business Services, Legal Services, Construction, Financial, Insurance, Retail, Cryptocurrency	South Korea, United States, Japan, Vietnam, Thailand, Brazil, Germany, Russia, Canada, and broader Europe including Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, and Albania
	MOTIVE		
	Espionage, Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2017-11882 CVE-2018-0802 CVE-2019-0708 CVE-2019-1405 CVE-2020-0787 CVE-2024-1709 CVE-2025-48703	AppleSeed (KGH_SPY), AlphaSeed, HappyDoor, PebbleDash, HelloDoor, httpMalice, httpTroy, MemLoad, HTTPSpy, AsyncRAT, BabyShark, GoldDragon, KLogEXE, Troll Stealer, Gomir, NavRAT, NikiHTTP, NikiTeaR, ComeBacker, DRATzarus, FastFire, FastSpy, FlowerPower, RandomQuery, Yorekey, Grease, TRANSLATEXT, QuasarRAT, Gh0st RAT, KimJongRAT, CSPY Downloader, BITTERSWEET, VENOMBITE, xRAT, MailFetch.py, Reger Dropper, Pidoc Dropper	GitHub, Pastebin, Dropbox, Slack, Cloudflare Quick Tunnels, Visual Studio, Microsoft 365, Okta

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1566: Phishing; T1657: Financial Theft; T1041: Exfiltration Over C2 Channel; T1204: User Execution; T1082: System Information Discovery; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1111: Multi-Factor Authentication Interception; T1056: Input Capture; T1102: Web Service; T1071: Application Layer Protocol; T1005: Data from Local System; T1001: Data Obfuscation; T1003: OS Credential Dumping; T1020: Automated Exfiltration; T1030: Data Transfer Size Limits; T1036: Masquerading; T1053: Scheduled Task/Job; T1055: Process Injection; T1057: Process Discovery; T1059: Command and Scripting Interpreter; T1074: Data Staged; T1078: Valid Accounts; T1083: File and Directory Discovery; T1087: Account Discovery; T1098: Account Manipulation; T1105: Ingress Tool Transfer; T1106: Native API; T1113: Screen Capture; T1115: Clipboard Data; T1123: Audio Capture; T1133: External Remote Services; T1140: Deobfuscate/Decode Files or Information; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1218: System Binary Proxy Execution; T1219: Remote Access Software; T1497: Virtualization/Sandbox Evasion; T1518: Software Discovery; T1531: Account Access Removal; T1539: Steal Web Session Cookie; T1543: Create or Modify System Process; T1547: Boot or Logon Autostart Execution; T1553: Subvert Trust Controls; T1555: Credentials from Password Stores; T1557: Adversary-in-the-Middle; T1562: Impair Defenses; T1564: Hide Artifacts; T1567: Exfiltration Over Web Service; T1572: Protocol Tunneling; T1573: Encrypted Channel; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1585: Establish Accounts; T1586: Compromise Accounts; T1587: Develop Capabilities; T1588: Obtain Capabilities; T1589: Gather Victim Identity Information; T1592: Gather Victim Host Information; T1598: Phishing for Information; T1620: Reflective Code Loading; T1622: Debugger Evasion; T1682: Query Public AI Services; T1001.001: Junk Data; T1003.001: LSASS Memory; T1027.013: Encrypted/Encoded File; T1036.005: Match Legitimate Name or Location; T1053.005: Scheduled Task; T1055.001: Dynamic-link Library Injection; T1056.001: Keylogging; T1059.001: PowerShell; T1070.003: Clear Command History; T1070.004: File Deletion; T1071.001: Web Protocols; T1074.001: Local Data Staging; T1078.003: Local Accounts; T1087.004: Cloud Account; T1102.002: Bidirectional Communication; T1204.002: Malicious File; T1218.010: Regsvr32; T1497.001: System Checks; T1518.001: Security Software Discovery; T1543.003: Windows Service; T1547.001: Registry Run Keys / Startup Folder; T1553.002: Code Signing; T1555.003: Credentials from Web Browsers; T1562.004: Disable or Modify System Firewall; T1564.004: NTFS File Attributes; T1566.001: Spearphishing Attachment; T1567.002: Exfiltration to Cloud Storage; T1573.001: Symmetric Cryptography; T1583.001: Domains; T1584.004: Server; T1585.003: Cloud Accounts; T1586.002: Email Accounts; T1587.001: Malware; T1588.002: Tool; T1589.002: Email Addresses; T1598.003: Spearphishing Link; T1588.007: Artificial Intelligence; T1566.002: Spearphishing Link; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1059.007: JavaScript; T1027.001: Binary Padding; T1036.008: Masquerade File Type; T1070.006: Timestamp; T1218.011: Rundll32; T1564.003: Hidden Window; T1071.003: Mail Protocols; T1102.001: Dead Drop Resolver

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Stormous	-	Technology, Business Services & Consulting, Manufacturing, Retail, Hospitality, Education, Healthcare, Telecommunications, Media, Government, Financial Services, Pharmaceutical, Energy, Transportation, Casino & Gambling, Aerospace and Defense, Food Service, Religion, Agriculture, Real Estate, Aviation, Insurance	United States, United Kingdom, Spain, France, Italy, Malaysia, United Arab Emirates, China, Brazil, India, Argentina, Turkey, Indonesia, Germany, Vietnam, Japan, Thailand, Uzbekistan, Iran, Lebanon, Colombia, Poland, South Africa, Taiwan, Tanzania, Tunisia, Bolivia, Canada, Cuba, Australia, Philippines, Denmark, Netherlands, Morocco, Portugal, Egypt, Croatia, Serbia, Belarus, Singapore, Mexico, Hungary, Bulgaria, South Korea, North Macedonia, Belgium, Greece, Switzerland, Saudi Arabia, Estonia, Mozambique
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	StormousX	-
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0009: Collection, TA0010: Exfiltration, TA0040: Impact, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1585: Establish Accounts, T1585.001: Social Media Accounts, T1587: Develop Capabilities, T1587.001: Malware, T1078: Valid Accounts, T1566: Phishing, T1005: Data from Local System, T1213: Data from Information Repositories, T1114: Email Collection, T1567: Exfiltration Over Web Service, T1567.002: Exfiltration to Cloud Storage, T1486: Data Encrypted for Impact, T1657: Financial Theft			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Meowciety403 (aka Nekoneko200)	-	Financial Services, Financial Brokerage and Foreign Exchange, Information Technology, IT Consulting, Technology	United Arab Emirates, Singapore, Germany
	MOTIVE		
	Financial Gains, Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0008: Lateral Movement, TA0040: Impact, T1078: Valid Accounts, T1059: Command and Scripting Interpreter, T1547: Boot or Logon AutoStart Execution, T1562: Impair Defenses, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1080: Taint Shared Content, T1657: Financial Theft			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShinyHunters (aka UNC6240)	-	Higher education, technology, IT services, healthcare, agriculture, transportation, government	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-35273	SIDE EYE	Oracle PeopleSoft
TTPs			
TA0043:Reconnaissance, T1595:Active Scanning, T1595.002:Vulnerability Scanning, T1596:Search Open Technical Databases, T1596.003:Digital Certificates, T1596.005:Scan Databases, TA0001:Initial Access, T1190:Exploit Public-Facing Application, TA0002:Execution, T1059:Command and Scripting Interpreter, T1059.003:Windows Command Shell, T1059.004:Unix Shell, TA0003:Persistence, T1505:Server Software Component, T1505.003:Web Shell, TA0005:Defense Evasion, T1027:Obfuscated Files or Information, T1140:Deobfuscate/Decode Files or Information, T1553:Subvert Trust Controls, T1553.002:Code Signing, TA0006:Credential Access, T1552:Unsecured Credentials, T1552.001:Credentials In Files, T1110:Brute Force, T1110.003:Password Spraying, T1555:Credentials from Password Stores, T1555.003:Credentials from Web Browsers, TA0007:Discovery, T1082:System Information Discovery, T1016:System Network Configuration Discovery, TA0008:Lateral Movement, T1021:Remote Services, T1021.004:SSH, TA0011:Command and Control, T1105:Ingress Tool Transfer, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1572:Protocol Tunneling, T1090:Proxy, T1219:Remote Access Software, TA0009:Collection, T1560:Archive Collected Data, T1560.001:Archive via Utility, TA0010:Exfiltration, T1048:Exfiltration Over Alternative Protocol, TA0040:Impact, T1491:Defacement, T1491.001:Internal Defacement			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Storm-3069</u>	China	Telecommunications, Education, Healthcare, Nonprofits, Government	Worldwide
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	NeedyMantis	-
TTPs			
TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0011: Command and Control, TA0010: Exfiltration, T1129: Shared Modules, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1036: Masquerading, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1622: Debugger Evasion, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1057: Process Discovery, T1083: File and Directory Discovery, T1570: Lateral Tool Transfer, T1021: Remote Services, T1071: Application Layer Protocol, T1573: Encrypted Channel, T1132: Data Encoding, T1105: Ingress Tool Transfer, T1041: Exfiltration Over C2 Channel, T1543.003: Windows Service, T1574.002: DLL, T1036.005: Match Legitimate Resource Name or Location, T1036.008: Masquerade File Type, T1027.013: Encrypted/Encoded File, T1027.015: Compression, T1027.007: Dynamic API Resolution, T1021.002: SMB/Windows Admin Shares, T1071.001: Web Protocols, T1573.001: Symmetric Cryptography, T1132.001: Standard Encoding			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
	T1199: Trusted Relationship	
	T1200: Hardware Additions	
	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic

Tactic	Technique	Sub-technique
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.006: Python
		T1059.007: JavaScript
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.002: Malicious File
	T1610: Deploy Container	
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1133: External Remote Services	
	T1136: Create Account	T1136.003: Cloud Account
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder

Tactic	Technique	Sub-technique
TA0003: Persistence	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.002: Software Packing
		T1027.007: Dynamic API Resolution

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
		T1070.006: Timestamp
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.010: Regsvr32
		T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
		T1550.004: Web Session Cookie
	T1553: Subvert Trust Controls	T1553.002: Code Signing
		T1553.004: Install Root Certificate
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
		T1562.006: Indicator Blocking
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.004: NTFS File Attributes
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1610: Deploy Container	
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1110: Brute Force	T1110.003: Password Spraying
	T1111: Multi-Factor Authentication Interception	

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1007: System Service Discovery	
	T1016: System Network Configuration 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	T1087.001: Local Account
		T1087.002: Domain Account
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1622: Debugger Evasion	

Tactic	Technique	Sub-technique
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
	T1080: Taint Shared Content	
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
		T1550.004: Web Session Cookie
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.001: Local Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1123: Audio Capture	
	T1213: Data from Information Repositories	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1020: Automated Exfiltration	

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1001: Data Obfuscation	T1001.001: Junk Data
	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.003: Mail Protocols
	T1090: Proxy	T1090.001: Internal Proxy
	T1102: Web Service	T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	

Tactic	Technique	Sub-technique
TA0040: Impact	T1491: Defacement	T1491.001: Internal Defacement
	T1499: Endpoint Denial of Service	
	T1531: Account Access Removal	
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.004: Server
		T1583.006: Web Services
	T1584: Compromise Infrastructure	T1584.004: Server
	T1585: Establish Accounts	T1585.001: Social Media 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
		T1588.005: Exploits
		T1588.007: Artificial Intelligence
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
	T1590: Gather Victim Network Information	T1590.002: DNS
	T1592: Gather Victim Host Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1596: Search Open Technical Databases	T1596.003: Digital Certificates

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1596: Search Open Technical Databases	T1596.005: Scan Databases
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1598.003: Spearphishing Link
		T1598.004: Spearphishing Voice

Top 5 Takeaways

#1

In September 2026, **20 zero-day vulnerabilities** surfaced. These zero-days were found across products from **PaperCut, SonicWall, Google Chrome, Adobe, Microsoft Windows, N-able, Cisco, Check Point, F5, Arista, Citrix, Apple, and Oracle.**

#2

Newly identified malware active in September included a broad mix of **backdoors and RATs**. Key discoveries were **NodeRabbit, PollCat, Retrograde/MiniFast, and SIDEYE**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

#3

Cyberattacks concentrated heavily on **Germany, Mexico, the United Arab Emirates, South Africa, and Canada, which absorbed most** of the hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4

Government, Finance, Education, Technology, and Retail 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 **TA412, UTA0560, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket, ShinyHunters, and Storm-3069**, 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 **36 significant vulnerabilities** and block the indicators related to the **12 active threat actors**, **31 active malware**, and **209 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 **36 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>NodeRabbit</u>	Domains	naturalapplication[.]azurewebsites[.]net, retaildemo[.]azurewebsites[.]net, tubitak[.]azurewebsites[.]net, rgbteller[.]azurewebsites[.]net, wslwebui[.]azurewebsites[.]net, plugplay[.]azurewebsites[.]net, crossdwm[.]azurewebsites[.]net, wdisystem[.]azurewebsites[.]net, wslmenus[.]azurewebsites[.]net, dnshnsdev[.]azurewebsites[.]net, hpjumpsrv[.]azurewebsites[.]net, storview[.]azurewebsites[.]net, healthcomfsdpower[.]com, visitfinancedentists[.]com, kyrasey-f8hhexa5cqamh7fk[.]westeurope-01[.]azurewebsites[.]net, greenyjsgfd[.]azurewebsites[.]net, helptellerbls[.]azurewebsites[.]net, timedrv[.]azurewebsites[.]net, userwellgtfs[.]azurewebsites[.]net, hecowime-aqdphyd4bbdef6es[.]westeurope-01[.]azurewebsites[.]net, msmanagementgrp[.]com, msmanagementgrpmedia[.]com
<u>PollCat</u>	URL	hxxps[:]//lifespotify[.]com/api/users/b879746e-fed9-4211-a6da-4d8223681267/otp/validate
	Filenames	RankChallenge-react-6uJSX3-main.zip, requireObject.js
	Domains	lifespotify[.]com

Attack Name	TYPE	VALUE
<u>PollCat</u>	Domains	gamebarapp[.]azurewebsites[.]net, gamebarappinformation[.]azurewebsites[.]net, sahi-finance[.]com
<u>Retrograde/M iniFast</u>	MD5	810F8E3B88EB05F710C09552941D6F56
	SHA256	0db36a04d304ad96f9e6f97b531934594cd95a5cea9ff2c9af2492 01089dc864
<u>COBALTSPIN</u>	SHA256	3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da 2759d27ceec
<u>REALBREEZE</u>	SHA256	2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b 74441200439a
<u>MILDFROST</u>	SHA256	c0db6ddd6222d02ad7490399d33c61ded0076f0037409dc84989 24458646d78a
<u>BOATBEAM</u>	SHA256	6d4012e0dd3b56a3e52857734fa0d582cdf3c56f0e5decc8005c8 82d1d1c6ceb
<u>KICKPLATE</u>	SHA256	f139b4ca15feffb7a6633ec1a431c5c604b397576b56b5c863ae8f e4fa14db4f
<u>XWORM</u>	SHA256	51fdd83b3737add7f3832bd0ad0b56863c0a8f7cf9bcc16fd787d1 ae4b403ce6, d2aa40cc53b40c6e76ac0677c4a54387b3f27ee94c85d9b2c3a3d 66aeef92a66, 447e3a131e62bd33b1297739a7b959a92358a97f585544690446 36a3c4f244e8
<u>JSceal</u>	SHA256	1f5acba97db6d514e4b35ba0601c5269697e8ab3bb99d097db25 ec7e74464594
<u>GRIMWEDGE</u>	SHA256	69c1603f3f9015beb0097d0a3bb0f17400c314e2eae65a7eceacd 3b93ea570dc, 59dc108e22cb856c228bbf8a1ab955fb66f0844a07fe10fa0d9fc3 823d2cbbcb
	Domain	ocr[.]opusaccel[.]top

Attack Name	TYPE	VALUE
<u>SUPERSTOMP</u>	SHA256	e2a59432ce2b0d83ded936374a11fca3d3defaf4aab90eb37fca58683eae32c0
<u>LONGTALE</u>	SHA256	5eb5645511b00e4f4d73125654eeb3a3930fcf09c65685dc7f03f725331492e3
	URL	hxxps://xyz0102.gitprogram[.]com/a001
	Hostname	extension-management-portal.centerfjdr658.workers[.]dev, extension-management-portal.kmjukilo-lkjh.workers[.]dev
<u>ShadowPad</u>	Hostname	ms.checcrity[.]com
	IPv4	79[.]133[.]56[.]90
	Domain	checcrity[.]com
<u>Panzer</u>	TOR Address	pnzruro7syvwvafx5mpo2fhzi4jftgquynsqf3vy5x3no57yp2iz4nyd[.]onion
	Tox ID	8C3D96497A9438794F705C055FC2FD3059F6CF11FF51060EE55ED7F0679CFC7218825BD56CB1
<u>AppleSeed (KGH_SPY)</u>	SHA256	0845f218a588f7619169787c4db69ce9de0c84143b100400b6476d7289a1c493, 2c796053053a571e9f913fd5bae3bb45e27a9f510eace944af4b331e802a4ba0, 8c35eed98b295d2fc13cb7280e17dcbf232f6703ee74052a479196786ea9f333
<u>HappyDoor</u>	SHA256	4ac02dc231f2546ce64335729145db672b5ab01d8943df8a550cc77fc436df14
	Domains	cms[.]spaceyou[.]o-r[.]kr, erp[.]spaceme[.]p-e[.]kr
<u>HelloDoor</u>	SHA256	db284cc9b6536ab6f956a45ce9e5905716c7547f5e8dc572dc07aa125d27819e

Attack Name	TYPE	VALUE
<u>HelloDoor</u>	SHA256	62aac86f38f26700cf534c0a316d31882ffb74488bd1d87a3caeef604fc3a124
	FileName	[별지 제8호서식] 개인정보(열람 정정삭제 처리정지) 요구서(개인정보 보호법 시행규칙).hwp.jse
<u>httpMalice</u>	SHA256	23420100260cc80055fbf02f4464212278c0e71a4387537771f3fb50f2f891e5
	URL	hxxps[:]//www[.]pyrotech[.]co[.]kr/common/include/tech/default[.]php, hxxp[:]//newjo- imd[.]com/common/include/library/default[.]php
	MD5	08160acf08fccecd7b34090db18b321, 94faed9af49c98a89c8acc55e97276c9
<u>httpTroy</u>	MD5	7e0825019d0de0c1c4a1673f94043ddb
	Domains	file[.]bigcloud[.]n-e[.]kr, load[.]auraria[.]org
<u>MemLoad</u>	MD5	58ac2f65e335922be3f60e57099dc8a3, f73ba062116ea9f37d072aa41c7f5108
	SHA256	2d597c3a726970927b302bf015cec4e37cdc974959cb846dbcb23cdb46386a6c
	Domains	load[.]ssangyongcne[.]o-r[.]kr, load[.]yju[.]o-r[.]kr, attach[.]docucloud[.]o-r[.]kr, load[.]supershop[.]o-r[.]kr, load[.]erasecloud[.]n-e[.]kr
<u>HTTPSpy</u>	URLs	hxxps[:]//bigfile[.]jaycloudlab[.]com/download[.]php?id=745896 , hxxps[:]//download[.]birdriver[.]org/download[.]php?id=393156
	MD5	a581fdea0970f8a5b6cfec4853c802d7

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3
<u>StormousX</u>	TOR Address	3slz4povugieoi3tw7sblxoowxhbzxeju427cfsst5fo2tizepwatid[.]onion, h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd[.]onion, pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjns25irdgqd[.]onion, 6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd[.]onion, zib7duoiglvzvpj5faly6bio4xhwiby2lupsnxrkjnx46gmwdfyrid[.]onion, ahb6hjhe4nomgfwxequu52hazigh4ty4gdcnr3r7z5tiyhour5py2id[.]onion, stniiomyjliimcgkvdszvgen3eaa0z55hreqqx6o77yvmpt7gklffqd[.]onion, 5pbckbo5ra36srfwmb2y6mqpqj7akx3e6ewanujszv7nnjndbbgsjsad[.]onion
<u>XMRig</u>	Filename	SearchIndex.exe
<u>PAYLOAD Ransomware</u>	SHA256	1CA67AF90400EE6CBBD42175293274A0F5DC05315096CB2E214E4BFE12FFB71F
	MD5	E0FD8FF6D39E4C11BDAF860C35FD8DC0, 0108656A3E1ADE6CA4F21B084F5E1208, BEA5E267F24D7DA59F6821BFFDBFF293
	TOR Address	payloadrz5yw227brtbvdqpnlhq3rdcdekdn3rgucbcdeawq2v6vuyd[.]onion

Attack Name	TYPE	VALUE
<u>PAYLOAD Ransomware</u>	TOR Address	payload6eualw6kni6v2lqn7ovjcl76ojx25z5unsyvqo3lbqy3bo5qd[.]onion, payloadynyvabjacbun4uwvmxc7yvdzorycslnleguxjn7glahsvqd[.]onion
<u>DragonForce Ransomware</u>	SHA256	e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb377ff16eb96b22, a4eb9be98d00c961ad8c3329ee80690c1eec98d4c8fa8dd91c371d9ecc451581
	SHA1	55acb53f348c9f6b89343dc8d96522aa75e4cfdb
	MD5	bd47ae24b03e5ba0f1ab2e95e7acb989
	File Path	C:\Users\Public\log.log
	TOR Address	3pktcrbcmssvrnwe5skburdwe2h3v6ibdn5kbjqihsg6eu6s6b7ryqd[.]onion, z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion
	TOX ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20
<u>SIDEEYE</u>	SHA256	3ba215692665513abfffd4e815c5c45f2d41e5dcc4283a2a3b740930c5c417c3
	IPv4	162[.]219[.]30[.]165
<u>NeedyMantis</u>	SHA256	e842dd7642c8e04b5ec20b6393848a9c904e4832930950c16664fe7800ba382e, 9cb68f986043a576e19d32184c583b7d8f571c7219d8dc0065dc ed1c13f077ef, c82520eb03c084226be4eafbff46f56dca0aa8804a2a7f23a085a96afe71ef77

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

October 01, 2026 • 7:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com