

Date of Publication
August 4, 2026



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JULY 2026

Table Of Contents

<u>Summary</u>	03
<u>Insights</u>	04
<u>Threat Distribution</u>	05
<u>Celebrity Vulnerabilities</u>	06
<u>Vulnerabilities Summary</u>	11
<u>Attacks Summary</u>	16
<u>Adversaries Summary</u>	20
<u>Targeted Products</u>	22
<u>Targeted Countries</u>	27
<u>Targeted Industries</u>	28
<u>Top MITRE ATT&CK TTPs</u>	29
<u>Top Indicators of Compromise (IOCs)</u>	30
<u>Vulnerabilities Exploited</u>	34
<u>Attacks Executed</u>	64
<u>Adversaries in Action</u>	93
<u>MITRE ATT&CK TTPs</u>	99
<u>Top 5 Takeaways</u>	109
<u>Recommendations</u>	110
<u>Appendix</u>	111
<u>Indicators of Compromise (IoCs)</u>	112
<u>What Next?</u>	125

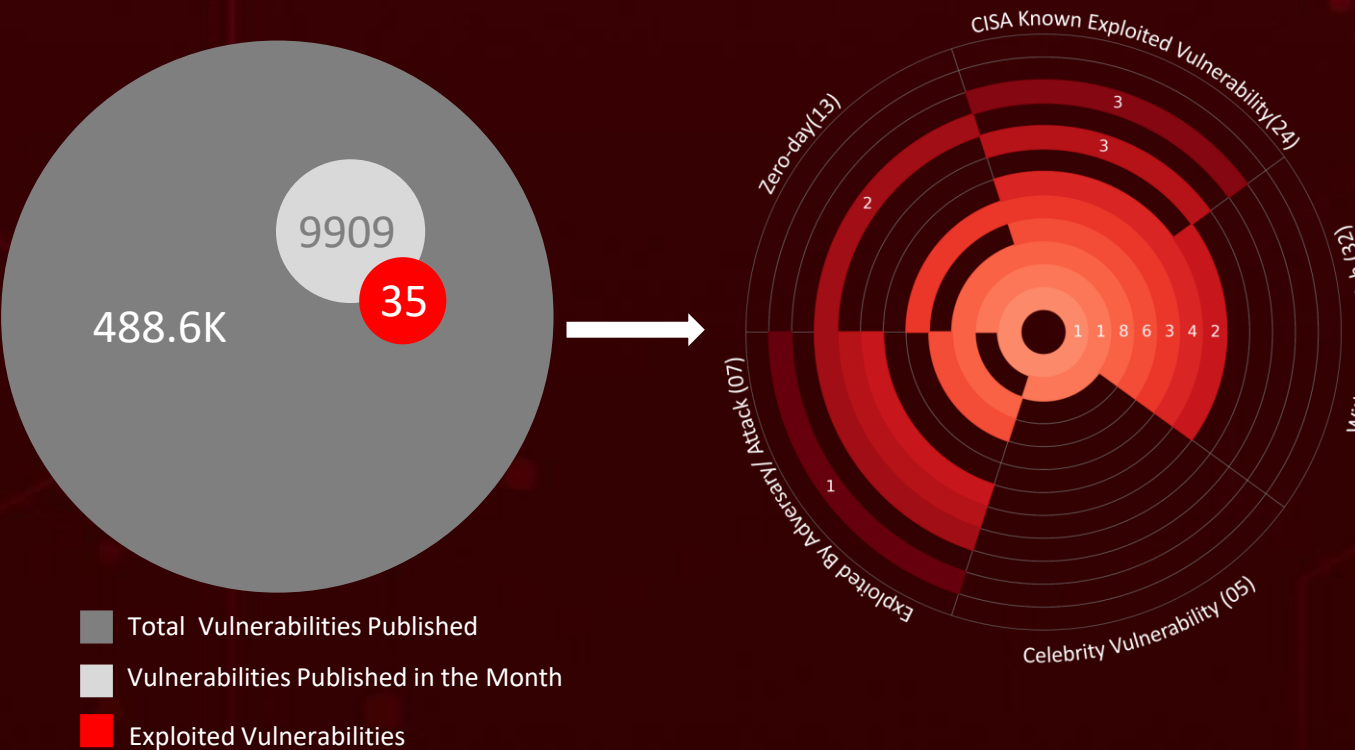
Summary

July reshaped the cybersecurity landscape with active exploitation of **thirteen** zero-days. A rising cyber-espionage threat is gaining attention: **TA488's OWAReaper campaign**. This campaign is intensifying attacks across the United States and Europe, using booby-trapped emails that exploit a Microsoft Exchange vulnerability (CVE-2026-42897) to silently infiltrate targeted systems.

Meanwhile, **UNK MassTraction**, a China-aligned espionage cluster targeting the research sector, is carrying out highly targeted espionage against North American universities' physics and engineering departments. By exploiting the CVE-2025-49113 vulnerability in Roundcube Webmail, they can execute arbitrary code and gain unauthorized access.

In response, Arista has urgently patched **CVE-2026-16812**, a maximum-severity zero-day command-injection flaw in its on-premises VeloCloud Orchestrator that hands attackers privileged internal access. On another front, attackers have been actively exploiting the **SonicWall** SMA1000 zero-days (CVE-2026-15409 and CVE-2026-15410), chaining a server-side request forgery flaw with code injection to gain unauthorized root-level access to trusted infrastructure appliances.

Finally, **Cavern Manticore**, an Iranian state-aligned APT group tied to Iran's Ministry of Intelligence and Security (MOIS), has launched a stealthy new espionage campaign. This campaign targets organizations across Israel's government, defense, and IT-services sectors, underscoring the growing threat landscape. With these increasing risks, strengthening defensive measures is more critical than ever in today's digital landscape.



In July 2026, a geopolitical cybersecurity landscape unfolds, revealing **United States, Canada, Spain, Malta, and Bulgaria** as the top-targeted countries

Highlighted in **July 2026** is a cyber battleground encompassing the **Government, Financial, Manufacturing, IT Services, and Retail** sectors, designating them as the top industries

Cisco's own firewall manager had a skeleton key baked in; **CVE-2026-20316** turns static, built-in credentials into an actively exploited zero-day.

Just opening the email is the exploit; **TA488's CVE-2026-42897** turns a glance at Outlook Web Access into OWAReaper, a backdoor that never touches the disk.

RoguePlanet (CVE-2026-50656): Race Condition LPE in the Microsoft Defender Scanning Engine

From dominant to more dominant, **Qilin's** latest chapter adds **CVE-2026-0257** to an already growing arsenal.

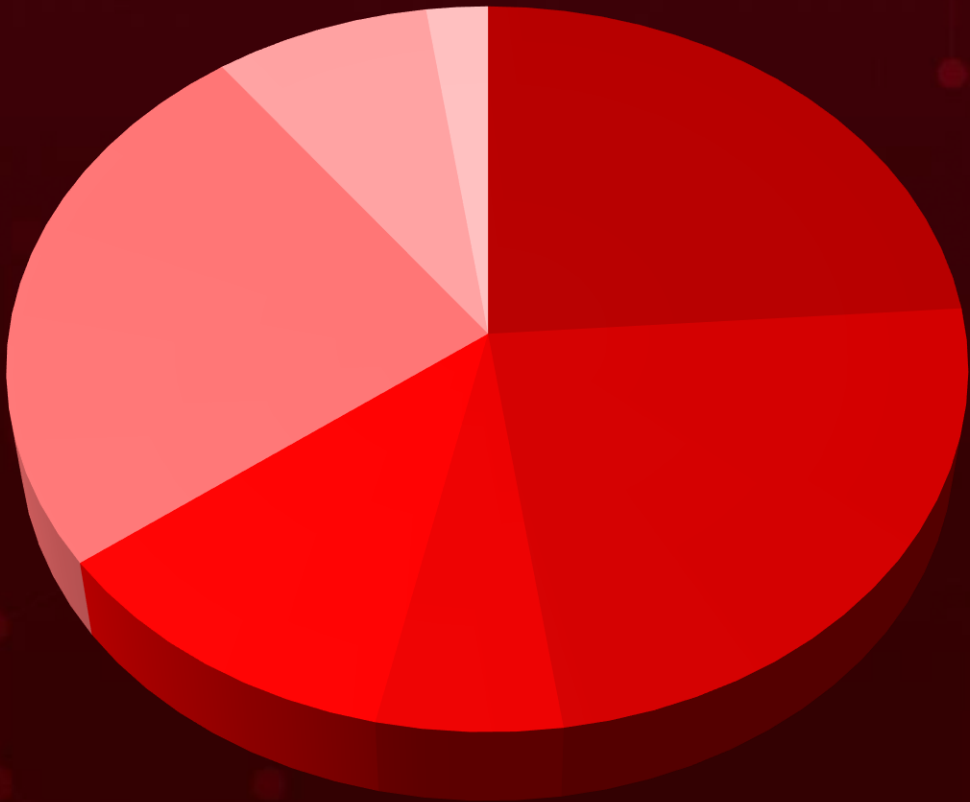
500 million WordPress sites, one flaw chain, zero authentication: **wp2shell** turns **CVE-2026-63030** and **CVE-2026-60137** into instant takeover.

LabubaRAT poses as NVIDIA software and takes C2 config at startup instead of hardcoding it, one reusable binary built for Malware-as-a-Service.

One low-tier Site Member login is all it takes; **CVE-2026-45659** turns SharePoint's insecure deserialization into full remote code execution.

Coinbase Cartel: 100 Victims, Zero Encryption, All Extortion

Threat Distribution



- Malware Attacks
- Injection Attacks
- Denial-of-Service Attacks
- Social Engineering
- Eavesdropping Attacks
- Password Attacks
- Supply Chain Attacks



Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-46242	Bad Epoll	Linux kernel: v6.4 up to (excluding) 6.18.33; v6.19 up to (excluding) 7.0.10; stable 5.15.209 up to (excluding) 5.16; stable 6.1.175 up to (excluding) 6.2. Fixed in 6.18.33, 7.0.10, and 7.1.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Bad Epoll (Linux Kernel Use After Free Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINKs
	CWE-416	T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities, T1588.006: Vulnerabilities	https://git.kernel.org/schedule/c/a6dc643c69311677c574a0f17a3f4d66a5f3744b , https://git.kernel.org/schedule/c/ced39b6a8062bac5c18a1c3df85634107eb8664a , https://git.kernel.org/schedule/c/ef4ca02e95363e78977ca04340d44fe3b4b2b81f , https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=9324de74a3a59b9fde9b62ee45ebaa71458ba2e5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-50656</u>	RoguePlanet	Microsoft Defender - Malware Protection Engine (Before 1.1.26060.3008)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:malware_protection_engine:-:*:*:*:*:*	-
Microsoft Defender Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-50656

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-5777</u>	CitrixBleed 2	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1- 37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability		cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1190: Exploit Public-Facing Application, T1539: Steal Web Session Cookie	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-63030</u>	wp2shell	WordPress WordPress Core (Version before 6.9.5 and 7.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress: *.~.*.*.*.*.*.*	-
wp2shell (WordPress Core Interpretation Conflict Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-436	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-60137</u>	wp2shell	WordPress WordPress Core (Version before 6.9.5 and 7.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress:*.~*~*~*~*~*~*	-
wp2shell (WordPress Core SQL Injection Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-29635	D-Link DIR-823X Command Injection Vulnerability	D-Link DIR-823X			
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532			
CVE-2018-8007	Apache CouchDB Privilege Escalation Vulnerability	Apache CouchDB			
CVE-2024-1781	Totolink Command Injection Vulnerability	TOTOLINK X6000R			
CVE-2026-45659	Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint Server			
CVE-2025-3248	Langflow Missing Authentication Vulnerability	Langflow			
CVE-2021-29441	Nacos AuthFilter Authentication Bypass by Spoofing Vulnerability	Alibaba Nacos			
CVE-2026-46242	Bad Epoll (Linux Kernel Use After Free Vulnerability)	Linux Kernel			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-48282	Adobe ColdFusion Path Traversal Vulnerability	Adobe ColdFusion			
CVE-2024-42009	RoundCube Webmail Cross-Site Scripting Vulnerability	Roundcube Webmail			
CVE-2025-49113	RoundCube Webmail Deserialization of Untrusted Data Vulnerability	Roundcube Webmail			
CVE-2020-22653	Ruckus Unauthorized Image Signature Injection Vulnerability	Ruckus Wireless			
CVE-2020-22658	Ruckus Unauthorized Image Boot Vulnerability	Ruckus Wireless			
CVE-2023-25717	Multiple Ruckus Wireless Products CSRF and RCE Vulnerability	Ruckus Wireless			
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler			
CVE-2026-50656	RoguePlanet (Microsoft Defender Privilege Escalation Vulnerability)	Microsoft Defender			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-56291	Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	Balbooa Forms			
CVE-2026-56164	Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability	Microsoft SharePoint Server			
CVE-2026-56155	Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability	Microsoft AD FS			
CVE-2026-50661	Windows BitLocker Security Feature Bypass Vulnerability	Microsoft Windows BitLocker			
CVE-2026-15409	SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability	SonicWall SMA1000			
CVE-2026-15410	SonicWall SMA1000 Appliances Code Injection Vulnerability	SonicWall SMA1000			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS			
CVE-2024-57727	SimpleHelp Path Traversal Vulnerability	SimpleHelp			
CVE-2025-5777	Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability	Citrix NetScaler			
CVE-2026-63030	wp2shell (WordPress Remote Code Execution Vulnerability)	WordPress Core			
CVE-2026-60137	wp2shell (WordPress SQL Injection Vulnerability)	WordPress Core			
CVE-2026-6875	ServiceNow AI Platform Remote Code Execution Vulnerability	ServiceNow AI Platform			
CVE-2026-16232	Check Point SmartConsole Improper Authentication Vulnerability	Check Point SmartConsole			
CVE-2026-0257	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-16812	Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability	Arista VeloCloud Orchestrator			
CVE-2026-12569	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	PTC Windchill and FlexPLM			
CVE-2026-16723	Alibaba FastJson Remote Code Execution Vulnerability	Alibaba Fastjson			
CVE-2026-42897	Microsoft Exchange Server Cross-Site Scripting Vulnerability	Microsoft Exchange Server			
CVE-2026-20316	Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability	Cisco Secure Firewall Management Center			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
RustDuck	Botnet	CVE-2025-29635 CVE-2017-17215 CVE-2018-8007 CVE-2024-1781	Huawei HG532, D-Link DIR-823X, Totolink X6000R, Apache CouchDB, TP-Link, ZTE, Ruijie, TVT, ThinkPHP, Jenkins, Hadoop YARN		Guessing Weak Passwords on Exposed Telnet and SSH Services, and Exploiting Known Vulnerabilities
Veil#Drop	Framework	-	Windows	-	Phishing
PureLog Stealer	Infostealer	-	Windows	-	Phishing
Ousaban	Banking Trojan	-	Windows	-	Phishing
JADEPUFFER	Ransomware	CVE-2025-3248 CVE-2021-29441	Langflow, Alibaba Nacos, MySQL, MinIO		Exploiting Vulnerability
VShell	Backdoor	CVE-2024-42009 CVE-2025-49113	Roundcube Webmail		Exploiting Vulnerability, Phishing
IceCube	Stealer	CVE-2024-42009 CVE-2025-49113	Roundcube Webmail		Exploiting Vulnerability, Phishing
SquareShell	Webshell	CVE-2024-42009 CVE-2025-49113	Roundcube Webmail		Exploiting Vulnerability, Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SNOWLIGHT	Loader	CVE-2024-42009 CVE-2025-49113	Roundcube Webmail		Exploiting Vulnerability, Phishing
SHORTLEASH	Backdoor	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	Ruckus wireless routers		Exploiting Vulnerability, Phishing
LONGLEASH	Backdoor	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	Ruckus wireless routers		Exploiting Vulnerability, Phishing
DOGLEASH	Backdoor	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	Ruckus wireless routers		Exploiting Vulnerability, Phishing
LEASHTEST	Linux binary	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	Ruckus wireless routers		Exploiting Vulnerability, Phishing
JARLEASH	Backdoor	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	Ruckus wireless routers		Exploiting Vulnerability, Phishing
AsyncRAT	RAT	-	-	-	Social Engineering
Cavern	Modular Framework	-	Windows	-	Supply Chain Compromise
GigaWiper	Backdoor	-	Microsoft Windows	-	-
CrashStealer	Infostealer	-	macOS	-	-
LabubaRAT	RAT	-	Microsoft Windows	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
TELEPUZ	Modular malware	-	Chromium-based browsers (e.g., Chrome) and Mozilla Firefox	-	ClickFix
INC Ransomware	Ransomware	CVE-2023-3519 CVE-2023-48788 CVE-2024-57727 CVE-2025-5777	Citrix NetScaler ADC and NetScaler Gateway, Fortinet FortiClient EMS , SimpleHelp Remote Support Software		Exploiting Vulnerabilities
Spirals	Ransomware	-	Windows	-	ASP. NET web shell on an internet-facing IIS server
HOLLOWGRAPH	Backdoor	-	Windows	-	Microsoft 365 mailbox calendar
HelloInjector	Loader	-	ViPNet Update System	-	DLL Sideloadng
HelloProxy	Loader	-	ViPNet Update System	-	In-memory injection (via HelloInjector)
HelloExecutor	Backdoor	-	ViPNet Update System	-	In-memory execution (via HelloProxy)
HelloCleaner	Wiper	-	ViPNet Update System	-	In-memory execution (via HelloProxy)

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
HelloBackdoor	Backdoor	-	ViPNet Update System	-	In-memory execution (via HelloProxy)
SmartLoader	Loader	-	Windows	-	Social Engineering
StealC	Information Staler	-	Windows	-	Social Engineering
Qilin Ransomware	Ransomware	CVE-2026-0257	Palo Alto Networks PAN-OS / Prisma Access		Social Engineering
OWAReaper	Backdoor	CVE-2026-42897	Microsoft Exchange Server		Exploiting Vulnerability
Tengu	Botnet	-	Linux, Android	-	Telnet credential brute force

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNK_MassTraction	Espionage and Information Theft	China	CVE-2024-42009 CVE-2025-49113	VShell, IceCube, SquareShell, SNOWLIGHT	Roundcube Webmail
UAT-7810	Espionage and Information Theft	China	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	SHORTLEASH, LONGLEASH, DOGLEASH, LEASHTEST, JARLEASH	Ruckus wireless routers
APT41	Financial crime, Information theft and espionage	China	-	-	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Cavern Manticore	Espionage	Iran (MOIS-aligned)	-	Cavern (aka Cav3rn, CAV3RN)	Remote Monitoring and Management (RMM) tooling, browser-based remote desktop technologies, Active Directory, LDAP, SMB, Microsoft IIS
Coinbase Cartel	Financial crime	-	-	-	Windows, Linux, VMware ESXi (projected), cloud SaaS environments
TA488	Information theft and espionage	Russia	CVE-2026-42897	OWAReaper	Microsoft Exchange Server



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Collaboration Server	SharePoint Server Subscription Edition, SharePoint Server 2019, SharePoint Enterprise Server 2016
	Mail & Collaboration Server	Exchange Server
	Identity & Access Management	AD FS on Windows 10; Windows Server 2012, 2016, 2019, 2022, 2025
	Endpoint Security Software	Defender, Malware Protection Engine, before 1.1.26060.3008
	Operating System	Windows BitLocker: Windows 10 to 11 26H1; Windows Server 2016, 2019, 2022, 2025
	Operating System	Palo Alto Networks PAN-OS (PA-Series, VM-Series) Versions 10.2.x, 11.1.x, 11.2.x, 12.1.x
	Network Device	DIR-823X 240126 and 240802

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Network Device	HG532
 HTTP SERVER PROJECT	Database Server	Apache CouchDB: all versions up to and including 1.7.1
 The Smartest Network Device	Network Device	TOTO Link X6000R AX3000 9.4.0cu.852_20230719
	Application	Langflow versions prior to 1.3.0
	Application	Alibaba Nacos before 1.4.1
	Software Library	Alibaba Fastjson 1.x (1.2.68 through 1.2.83)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	Linux Kernel v6.4 up to (excluding) 6.18.33; v6.19 up to (excluding) 7.0.10; stable 5.15.209 up to (excluding) 5.16; stable 6.1.175 up to (excluding) 6.2 (fixed in 6.18.33, 7.0.10, 7.1)
	Application	Adobe ColdFusion 2025.9, 2023.20 and earlier
	Application	Roundcube Webmail prior to 1.6.8 and 1.5.8 (CVE-2024-42009); before 1.5.10 and 1.6.x before 1.6.11
	Network Device	Ruckus Wireless Networking Devices, Ruckus Wireless Admin
	Network Device	NetScaler ADC and NetScaler Gateway 14.1BEFORE 14.1-43.56, 13.1BEFORE 13.1-58.32NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPPNetScaler ADC 12.1-FIPSBEFORE 12.1-55.328-FIPS

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	CMS Extension / Plugin	Balbooa Forms (com_baforms): all versions up to and including 2.4.0
	Security Appliance	SonicWall SMA1000 Series 6210, 7210, 8200v: 12.4.3-03245, 12.4.3-03387, 12.4.3-03434 (platform-hotfix); 12.5.0-02283, 12.5.0-02624, 12.5.0-02800 (platform-hotfix)
	Endpoint Management Software	Fortinet FortiClientEMS 7.2.0 through 7.2.2; 7.0.1 through 7.0.10
	Application	SimpleHelp v5.5.7 and before
	Content Management System	WordPress Core: before 6.9.5 and 7.0.2
	Application	ServiceNow AI Platform: before Australia Patch 2, Yokohama Patch 12 Hot Fix 1b, Yokohama Patch 13, Zurich Patch 7b, Zurich Patch 9, Brazil EA, Brazil GA

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
 CHECK POINT	Security Software	Check Point Security Management Server / Multi-Domain Security Management: R77.30, R80, R80.10, R80.20, R80.30, R81, R81.10, R81.20, R82, R82.10
 ARISTA	Network Management Platform	Arista VeloCloud Orchestrator (VCO) On-Prem: 5.2.x before 5.2.3.14, 6.1.x before 6.1.3.4, 6.4.x before 6.4.2.4, 7.0.x before 7.0.0.1
 ptc	Application	PTC Windchill PDMLink and FlexPLM: all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030
 CISCO	Security Management Appliance	Cisco Secure Firewall Management Center (FMC) Software: 7.0.x through 7.7.x and 10.0.x releases prior to the fixed hot-fix builds

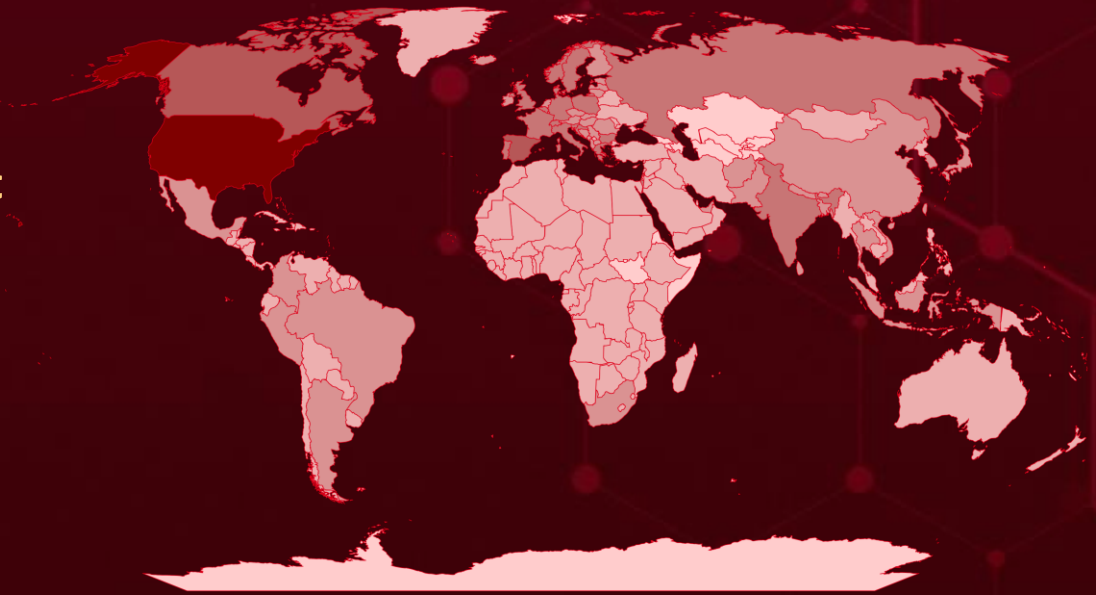


Targeted Countries

Most



Least



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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	United States		United Kingdom		Peru		Liechtenstein		Guadeloupe
	Canada		Slovakia		China		Vietnam		Panama
	Spain		Czech Republic		Bangladesh		Lithuania		Guam
	Malta		Taiwan		Luxembourg		Afghanistan		Qatar
	Bulgaria		Hungary		Romania		Timor-Leste		Guatemala
	Poland		Estonia		Maldives		Rwanda		Saint Lucia
	Russia		Iceland		San Marino		American Samoa		Guernsey
	Switzerland		Albania		Colombia		Gabon		Akrotiri and Dhekelia
	Croatia		Brazil		Singapore		Barbados		Guinea
	Belgium		Pakistan		Mexico		Benin		Ecuador
	Italy		Indonesia		Finland		Venezuela		Guinea-Bissau
	Denmark		Republic of Ireland		Monaco		Ghana		Belarus
	Norway		Andorra		South Korea		Philippines		Guyana
	France		Serbia		Montenegro		Gibraltar		Trinidad and Tobago
	Portugal		Argentina		Sri Lanka		Cyprus		Haiti
	Germany		South Africa		Nepal		Bermuda		Angola
	Slovenia		Japan		Bosnia and Herzegovina		Swaziland		Anguilla
	Greece		Bhutan		Netherlands		Greenland		French Guiana
	Sweden		Latvia		Thailand		Uganda		Honduras
	India		Holy See		North Macedonia		Grenada		Northern Cyprus
	Israel		United Arab Emirates		Austria		North Korea		Hong Kong

Targeted Industries

Most



Government



Financial



Manufacturing



IT Services



Retail



Education



Tele-communications



Aerospace



Energy



Transportation



Technology



Hospitality



Healthcare



Media



Real Estate



Aviation



Defence



Pharmaceutical



Legal



Agriculture



Insurance



Entertainment



NGOs



Automotive



Religious



Banking



Logistics



Engineering



Professional Services



Fashion



Chemical



Oil & Gas



Industrials & Engineering



Construction



Think-Tanks



Electrical



Food products



Jewellery



Gaming



Political Entities



FinTech



Biomedical



Sports



E-commerce



Maritime



Raw Material



Research Organizations



Consumers



FMCG



Extractive

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1588

Obtain Capabilities

T1036

Masquerading

T1041

Exfiltration Over C2 Channel

T1140

Deobfuscate/Decode Files or Information

T1105

Ingress Tool Transfer

T1071.001

Web Protocols

T1027

Obfuscated Files or Information

T1078

Valid Accounts

T1588.006

Vulnerabilities

T1070

Indicator Removal

T1573

Encrypted Channel

T1562

Impair Defenses

T1005

Data from Local System

T1082

System Information Discovery

T1036.005

Match Legitimate Name or Location

T1068

Exploitation for Privilege Escalation

T1021

Remote Services

T1204

User Execution

T1059.001

PowerShell

T1566

Phishing

T1486

Data Encrypted for Impact

T1505

Server Software Component



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>PureLog Stealer</u>	SHA256	7e4646d0cf91153653c5e366f98a65aad5ef363e0edeb246c809f53085971453, 3d3342af3608399704d5daf9dc061ad1f8b243531fd9ef8497a10c6a9dd59661
<u>SNOWLIGHT</u>	SHA256	e9fce3c19902fa735372c8626f8837330bbd675e58571ce9edc2400688853664, 72bb962565c44928a76b482acd93401ecd1a03c8e2ad81b691ea297ce86120ed, 93deefd83c9a0628c3602a86051611ab0900618a87163517788900aa18314056, d7768573b5fa2a95c6f8e08391d6fac7c3476b107b7fb887f1a759e235d31fa5, fcde1804f700fc2dbe2cf724c54a9b794f2d2ea8334fcf835e2cc8a0c2ea68cb, 4ab7bde56d0f7969ae6e33c7ada236dbae7e5a95f2b0c2d49618cfb47c5ce5de, 735c0e6069b17195be3a103d5cc8f73cb742a9de7d1f4f21a87793b180ce63f8, bb2df6702e3c8bb0b0bb446aed54fc7f854f31809fc0e76ab93d2aca8b248c6f, 2d05ac4e84f9b7011e13b209b4b7602685d53f61ff9670129e6bf599a41fdb5a, ce2530e405d506c60e06f4bf95c49e7a2ed221789bdb9d2404710c722d43e99c
<u>Qilin</u>	SHA256	73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdffb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bec046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38, d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
	Tor Leak Site	ijzn3sicrcy7guixkzkib4ukbiilwc3xhnmbby4mcbccnsd7j2rekvqd[.]onion
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ecec197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878f7c7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0, eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286, c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd, 02aa8cabeea2a0120a31adb0886f821d10953fc6d4d9cd1959568093c48b04d, 279b157c99432100bab17e6f23bd90cb397582324b091010d8cf1ec2683d3e4d, 6da6e608ba1bf369e01785d677c8fc95e551ee847d420a1be885677871a30134
<u>INC Ransomware</u>	SHA256	31800380c359143ae82c4f9011eee653dd22443d03d6a499148203bbfc275502, ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22, 8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4, bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc,

Attack Name	TYPE	VALUE
<u>INC Ransomware</u>	SHA256	24f6c0ca39b2a5593086ff56d818ddfbde121f8e44d54faa762e 510397dc9db7, dc9938f51150d13a69fc25f3f19052each1bf0a086fd5cf397625 01fb3ddd7da, acce811c4fc2a6e3fddd4231e386f1648ca44f039d2d275316bc 0a0fc96e0af4, 90e46e89fec2108a1cb4850bb33e3563e92a14d04e1e613ac8c 9311f152d294c, ff5da8f0330a4c581c37284c74aae2683c007dc6e406e1e2e680 3e7bb398b77b, 97aebda5482899fef84a24e456bff055acaa47e5ab4029f768d9 e0c62a660ce2, 1d10d8f5a420d0e4683b4cb40bcf0c984d1e7ea1f3b4442a00a 525584632ac11, f6a01d0246ce31faf6938ea488086d4358505405a4ef5c5faa48 2e79e92cb347, d65120291dee76c694f8bea54841f7f68329b499b28f4aee5ea 5c9369a7432cb, 765508aa2ec6a1b73a76a23f4fa559d32355622748c91a46ed7 b315eae2ee60a, d26bfb0147f60dc6500a9298d521ee67b49daaf4b8f8be54e7cc 8fd86a597570, 589d9480fbfec2d8e61638eb0b537183d0f9977411fd1d2c0f8e b611feebe880, 7f37351979c249417cb180b4ede0ed17e5fe2a1f08add4d7260 6b589f8fdb245, 5cc212f84d2bf3fbab165aaf09b16e00fcf2f1ccd880d24b14404 c53dcdbf241, 60aeb9f7bccf377ff02ed64783e66a62c0f976878d9729b067bc 7e5b0b9da9d6, 6cd349eda0fa6c8b274a0920852c68f8b727afea1fdbbc69ad183 cef05d9cf141, 6bf155b269d452f3c3b62832b27bbebe4da436e228dbf521155 b1d5989e3743f, 1898d056463284d849801cbdea6a3dec6c9f568f01569912c38 68a5eea9a5449
<u>SmartLoader</u>	SHA256	6f61812b300244df4921cc0eba252181bb2138f76cfe4e6848c 73a46917daee1, 66afc7d87d10dbe392898c4e5c613e0442fabbb396415c2bef3a 5ef2ac752c5ad

Attack Name	TYPE	VALUE
<u>StealC</u>	SHA256	2fc8cabf074616e31880562c58c62874e5d9e3925d2c8603460ba26560b5ffa4, ff8ee64171af93214e844d098c40b2a12e3360a23ecdc7ae9f56a31ea4248c9d, 2335e3bee58734fa08dd2b54905e0ad3e25141521f2ac3e6c3622642de392041, 398ad6a1f99275e87c34ca3ee2785e31b1d4959f4e97d2ce35bf2f61d222454e, 4f4bd485e8615f45401e0ba17c9f6543f185dea4df144a833c4cbdd17696903e, 71962aad3717cd520083309723df6dc7da4ae153a15ea1eed990c832c63db130, c825804d4c73e0264b6c169f59128479090e1854edb5344689c909340b283d32, 2db8be4701751d2cb69f3004939826181ca09faf04ecbe0511322e21cf5955a6, b65d87bdd8660a6dae6cd183964bdd27c521d94123c0f1ae6b490d5fb4963525, 3de02e03f9890e8b6707cfdcaabf5cc829d284209f54fb8496fb7ef2dd36dfcb, a0f34df9b0a19cccf41655ef4a69c28862515a4d8eb607b9ff8992f379471d12, 7f9e2dc8918ea3f90d35ff18dd92963b81e331651d234d6373e269e036606762, 65ba3988d38f83b9ee1f31cafa5bd37dc6b72279f5618aac94d71a904efa0cac, 049f644f98603e4c350f5a46e73f5b7091df869d3cb6f66d3e76ff7767ef2823, 74a37522f2b0ef1d1887d8b93bcd488365cdc675ecb715aa0d4095aa14de7454, b97a437a3058f45bae911a3b95aea1f78ae1b52da557fc67797e36dadee07592, f3eb200ac64568dbad840f6e13fe3c8651a072b1918a4e2eb28dfefaf48a2c03, 1e40fa9dd232593a6f918e0a00efcb542758768ff99afb48c8323fef0f357b55, c4dff48038c602d884dcdf18cdd9d39b332f5b0d76bbf7018360e786dd9320fb



Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-29635</u>		D-Link DIR-823X 240126 and 240802	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:dlink:dir-823x:- :*:*:*:*:*:*	-
D-Link DIR-823X Command Injection Vulnerability		cpe:2.3:o:dlink:dir-823x_firmware:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and scripting interpreter	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10469

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2017-17215</u>		Huawei HG532	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*	-
Huawei HG532 Remote Code Execution Vulnerability		cpe:2.3:h:huawei:hg532:-:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://www.huawei.com/en/psirt/security-notices/2017/huawei-sn-20171130-01-hg532-en

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2018-8007</u>		Apache CouchDB All versions up to and including 1.7.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:couchdb:*:*:*:*:*:*	-
Apache CouchDB Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation	https://couchdb.apache.org/#download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-1781</u>		Totolink X6000R AX3000 9.4.0cu.852_20230719	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:totolink:x6000r:- :*:*:*:*:*:* cpe:2.3:o:totolink:x6000r_firmware:9.4.0cu.852_b20230719:*:*:*:*:*	-
Totolink Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1595: Active Scanning, T1059: Command and Scripting Interpreter	https://www.totolink.tw/support_view/X6000R

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-45659</u>		Microsoft SharePoint Server Subscription Edition, SharePoint Server 2019, SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability		cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:*:enterprise:*:* cpe:2.3:a:microsoft:sharepoint_server:-:*:*:*:subscription:*:*:	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application,T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-3248</u>		Langflow versions prior to 1.3.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:langflow:langflow.*:*:*.*.*.*.*	-
Langflow Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94, CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552: Unsecured Credentials, T1552.001: Credentials In Files	https://github.com/langflow-ai/langflow/releases/tag/1.3.0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-29441</u>		Nacos before version 1.4.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:alibaba:nacos:*:*:*:*:*:*	-
Nacos AuthFilter Authentication Bypass by Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application, T1211: Exploitation for Defense Evasion	https://github.com/alibaba/nacos/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-48282</u>		ColdFusion versions 2025.9, 2023.20 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:*:*:*:*:*:*	-
Adobe ColdFusion Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-42009</u>		RoundCube Version Prior to 1.6.8 and 1.5.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail.*:*.~*~*~*~*~*	-
RoundCube Webmail Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1203: Exploitation for Client Execution	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-49113</u>		Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:roundcube:webmail.*:*.~*~*~*~*~*	-
RoundCube Webmail Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2020-22653</u>		Ruckus Wireless Networking Devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:ruckuswireless- :*:*:*:*:*:*	-
Ruckus Unauthorized Image Signature Injection Vulnerability		cpe:2.3:o:ruckuswireless- :*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-347	T1190: Exploit Public-Facing Application, T1553: Subvert Trust Controls, T1553.006: Code Signing Policy Modification, T1036: Masquerading	https://support.ruckuswireless.com/security-bulletins/302

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2020-22658</u>		Ruckus Wireless Networking Devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:h:ruckuswireless- :*.~*.~*.~*.~*.~* cpe:2.3:o:ruckuswireless- :*.~*.~*.~*.~*.~*	-
Ruckus Unauthorized Image Boot Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1190: Exploit Public-Facing Application, T1553: Subvert Trust Controls, T1553.006: Code Signing Policy Modification, T1036: Masquerading	https://support.ruckuswireless.com/security-bulletins/302

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-25717</u>		Ruckus Wireless Admin	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ruckuswireless:ruckus_wireless_admin:*:*:*:*:*:*	-
Multiple Ruckus Wireless Products CSRF and RCE Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://support.ruckuswireless.com/security_bulletins/315

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-3519</u>		NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13; NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13; NetScaler ADC and NetScaler Gateway version 12.1, now end of life; NetScaler ADC 13.1-FIPS before 13.1-37.159; NetScaler ADC 12.1-FIPS before 12.1-55.297; NetScaler ADC 12.1-NDcPP before 12.1-55.297, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13; NetScaler ADC and NetScaler Gateway 13.0 before 13.0- 91.13; NetScaler ADC and NetScaler Gateway version 12.1, now end of life; NetScaler ADC 13.1-FIPS before 13.1-37.159; NetScaler ADC 12.1-FIPS before 12.1-55.297; NetScaler ADC 12.1-NDcPP before 12.1-55.297	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKs
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX561482 , https://support.citrix.com/supporthome/kbsearch/article?articleNumber=CTX561482

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-56291</u>		Balbooa Forms (`com_baforms`) for Joomla: all versions up to and including 2.4.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:balbooa:forms:*:*:*:*:joomla\! :*:*	-
Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.balbooa.com/joomla-forms%20;%20https://www.balbooa.com/help/joomla-forms-documentation/basics/changelog

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-56164</u>		Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability		cpe:2.3:a:microsoft:sharepoint_server:*:*:*:subscription:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:enterprise:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-56155</u>		Windows 10, Windows Server 2012, 2016, 2019, 2022, 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability		cpe:2.3:o:microsoft:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1220	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56155

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-50661</u>		Windows 10 - 11 26H1, Windows Server 2016, 2019, 2022, 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:*:*:*:*:*:*:*:*	-
Windows BitLocker Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50661

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-15409</u>		SonicWall SMA1000 Series 6210, 7210, 8200v 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform- hotfix) 12.5.0-02283, 12.5.0- 02624 and 12.5.0-02800 (platform-hotfix)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-15410</u>		SonicWall SMA1000 Series 6210, 7210, 8200v 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform- hotfix) 12.5.0-02283, 12.5.0- 02624 and 12.5.0-02800 (platform-hotfix)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-48788</u>		FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*	-
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1219: Remote Access Software	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-57727</u>		SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*	-
SimpleHelp Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery, T1552.001: Unsecured Credentials: Credentials In Files	https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-6875</u>		ServiceNow AI Platform (before Australia Patch 2, Yokohama Patch 12 Hot Fix 1b, Yokohama Patch 13, Zurich Patch 7b, Zurich Patch 9, Brazil EA, and Brazil GA)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:servicenow:ai_platform:*:*:*:*:*:*	-
ServiceNow AI Platform Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3137947

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-16232</u>		Check Point Security Management Server/ Multi Domain Security Management (R77.30, R80, R80.10, R80.20, R80.30, R81 R81.10, R81.20, R82, R82.10)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:checkpoint:multi-domain_security_management:*:*:*:*:*:*	-
Check Point SmartConsole Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application,T1550: Use Alternate Authentication Material, T1550.001: Application Access Token	https://support.checkpoint.com/results/sk/sk185169/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-0257</u>		Palo Alto Networks PAN-OS / Prisma Access	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-565	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2026-0257

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-16812</u>		Arista VeloCloud Orchestrator (VCO) On- Prem (5.2.x before 5.2.3.14, 6.1.x before 6.1.3.4, 6.4.x before 6.4.2.4, 7.0.x before 7.0.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*	-
Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-12569</u>		PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ptc:windchill_pdmlink:*:*:*:*:*:*:*:*; cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*:*:*	-
PTC Windchill and FlexPLM Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502, CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.ptc.com/en/support/article/CS473270 , https://support.ptc.com/appserver/common/login/ssl/login.jsp?dest=%2Fappserver%2Fcss%2Fview%2Fsolution.jsp%3Fn%3DCS473270&msg=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-16723</u>		Alibaba FastJson 1.x (1.2.68 through 1.2.83)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:alibaba:fastjson:*:*:*:*:*:*:*	-
Alibaba FastJson Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502, CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42897</u>		Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	-
Microsoft Exchange Server Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-20316</u>		Cisco Secure Firewall Management Center (FMC) Software (7.0.x through 7.7.x and 10.0.x releases prior to the fixed hot-fix builds)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:secure_firewall_management_center:*.~.*.*.*.*.*.*.*.*	-
Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-259	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>RustDuck</u>	RustDuck is a two-stage botnet, active since February 2026, whose main purpose is launching large-scale distributed denial-of-service (DDoS) attacks. It spreads opportunistically through weak Telnet and SSH passwords, exposed Android Debug Bridge interfaces, and a mix of older vulnerabilities in devices and web applications-affecting routers, DVRs, IP cameras, and Linux servers.	Guessing Weak Passwords on Exposed Telnet and SSH Services, and Exploiting Known Vulnerabilities	CVE-2025-29635 CVE-2017-17215 CVE-2018-8007 CVE-2024-1781
TYPE		IMPACT	AFFECTED PLATFORM
Botnet		Service disruption, Network downtime, Device hijacking	Huawei HG532, D-Link DIR-823X, Totolink X6000R, Apache CouchDB, TP-Link, ZTE, Ruijie, TVT, ThinkPHP, Jenkins, Hadoop YARN
ASSOCIATED ACTOR			PATCH LINK
-			https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10469 , https://www.huawei.com/en/psirt/security-notices/2017/huawei-sn-20171130-01-hg532-en , https://couchdb.apache.org/#download , https://www.totolink.tw/support_view/X6000R

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>Veil#Drop</u>	Veil#Drop is a multi-stage delivery framework that chains social engineering, compromised websites, and malicious JavaScript launchers into PowerShell download cradles, then abuses trusted cloud-hosted infrastructure to run PureLog Stealer entirely in memory, never touching disk.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Framework		Execute Commands, load additional payload	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>PureLog Stealer</u>	PureLog Stealer is a .NET-based information stealer that harvests browser credentials, cookies, autofill data, and browsing history, alongside cryptocurrency wallet information and system reconnaissance data.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Steal Data	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>Ousaban</u>	Ousaban banking trojan campaign has been observed targeting Windows users in Spain and Portugal. The malware monitors banking sessions, captures screenshots and keystrokes, manipulates clipboard content, displays fraudulent dialogs, and grants attackers remote control of infected systems.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Banking Trojan		Credential theft, Financial fraud, Session hijacking	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>JADEPUFFER</u>	JADEPUFFER is an agentic ransomware operation run end-to-end by a large language model, with initial access gained through an internet-facing Langflow instance. It is classified as an agentic threat actor (ATA) an operator whose attack capability is delivered by an AI agent rather than a human-driven toolkit. Its payloads were self-narrating, containing natural language reasoning, target prioritization, and detailed annotations that human operators rarely write but LLM-generated code produces reflexively.	Exploiting Vulnerability	CVE-2025-3248 CVE-2021-29441
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, Data exfiltration, Financial loss	Langflow, Alibaba Nacos, MySQL, MinIO
ASSOCIATED ACTOR			PATCH LINK
-			https://github.com/langflow-ai/langflow/releases/tag/1.3.0 , https://github.com/alibaba/nacos/releases

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>VShell</u>	VShell is a cross-platform backdoor written in Go that China-aligned attackers often reach for, and because it can run without dropping files to disk it's tough to spot. Once inside, it hands attackers an interactive reverse shell, port-forwarding, and file theft across Linux, Windows, and macOS, with the shell and port-forwarding features being the ones most likely used to burrow deeper into the target's network.	Exploiting Vulnerability, Phishing	CVE-2024-42009 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINK
UNK_MassTr action			https://github.com/roundcube/roundcube-mail/releases

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>IceCube</u>	IceCube is a JavaScript-based credential stealer built for targeted cyber-espionage. Attackers slip it in through Cross-Site Scripting (XSS) flaws in webmail platforms like Roundcube, and once it runs in the victim's browser it quietly scoops up login credentials, session cookies, and even two-factor authentication (2FA) tokens.	Exploiting Vulnerability, Phishing	CVE-2024-42009 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Steal Data	Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINK
UNK_MassTr action			https://github.com/roundcube/roundcube-mail/releases

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SquareShell</u>	SquareShell is a webshell that attackers can reach remotely through the endpoint, giving them remote code execution on the server. To stay hidden, it timestamps itself, copying the last-modified date from a legitimate plugin so it blends in with the surrounding files, and it can run its commands through any of several system utilities.	Exploiting Vulnerability, Phishing	CVE-2024-42009 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Webshell		Execute Command	Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINK
UNK_MassTr action			https://github.com/roundcube/roundcube-mail/releases

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>SNOWLIGHT</u>	A lightweight Linux loader used to stage and deploy additional payloads. Commonly observed executing follow- on implants such as VSHELL and establishing persistence via system services or cron jobs.	Exploiting Vulnerability, Phishing	CVE-2024-42009 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional payload	Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINK
UNK_MassTr action			https://github.com/roundcube/roundcube-mail/releases

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>SHORTLEASH</u> <u>H</u>	SHORTLEASH is a backdoor that can call home to its command-and-control (C2) server, stand up its own web server, manage tunnels, and act as both a C2 server and client. LONGLEASH builds on that with a range of extra capabilities, a sign that UAT-7810 is actively developing it to use against their targets.	Exploiting Vulnerability, Phishing	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Ruckus wireless routers
ASSOCIATED ACTOR			PATCH LINK
UAT-7810			https://support.ruckuswireless.com/security_bulletins/302 , https://support.ruckuswireless.com/security_bulletins/315

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>LONGLEASH</u>	LONGLEASH is a newer version of SHORTLEASH, built on the same codebase, both tools even share the internal name "ff-agent." The MIPS-processor build uses the asynchronous Boost.Asio library to cut down on blocking time and squeeze the most out of the network. It can also act as an intermediate C2 server, pulling commands and data from the original C2 and passing them along to its peers.	Exploiting Vulnerability, Phishing	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Ruckus wireless routers
ASSOCIATED ACTOR			PATCH LINK
UAT-7810			https://support.ruckuswireless.com/security_bulletins/302 , https://support.ruckuswireless.com/security_bulletins/315

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>DOGLEASH</u>	DOGLEASH is a backdoor that can run arbitrary shellcode on a compromised Linux device. It binds and listens for incoming requests on a hardcoded local port, decodes any TCP data it receives using a hardcoded password string, and then, based on the command code and data that come in, spins up a new thread to carry out the requested action.	Exploiting Vulnerability, Phishing	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise, Execute Commands	Ruckus wireless routers
ASSOCIATED ACTOR			PATCH LINK
UAT-7810			https://support.ruckuswireless.com/security_bulletins/302 , https://support.ruckuswireless.com/security_bulletins/315

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>LEASHTEST</u>	LEASHTEST is a Linux (ELF) binary used to test basic functionality on MIPS-based embedded devices. It isn't malicious on its own, but finding it on a device is a strong sign of compromise. Internally named "iot-test," it checks whether it can perform a handful of rudimentary actions on an Internet-of-Things (IoT) device: create and join a thread, bind and listen on a port to open a TCP acceptor, spawn a child process, set up an async timer, print "Hello World!", and test its exception-handling routine.	Exploiting Vulnerability, Phishing	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717
TYPE		IMPACT	AFFECTED PLATFORM
Linux binary		used for testing rudimentary functionality on MIPS-based embedded devices	Ruckus wireless routers
ASSOCIATED ACTOR			PATCH LINK
UAT-7810			https://support.ruckuswireless.com/security_bulletins/302 , https://support.ruckuswireless.com/security_bulletins/315

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
JARLEASH	JARLEASH is a JAR-based backdoor that UAT-7810 drops onto both their own infrastructure and compromised systems that have Java available, giving them easy access to the machine. It comes with a startup script that first kills any running instances of JARLEASH, then spins up the Java container to deploy a fresh one.	Exploiting Vulnerability, Phishing	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Host a web-based file management interface, FTP and SFTP servers, Run a netcat server on a specified IP and port number	Ruckus wireless routers
ASSOCIATED ACTOR			PATCH LINK
UAT-7810			https://support.ruckuswireless.com/security_bulletins/302 , https://support.ruckuswireless.com/security_bulletins/315

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 an open-source Windows RAT, ranked 6th in global prevalence in 2024. Its capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Information theft, Financial Loss	-
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>Cavern</u>	Cavern is a modular .NET C2 framework built around a Cavern agent and Cavern modules that evolved from an earlier non-modular toolset internally named "Cav3rn." An older variant of mhm.dll retains legacy Cav3rn artifacts in its static configuration: file extensions .CvnC.png, .CvnA.png, .CvnR.png for command, API, and result files, a config filename Cvn.cfg, a hardcoded page name cac.aspx, and embedded JPEG header magic bytes.	Supply Chain Compromise	-
TYPE		IMPACT	AFFECTED PLATFORM
Modular Framework		Data exfiltration, Credential theft, Espionage	Windows
ASSOCIATED ACTOR			PATCH LINK
Cavern Manticore			-

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>GigaWiper</u>	GigaWiper is a versatile implant that pairs strong command-and-control (C2) features with several destructive payloads, including disk wiping, fake ransomware, and system-level sabotage. It's really an amalgamation of at least three standalone malware families stitched together as commands inside a single implant, plus new backdoor functionality on top. That backdoor lets attackers keep control of infected systems, run commands, deploy more tooling, and trigger any of its destructive options on demand, giving them the flexibility to switch between quiet espionage and full-on wiping whenever they choose.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise, Execute commands	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
CrashStealer	CrashStealer is a C++ macOS infostealer that disguises itself as Apple's crash-reporting framework to steal browser credentials, cryptocurrency wallets, and keychain data. Before sending anything out, it encrypts the stolen files with AES-GCM, then exfiltrates them to a remote command-and-control server.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Steal Data	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
<u>LabubaRAT</u>	LabubaRAT is a new remote access tool that poses as NVIDIA software to infect Windows computers. Rather than hardcoding its control server, it accepts configuration at startup, letting attackers reuse the same malware across targets. Once installed, it profiles the host to identify security tools and browsers before awaiting operator commands, indicating a reusable framework built for Malware-as-a-Service deployments.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Credential theft, Data exfiltration, Persistent access	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>TELEPUZ</u>	TELEPUZ is a modular malware that first surfaced through CLICKFIX-VIDAR attacks in April. Written in C, likely by hand, it's lightweight, modular, and reasonably well built, with sparse memory allocations, little middleware, and some features still under development. Those traits suggest the project is run by a solo developer or a very small team who code for a living. To slow down reverse engineers, TELEPUZ interleaves its real code with "garbage instructions" that serve no functional purpose; some are even designed to produce side effects, like updating global variables or calling Windows APIs, so the compiler or disassembler won't strip them out as dead code.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Modular malware		System Compromise, Persistence	Chromium-based browsers (e.g., Chrome) and Mozilla Firefox
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>INC Ransomware</u>	INC is a Rust-based ransomware-as-a-service operation (aka GOLD IONIC) that has claimed 800+ victims since 2023 and ranks among 2026's most active groups, hitting legal, manufacturing, healthcare, technology, and construction targets predominantly in the US. Operators gain entry via unpatched edge appliances (notably CVE-2023-3519 and CVE-2023-48788) or broker-supplied credentials, then use living-off-the-land binaries and a modified Veeam credential dumper to move laterally across Windows, Linux, and ESXi. Data is exfiltrated to attacker cloud storage before double-extortion encryption, with aggressive defense impairment via driver-dropping process killers and shadow-copy deletion. Pressure is applied through a Tor negotiation portal, a public leak site, wallpaper defacement, and ransom notes printed to networked printers.	Exploiting Vulnerabilities	CVE-2023-3519 CVE-2023-48788 CVE-2024-57727 CVE-2025-5777
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		File encryption, Data exfiltration, Double extortion	-
ASSOCIATED ACTOR			PATCH LINK https://support.citrix.com/support/home/kbsearch/article?articleNumber=CTX561482%20%0a;%20%0ahttps://fortiguard.fortinet.com/psirt/FG-IR-24-007%20%0a;%20%0ahttps://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities,;https://support.citrix.com/support/home/kbsearch/article?articleNumber=CTX693420,https://support.citrix.com/support/home/kbsearch/article?articleNumber=CTX561482,https://support.citrix.com/support/home/kbsearch/article?articleNumber=CTX561482,https://fortiguard.fortinet.com/psirt/FG-IR-24-007,https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities
-			

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
Spirals	Spirals is a Rust-based ransomware family used in a double extortion attack in June 2026. Attackers gained initial access via an ASP.NET web shell on an internet-facing IIS server and deployed the payload network-wide in under 24 hours, using PsExec to push it as bitsadmin.exe to impersonate a legitimate Windows utility. Files are encrypted with per-file AES-128 keys wrapped by an attacker-controlled ECDH P-256 public key, with intermittent encryption across jittered chunks applied to files over 5 MB for speed.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		File encryption, Data exfiltration, Double extortion	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>HOLLOWGR</u> <u>APH</u>	HOLLOWGRAPH is a Windows backdoor that communicates exclusively through third-party services rather than attacker-controlled infrastructure. It uses the Microsoft Graph API to exchange commands and exfiltrate data through a compromised Microsoft 365 calendar, while DNS tunneling is used to retrieve and refresh Microsoft Entra ID credentials.	Microsoft 365 mailbox calendar	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	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>HelloInjector</u>	HelloInjector is the initial loader in the HelloNet chain, deployed as a malicious wtsapi32.dll sideloaded by the signed ViPNet update binary at system startup. It decrypts an embedded payload and injects it into a netsvcs svchost.exe instance using native NT APIs, giving the operators a stealthy foothold inside a trusted, signed process.	DLL Sideload	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		System Compromise, Defense Evasion	ViPNet Update System
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
HelloProxy	HelloProxy is the main HelloNet payload, functioning as both a network proxy and an in-memory loader. It hooks network-related APIs via a legitimate hooking library and intercepts AFD IOCTLs to hinder user-mode security tools, listening on ports 5003 and 5060 behind a handshake-gated C2 to distinguish operator traffic before processing commands.	In-memory injection (via HelloInjector)	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Defense Evasion, C2 Communication, Payload Delivery	ViPNet Update System
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
HelloExecutor or	HelloExecutor is a command-execution implant used for internal reconnaissance within compromised networks. It runs discovery commands for users, groups, and network configuration, and specifically harvests ViPNet Administrator and Client export paths to map the secure-networking environment.	In-memory execution (via HelloProxy)	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Discovery, Internal Reconnaissance	ViPNet Update System
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HelloCleaner	HelloCleaner is an anti-forensic module that scrubs ViPNet software log files to erase evidence of the operators' activity, supporting the campaign's emphasis on stealth and long-dwell persistence.	In-memory execution (via HelloProxy)	-
TYPE		IMPACT	AFFECTED PLATFORM
Wiper		Defense Evasion, Indicator Removal	ViPNet Update System
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
HelloBackdoor or	HelloBackdoor is a Rust-based backdoor that listens on port 443 and activates only on receipt of a specific trigger string derived from an MD5 hash. Once active it supports file upload, download, and arbitrary command execution via the command shell, providing a resilient secondary access channel.	In-memory execution (via HelloProxy)	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote Access, Command Execution, Data Transfer	ViPNet Update System
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SmartLoader	SmartLoader sets up persistence and installs StealC, an information stealer that goes after credentials, active sessions, and other sensitive data. Attackers have used SmartLoader to target developers through convincing-looking GitHub projects, turning what feels like normal software discovery into malware delivery.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Establishes persistence and installs StealC	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>StealC</u>	StealC is an information stealer that goes after credentials, active sessions, and other sensitive data, including browser passwords, cookies, browser extension data, email and remote-access credentials, screenshots, and host details. The malware chain itself is nothing new; what changes is the route that leads to it being run.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Information Stealer		Targeting credentials, active sessions, and other sensitive data	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>Qilin Ransomware</u>	Qilin is a prolific Ransomware-as-a-Service operation whose affiliates use double extortion encrypting victims' files and stealing sensitive data to threaten public release unless a ransom is paid. In a notable evolution, affiliates now run a Linux ransomware variant on Windows hosts by abusing legitimate remote-management tools like AnyDesk, ScreenConnect, and Splashtop evading Windows-focused defenses and improving stealth in mixed-OS environments.	Social Engineering	CVE-2026-0257
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		System Compromise, Encrypt Data, Financial Loss	Palo Alto Networks PAN-OS / Prisma Access
ASSOCIATED ACTOR			PATCH LINK
-			https://security.paloaltonetworks.com/CVE-2026-0257

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>OWAReaper</u>	OWAReaper is a sophisticated backdoor delivered via half-click exploits, notable for its subtle persistence tricks. An evolution of the earlier ZimReaper payload, it shares much of the same code and behavior, including grabbing autofill passwords from the DOM with an invisible pop-up, but skips mass email exfiltration to stay quieter. It runs entirely inside the Outlook Web Access (OWA) reading pane, using Outlook APIs to rewrite the malicious email and strip out the exploit content while harvesting the victim's saved OWA credentials. For persistence, it hides an encrypted copy of itself in the browser's localStorage under a legitimate OWA settings key, so the backdoor executes automatically every time the user opens an OWA tab.	Exploiting Vulnerability	CVE-2026-42897
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Exchange Server
ASSOCIATED ACTOR			PATCH LINK
TA488			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

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
Tengu	Tengu is a Linux botnet malware family derived from Mirai but substantially more advanced in stealth and self-preservation. It spreads by brute-forcing exposed Telnet services with weak or default credentials, exploiting no software vulnerability, and targets IoT and embedded Linux devices across a wide range of processor architectures.	Telnet credential brute force	-
TYPE		IMPACT	AFFECTED PLATFORM
Botnet		Persistent compromise	Linux (embedded and IoT), Android; samples compiled for i386, amd64, MIPS, ARM, PowerPC, and m68k
ASSOCIATED ACTOR			PATCH LINK
-			-

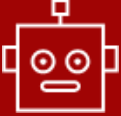
The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNK MassTracticon	China	-	-
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2024-42009 CVE-2025-49113	-	Roundcube Webmail
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0006: Credential Access; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command-and-Control; TA0010: Exfiltration; T1566: Phishing; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.004: Unix Shell; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1111: Multi-Factor Authentication Interception; T1505: Server Software Component; T1505.003: Web Shell; T1070: Indicator Removal; T1070.006: Timestamp; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UAT-7810</u>	China	-	-
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2020-22653 CVE-2020-22658 CVE-2023-25717	-	Ruckus wireless routers
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1587.001: Malware; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1620: Reflective Code Loading; T1562: Impair Defenses; T1562.004: Disable or Modify System Firewall; T1070: Indicator Removal; T1070.004: File Deletion; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1090: Proxy; T1090.003: Multi-hop Proxy; T1572: Protocol Tunneling; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Cavern</u> <u>Manticore</u>	Iran (MOIS-aligned)	-	-
	MOTIVE		
	Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Remote Monitoring and Management (RMM) tooling, browser-based remote desktop technologies, Active Directory, LDAP, SMB, Microsoft IIS
TTPs			
TA0001: Initial Access; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1199: Trusted Relationship; TA0002: Execution; T1129: Shared Modules; T1106: Native API; TA0005: Defense Evasion; T1574: Hijack Execution Flow; T1574.001: DLL; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1055: Process Injection; TA0006: Credential Access; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1110: Brute Force; T1110.001: Password Guessing; TA0007: Discovery; T1087: Account Discovery; T1087.002: Domain Account; T1069: Permission Groups Discovery; T1069.002: Domain Groups; T1018: Remote System Discovery; T1046: Network Service Discovery; T1135: Network Share Discovery; T1201: Password Policy Discovery; TA0008: Lateral Movement; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1219: Remote Access Software; TA0009: Collection; T1005: Data from Local System; T1039: Data from Network Shared Drive; T1560: Archive Collected Data; T1213: Data from Information Repositories; TA0011: Command and Control; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1572: Protocol Tunneling; TA0010: Exfiltration; T1041: Exfiltration Over C2 Channel; T1048: Exfiltration Over Alternative Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>APT41 (aka Winnti, Group 72, BARIUM, LEAD, GREF, WICKED PANDA, Earth Baku, HOODOO, Brass Typhoon, TA415)</u>	China	-	-
	MOTIVE		
	Financial crime, Information theft and espionage	-	-
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; T1127.001: MSBuild; T1127: Trusted Developer Utilities Proxy Execution; T1190: Exploit Public-Facing Application; T1574.002: DLL; T1021; TA0002: Execution; TA0011: Command and Control; TA0008: Lateral Movement; T1082: System Information Discovery; T1053.005: Scheduled Task; T1204; TA0003: Persistence; TA0010: Exfiltration; T1071: Application Layer Protocol; T1046; TA0007: Discovery; TA0009: Collection; T1059: Command and Scripting Interpreter; T1071.001: Network Service Discovery; T1053: Scheduled Task/Job; T1027: User Execution; T1574: Hijack Execution Flow; T1219: Remote Services: Obfuscated Files or Information; T1003.006: DCSync; T1041: Remote Access Software Exfiltration Over C2 Channel; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits: Web Protocols; T1548: Abuse Elevation Control Mechanism; T1059.001: PowerShell; T1003: OS Credential Dumping; T1059.003: Windows Command Shell			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Coinbase Cartel (aka <u>shinysp1d3r</u>)	-	-	-
	MOTIVE		
	Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Windows, Linux, VMware ESXi (projected), cloud SaaS environments
TTPs			
TA0001: Initial Access; T1078: Valid Accounts; T1199: Trusted Relationship; T1566: Phishing; T1566.004: Spearphishing Voice; TA0002: Execution ; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; TA0003: Persistence; T1136: Create Account; T1528: Steal Application Access Token; TA0004: Privilege Escalation; T1078: Valid Accounts; T1078.004: Cloud Accounts; TA0006: Credential Access; T1003: OS Credential Dumping; TA0005: Defense Evasion; T1070: Indicator Removal; T1562: Impair Defenses; T1090: Proxy; T1090.003: Multi-hop Proxy; TA0007: Discovery; T1580: Cloud Infrastructure Discovery; TA0008: Lateral Movement; T1021: Remote Services; T1021.004: SSH; T1021.001: Remote Desktop Protocol; TA0009: Collection; T1213: Data from Information Repositories; T1119: Automated Collection; TA0010: Exfiltration; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; TA0040: Impact; T1657: Financial Theft			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 TA488 (aka Void Blizzard, Laundry Bear)	Russia	-	-
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-42897	-	Microsoft Exchange Server
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0003: Persistence, TA0006: Credential Access, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1586: Compromise Accounts, T1583: Acquire Infrastructure, T1566: Phishing, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1070: Indicator Removal, T1098: Account Manipulation, T1555: Credentials from Password Stores, T1528: Steal Application Access Token, T1114: Email Collection, T1102: Web Service, T1090: Proxy, T1041: Exfiltration Over C2 Channel, T1048: Exfiltration Over Alternative Protocol, T1586.002: Email Accounts, T1583.001: Domains, T1059.007: JavaScript, T1070.008: Clear Mailbox Data, T1098.002: Additional Email Delegate Permissions, T1555.003: Credentials from Web Browsers, T1102.002: Bidirectional Communication			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1199: Trusted Relationship	
	T1566: Phishing	T1566.002: Spearphishing Link
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
		T1059.006: Python
		T1059.007: JavaScript
	T1106: Native API	

Tactic	Technique	Sub-technique
TA0002: Execution	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.002: Additional Email Delegate Permissions
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1542: Pre-OS Boot	T1542.001: System Firmware
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
	T1543: Create or Modify System Process	T1543.003: Windows Service
	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
	T1611: Escape to Host	
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1036: Masquerading	T1036.007: Double File Extension
	T1055: Process Injection	T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.008: Clear Mailbox Data
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1127: Trusted Developer Utilities Proxy Execution	T1127.001: MSBuild
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.004: InstallUtil
		T1218.007: Msiexec
		T1218.009: Regsvcs/Regasm
		T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1542: Pre-OS Boot	T1542.001: System Firmware
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
		T1562.004: Disable or Modify System Firewall
		T1562.006: Indicator Blocking
		T1562.009: Safe Mode Boot
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1599: Network Boundary Bridging	
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1110: Brute Force	T1110.001: Password Guessing

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1110: Brute Force	T1110.002: Password Cracking
	T1111: Multi-Factor Authentication Interception	
	T1212: Exploitation for 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	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1556: Modify Authentication Process	
	T1606: Forge Web Credentials	T1606.001: Web Cookies
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
		T1087.002: Domain Account
	T1135: Network Share Discovery	
	T1201: Password Policy Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1526: Cloud Service Discovery	
	T1580: Cloud Infrastructure Discovery	
	T1613: Container and Resource Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	

Tactic	Technique	Sub-technique
TA0009: Collection	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1213: Data from Information Repositories	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
		T1560.002: Archive via Library
TA0010: Exfiltration	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	T1001.002: Steganography
	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1102: Web Service	T1102.001: Dead Drop Resolver

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
	T1529: System Shutdown/Reboot	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe
		T1561.002: Disk Structure Wipe
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server

Tactic	Technique	Sub-technique
TA0042: Resource Development	T1585: Establish Accounts	
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
TA0043: Reconnaissance	T1590: Gather Victim Network Information	T1590.002: DNS
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1598.004: Spearphishing Voice

Top 5 Takeaways

#1

In July 2026, **thirteen zero-day** vulnerabilities surfaced. These zero-days were found across products from **SonicWall SMA1000, Arista VeloCloud Orchestrator, Cisco Secure Firewall Management Center, Microsoft Exchange, Adobe ColdFusion, Balbooa Forms, and Alibaba FastJson.**

#2

Newly identified malware active in July included a broad mix of **Ransomware, Stealers, Backdoors, RATs, and Wipers.** Key discoveries were **Spirals ransomware, JADEPUFFER, HOLLOWGRAPH, OWAREaper, CrashStealer, and GigaWiper,** each representing distinct capabilities ranging from stealthy persistence and credential theft to irreversible destruction and large-scale compromise.

#3

Cyberattacks concentrated heavily on **United States, Canada, Spain, Malta, and Bulgaria,** which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4

Government, Financial, Manufacturing, IT Services, 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 **APT41, UAT-7810, Cavern Manticore, and TA488,** 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 **35 significant vulnerabilities** and block the indicators related to the **6 active threat actors**, **33 active malware**, and **223 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 **35 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>RustDuck</u>	SHA256	a5d1b65b1055677156cd87b357ef488704115a2cbf52044dbb041072efed2f9d
<u>PureLog Stealer</u>	SHA256	7e4646d0cf91153653c5e366f98a65aad5ef363e0edeb246c809f53085971453, 3d3342af3608399704d5daf9dc061ad1f8b243531fd9ef8497a10c6a9dd59661
<u>Ousaban</u>	SHA256	ffb9eb47cc0cb2f43e04a10dc84df13d04bca1ebacbe47fad0b669728de2f59c, 18fd38988d58dd930f5992d448cc09a9400c1eafba76b820b9a83239ac48cf4e, 4ca2c863d740bb7022776dccabd8ae34bb9998768928042d76ebcf08984eefcb, 5837e47198a20877e1b04b270c36d9194206ee38d4f32fe3151b3c3b396c4f0d, e6e78eb2e9bd41a4bc62f7ad54d095ea9813864bebe37172ae30a1afa631fe14
<u>JADEPUFFER</u>	IPv4	45[.]131[.]66[.]106, 64[.]20[.]53[.]230
<u>VShell</u>	IPv4	45[.]86[.]229[.]111
	URL	hxxp[:]//45[.]86[.]229[.]111/slw[:]8080
<u>IceCube</u>	IPv4	45[.]150[.]109[.]151, 194[.]213[.]18[.]133
	URLs	hxxps[:]//45[.]150[.]109[.]151[.]sslip[.]io[:]23088/app/js/jquery[.]min [.]js

Attack Name	TYPE	VALUE
<u>IceCube</u>	URLs	hxxps[:]//194[.]213[.]18[.]133[.]sslip[.]io[:]23088/app/js/jquery[.]min [.]js, hxxps[:]//45[.]150[.]109[.]151[.]sslip[.]io[:]23088, hxxps[:]//194[.]213[.]18[.]133[.]sslip[.]io[:]23088
	SHA256	a02f124c5ce4180bd130a62ee03262f399c33491de3aed36e0b15155ae4926c0
<u>SNOWLIGHT</u>	SHA256	e9fce3c19902fa735372c8626f8837330bbd675e58571ce9edc2400688853664, 72bb962565c44928a76b482acd93401ecd1a03c8e2ad81b691ea297ce86120ed, 93deefd83c9a0628c3602a86051611ab0900618a87163517788900aa18314056, d7768573b5fa2a95c6f8e08391d6fac7c3476b107b7fb887f1a759e235d31fa5, fcde1804f700fc2dbe2cf724c54a9b794f2d2ea8334fcf835e2cc8a0c2ea68cb, 4ab7bde56d0f7969ae6e33c7ada236dbae7e5a95f2b0c2d49618cfb47c5ce5de, 735c0e6069b17195be3a103d5cc8f73cb742a9de7d1f4f21a87793b180ce63f8, bb2df6702e3c8bb0b0bb446aed54fc7f854f31809fc0e76ab93d2aca8b248cf, 2d05ac4e84f9b7011e13b209b4b7602685d53f61ff9670129e6bf599a41fdb5a, ce2530e405d506c60e06f4bf95c49e7a2ed221789bdb9d2404710c722d43e99c
<u>LONGLEASH</u>	SHA256	755fcee1337a252203002ecfdf673a08cfaded8d738bef2d518a08e0626aa4f
<u>DOGLEASH</u>	SHA256	604b53f87d6c070bf387e80c70a6df8d272fa3fc143148d41f13e59d52ab1f13

Attack Name	TYPE	VALUE
<u>DOGLEASH</u>	SHA256	c92541f273eeb576d39235d0a5c6f18f2574b132a1022598edfa38065783ab98, 29c7fccc6ef8cbfe4da9a169c7c74bacaea1fb515a1fddef91ab1b1522f76e4c, 425bf771c8c9f740b1ae9803dcb4fd45af4d6a6f171fcc72fc7d511095ca82ce, ac8eae94d27122f4751bc96d9ea52d30000b7ca37569a2291b2710824ca3396f, dc4f25b2247cfdd6fc96848db30a178baa4419a4c854e86e315b465836102d14, 3878dd5c8eba1e5b53ab2e07e7b5482e95a3fd3e98268bcd7861318bc9902376, 9b9e0e5a1eb469b8d20dc23351e08ff5d5731e1cedce0dde9bbd00a76217f13, 57bdab2ba4b05ec0338c06632599393d5b14227f31a43fe950ea8fdd47428715, b8d247fd1fb85d24a17afeec3815906dfbcfdc5359647910b4a153900ec999a0f, 5e225ea2648a8cba0fd94ec7fd8ce5315f5d0cc2922bafc9db3c8c41280e917c, d5cf7315186a78ab6a7475c338bdf101bc6461930aaa7a012a02cf93f347c207, dd0fc1a88180fde8367bec7086f99294f36b8332f12994293139ed532d2ebbac, 5c3f190571645c4641dcff2c07a4c3ab9acad06aa9607350a385729d8d6139f1, 880425fee707e9f42e0b8d60119ed639b1ad506ea29877d126bdebce379cd229, e5d2de8ae98579bfb940290f60e59a502b3065345aaf765456387989c0488b20, 2e0e43776e2e1a37d882a1b2ebb7d337ee88950177e43831dae645a367824feb,

Attack Name	TYPE	VALUE
<u>DOGLEASH</u>	SHA256	b5969636eec376ad6c3ece2202b1722219955638e09b6f96d4cfc0598d3b1890, 1660536f448b8b9f086ce9ea3ce4e9deefc59a76711ea53ee6d8f08fc8c1bb99, 65feba2c971c214e71303ad2e0fbf62b45ebcaa784cbf3d0dab62786cb4c0469, 53ac2b231c23d41234e55b1f7ed89f86234f785adbbe820959655d7b019d7df9, 33c10b77e1da9f0679023d55fb3057879d15609db9c1d46ee5c3ff1240a3d052, 5faea1650cac0f3ffd2dc1fb220182095a46e34158967d37c2a942e85e2ca97b, 62d4ec87ed21f0d15cb769b0b2a5577cab41fc2cdb1e7e796c5bdff09264dd9a, 534a4a5bff2609a2d6e088cb87465c08c2d69c6aaa7d2ffcbcd491274b8505f1, 5eab4c61baa67ae2838a36c2e6ff0476a8f2117b96a7027b830c8cb46ce78efc, 0af4c52a1d13e4132a1843ce7727abcf0ddd4d1ca6a4b17cdf599ec3f355c241, d4861088161fc72b9922abf933b4ea664a807105ec1eab4a173253aa60bfe6d7, 3d296af7f29c0425655bd1cc0be48fe4aba52ee6760a89e805ca2589f4ef4d77, f235d2e044c2f7814e6bbcd835b9fd9f10f227dacfb9396185ec2013e7df4db4, 4130f49fa81a699a667cafdbd6d1f6e781edd686c947eb8ae27134f6dc2c43d7, 0a8555a71868749be8c905ed53296ce335af50a9262772b5e154ad3f9c35c2e4, 323c3a91be60ebc3e06e942bad04899a15911cea23269e43d07829164b2ce5d4,

Attack Name	TYPE	VALUE
<u>DOGLEASH</u>	SHA256	5dbfa033676b5caacfae902734ce462cd871181eefbe299250ca8ac7e139719e, 20fcba222f74dd68aaeb1f0ad30cdf702a828ee164a182b30d05d600c35b72d9, 912adea5339c73cb4a777a3e9f98bf3cb08da6622c9dd3b4cc9b083cb03d10a2, 16971f9706d70ac4925651c7c8719b9d77aff63e4c0a618129efc32c2c46b989, 6917c0f9eafefe42e33e791b75a7e503ff8b081bc10a98449e4076787dfc6c16, c7c9bfa9ffcd8fb6a2afe656f510c406ddc58ebff48ce1d0fd3fad951b46a36e, b9fe48bda9a6c8787981a24f8bbc723a6f6aa80cab5fa53481937382f3c6ce85, f3bf4481f30fd840f35568746f54be49eb92b2c9ac95597a7760abb171cb54b, 6366d59b573d50fd23ff650923c4a8c1c918518a02d0a56f12c23533c45f439d, 3fcaa3038e365b6ab0b121e2cd319c56b74e37381943a0da0e8dce407087cdb8, bf70c6f3a8e913f526ec57eeec50e1306f7b34b037915b7a1cf2968cc46acc58, 0352f3e338261d98895df4c7b7a76b296485b2290c72bce56603351d167d0601, 52b871429833e1dee348263844efb531f6a3fcd321f88dc8a876caaae912cedd, 5db2ce9acd50f96d566e8d139f6490abf2bbf7a9293b876eeb4598fd2c37c515, 3169a6dbcce684e2c5a2f166996b58ffa673df6e58b8edf2bdf3e66271c8c69e, d871d76171504597bbda387689e12e7a5e354c360ff135f4df231cec68c761af,

Attack Name	TYPE	VALUE
<u>DOGLEASH</u>	SHA256	d1f963b88672f3676a7da1580262ba0d4f367cc57a94b551754c20f77a670c43, 76d9e2a2ff313f5b91cc67aab1127122baee1c3efbae1087e58a25bc5f1eb065, 03926e3da998f32ad898b640bd15cf145768f9e849e6f18d81350234254c424e, 8c104da0e66ef6384663309aaf8fb49f549f2785d835eec620b265f8aa11d9f0, c494c878e28284539419612616d964ab9224cbe27e57f42293d91d02d684e3db, 08701ed7975bf4f5688c2724d27ab497764200ad6f4dc53d3cc03b170378ced0, 0a8cae96e25e85c612b0736fe886f9b124ad70ec425bc2ec1a8a4135b25436ba, 8459ff264a2c81c68a34c4ee6bc109d141ad28b96037d34ff112322a4c853739, 68445a37a9943a267a8b2100fba2678353d6ec88844505ccbba659e586c7a105, 29686c933cec1e274467e2dae264625ae6f754824bb7f550bc9c3131f625562c, d973ad5a80c3d7468a9c392db4166857ed32b5d61cd6755766ba8922156dada3, f5a57dfae488d9dfe260b32460a1d947fb5af58ceaf2fb0139bc08b4bb79a966, 2ebc1b6cf543e2cb3f22d9a5b54b6676bb71dde98df7532f8791297734e44fdd, 6dbd507ca7cecea861f9cf704b3c5c37f5bd5392886a8c2562088892b7703fa5, 89f0a67bc595ab8bce02c2f95f9292ad06e1868207e809c76bd16f0cab800c06, d81201d0fc19977e51104438a5b9cba861f4da20cea3ae9183edf16ab11d98f8,

Attack Name	TYPE	VALUE
<u>DOGLEASH</u>	SHA256	9d52cb4febf3342c34dcc8198daf453458be3699ab47dc08616a a7f18daa7fa, 9a927c37a31b80975c5c5467f112b61478c9493c046281046443 525358a5acb0, 6cda1e81667f869940401f05a55c8dea94dbdf3ceffb93b5f320a6 462cfea44d, 745538dea8ed9aec4466e67a9d0aecf9e7026ff16a792d1d6f306 e8b67d3f34c, 13acadb3541e75af50e02d5be56c2238b93d8f154ce5514be155 8e6ee59a1432,
<u>LEASHTEST</u>	SHA256	1b5649b479fd625de5c8120873644b5eb669cc89cd504582c18e 0ae350fd8823
<u>JARLEASH</u>	SHA256	324d95024fc8da5c92b5a1f4825aed5a2a91c9ca8fb6aa52abb33 2a4c9cf4257, bafba443170e54ef7fd431ce7f1b5e202719f3fd022e4ef7078890 4f574d2cdf
<u>OWAReaper</u>	SHA256	6897b649f29e54d8910459963bbf94ed5c7a4fe66a56bc5962540 b226b8e48c4
	Domains	asecdns[.]com acocdn[.]com dnsrecursive[.]eu tdndns[.]com
<u>AsyncRAT</u>	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332 420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afc ff20ef524

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	SHA256	7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ecec197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bce02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878fetc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0, eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286, c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd, 02aa8cabeea2a0120a31adbf0886f821d10953fc6d4d9cd1959568093c48b04d, 279b157c99432100bab17e6f23bd90cb397582324b091010d8cf1ec2683d3e4d, 6da6e608ba1bf369e01785d677c8fc95e551ee847d420a1be885677871a30134
<u>Cavern</u>	SHA256	541b1f417b9e42078c3355693a8a492b6a76048850f6549a429e0be99e6819cb, cbc9485db715e1b8cc384fe94b4cceedca4006cda8a5e28adc8848529cfafc93

Attack Name	TYPE	VALUE
<u>Cavern</u>	SHA256	ccf218189c3aadb1c761da14bfda3bae686769031e1e1b10007648bd72e34748, 37e123bd7998af4eae32718ce254776f36365a80ba56952593da b46f536d4066
<u>GigaWiper</u>	SHA256	633d4cbd496b1094495da89a64f5e6c31a0f6d4d1488411db5b0c ba1cfe42001, ce9ad5f6c12019f4aae5b189bd8ddf5bb09e75b06a0a587b25a85 5c65948c913, f622ed85ef31ad4ab973f4e74524866fe1bb44f0965ad2b2ad796 cd657a05bfd, 9706a192e2c1a1faaf0a521daf31c2af60ff4590e3f47bbb4abc227 f42af0683, 3c30deb6556a94cfb84ae51798f4aecfae8c7358e55fdb321c5f23 76579631cd
	IPv4	185[.]182[.]193[.]21, 212[.]8[.]248[.]104
<u>CrashStealer</u>	SHA256	a1966a6d6f54a025f30d55571d21d6537977ca73ffa734c13494b 9c806cd7007
<u>LabubaRAT</u>	SHA256	b7443b0ab48d2f5786d1b6f3a580f02621e9ae5a3877ee3a44e0 1df13d984328
<u>TELEPUZ</u>	SHA256	58aec6e3835aaf20f7b4a7e308b36a19e7454673a6f71783871e9 bcf6cae8eed, bf3b4e645a3c0c23f87c55971069014f7424ad14497371ee7567e ff68ffaf343, ff791fe1532a2dc3b3c188a71bfd0177f973ef228e4d1dda1db6d3 c4b0d62b3e
<u>INC Ransomware</u>	SHA256	31800380c359143ae82c4f9011eee653dd22443d03d6a4991482 03bbfc275502

Attack Name	TYPE	VALUE
<u>INC Ransomware</u>	SHA256	ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22, 8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4, bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc, 6bf155b269d452f3c3b62832b27bbebe4da436e228dbf521155b1d5989e3743f, 1898d056463284d849801cbdea6a3dec6c9f568f01569912c3868a5eea9a5449, 24f6c0ca39b2a5593086ff56d818ddfbde121f8e44d54faa762e510397dc9db7, dc9938f51150d13a69fc25f3f19052eacb1bf0a086fd5cf39762501fb3ddd7da, acce811c4fc2a6e3fddd4231e386f1648ca44f039d2d275316bc0a0fc96e0af4, 90e46e89fec2108a1cb4850bb33e3563e92a14d04e1e613ac8c9311f152d294c, ff5da8f0330a4c581c37284c74aae2683c007dc6e406e1e2e6803e7bb398b77b, 97aebda5482899fef84a24e456bff055acaa47e5ab4029f768d9e0c62a660ce2, 1d10d8f5a420d0e4683b4cb40bcf0c984d1e7ea1f3b4442a00a525584632ac11, f6a01d0246ce31faf6938ea488086d4358505405a4ef5c5faa482e79e92cb347, d65120291dee76c694f8bea54841f7f68329b499b28f4aee5ea5c9369a7432cb, 765508aa2ec6a1b73a76a23f4fa559d32355622748c91a46ed7b315eae2ee60a, d26bfb0147f60dc6500a9298d521ee67b49daaf4b8f8be54e7cc8fd86a597570,

Attack Name	TYPE	VALUE
<u>INC Ransomware</u>	SHA256	589d9480fbfec2d8e61638eb0b537183d0f9977411fd1d2c0f8eb611feebe880, 7f37351979c249417cb180b4ede0ed17e5fe2a1f08add4d72606b589f8fdb245, 5cc212f84d2bf3fbab165aaf09b16e00fcf2f1ccd880d24b14404c53dcdbf241, 60aeb9f7bccf377ff02ed64783e66a62c0f976878d9729b067bc7e5b0b9da9d6, 6cd349eda0fa6c8b274a0920852c68f8b727afea1fdbbc69ad183cef05d9cf141
<u>Spirals</u>	SHA256	0f9574dc38e5c34a31153f0bcc603c6ec29cb3bf65c3d25380dbe86d42573141
<u>HOLLOWGRA PH</u>	SHA256	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509, F3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3, B3d0f6e4e3be395fd7cf9e8101c89963d77216578cbb117a6ac9bc3564485eff
<u>HelloInjector</u>	SHA256	ffdc194775b2904564bbbd1cf0eb01d1a01f83ef5197d1612b6e2d69de7a4732
<u>HelloBackdoor</u>	MD5	16C211C96735F2FAE9361B89BD7A31BF, 1BFE2B9493128574907A8279256A8BCC, f9eed2f0158dc98e7012fb809152209c
	SHA256	68b4c76a2280e3c31130d4de12b12dfd479a476f347f5b4a58cb2483d74aba7e
<u>SmartLoader</u>	SHA256	6f61812b300244df4921cc0eba252181bb2138f76cfe4e6848c73a46917daee1, 66afc7d87d10dbe392898c4e5c613e0442fabb396415c2bef3a5ef2ac752c5ad
<u>StealC</u>	SHA256	2fc8cabf074616e31880562c58c62874e5d9e3925d2c8603460ba26560b5ffa4

Attack Name	TYPE	VALUE
StealC	SHA256	ff8ee64171af93214e844d098c40b2a12e3360a23ecdc7ae9f56a31ea4248c9d, 2335e3bee58734fa08dd2b54905e0ad3e25141521f2ac3e6c3622642de392041, 398ad6a1f99275e87c34ca3ee2785e31b1d4959f4e97d2ce35bf2f61d222454e, 4f4bd485e8615f45401e0ba17c9f6543f185dea4df144a833c4cbd d17696903e, 71962aad3717cd520083309723df6dc7da4ae153a15ea1eed990c832c63db130, c825804d4c73e0264b6c169f59128479090e1854edb5344689c909340b283d32, 2db8be4701751d2cb69f3004939826181ca09faf04ecbe0511322e21cf5955a6, b65d87bdd8660a6dae6cd183964bdd27c521d94123c0f1ae6b490d5fb4963525, 3de02e03f9890e8b6707cfdcaabf5cc829d284209f54fb8496fb7ef2dd36dfcb, a0f34df9b0a19cccf41655ef4a69c28862515a4d8eb607b9ff8992f379471d12, 7f9e2dc8918ea3f90d35ff18dd92963b81e331651d234d6373e269e036606762, 65ba3988d38f83b9ee1f31cafa5bd37dc6b72279f5618aac94d71a904efa0cac, 049f644f98603e4c350f5a46e73f5b7091df869d3cb6f66d3e76ff7767ef2823, 74a37522f2b0ef1d1887d8b93bcd488365cdc675ecb715aa0d4095aa14de7454, b97a437a3058f45bae911a3b95aea1f78ae1b52da557fc67797e36dadee07592, f3eb200ac64568dbad840f6e13fe3c8651a072b1918a4e2eb28dfefaf48a2c03, 1e40fa9dd232593a6f918e0a00efcb542758768ff99afb48c8323fef0f357b55, c4dff48038c602d884dcdf18cdd9d39b332f5b0d76bbf7018360e786dd9320fb

Attack Name	TYPE	VALUE
<u>Qilin Ransomware</u>	Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
	SHA256	d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6, 73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38, d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
<u>Tengu</u>	SHA256	897226af37990fa60f25fea00b0509faa0e78d88bee10875c23b9b6ab0b8faed9

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

August 04, 2026 • 7:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com