

Date of Publication
September 3, 2026



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

AUGUST 2026

Table Of Contents

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

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

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

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

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

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

[Adversaries Summary](#)..... 19

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

[Targeted Countries](#)..... 24

[Targeted Industries](#)..... 25

[Top MITRE ATT&CK TTPs](#)..... 26

[Top Indicators of Compromise \(IOCs\)](#)..... 27

[Vulnerabilities Exploited](#)..... 29

[Attacks Executed](#)..... 54

[Adversaries in Action](#)..... 85

[MITRE ATT&CK TTPs](#)..... 94

[Top 5 Takeaways](#)..... 106

[Recommendations](#)..... 107

[Appendix](#)..... 108

[Indicators of Compromise \(IoCs\)](#)..... 109

[What Next?](#)..... 122

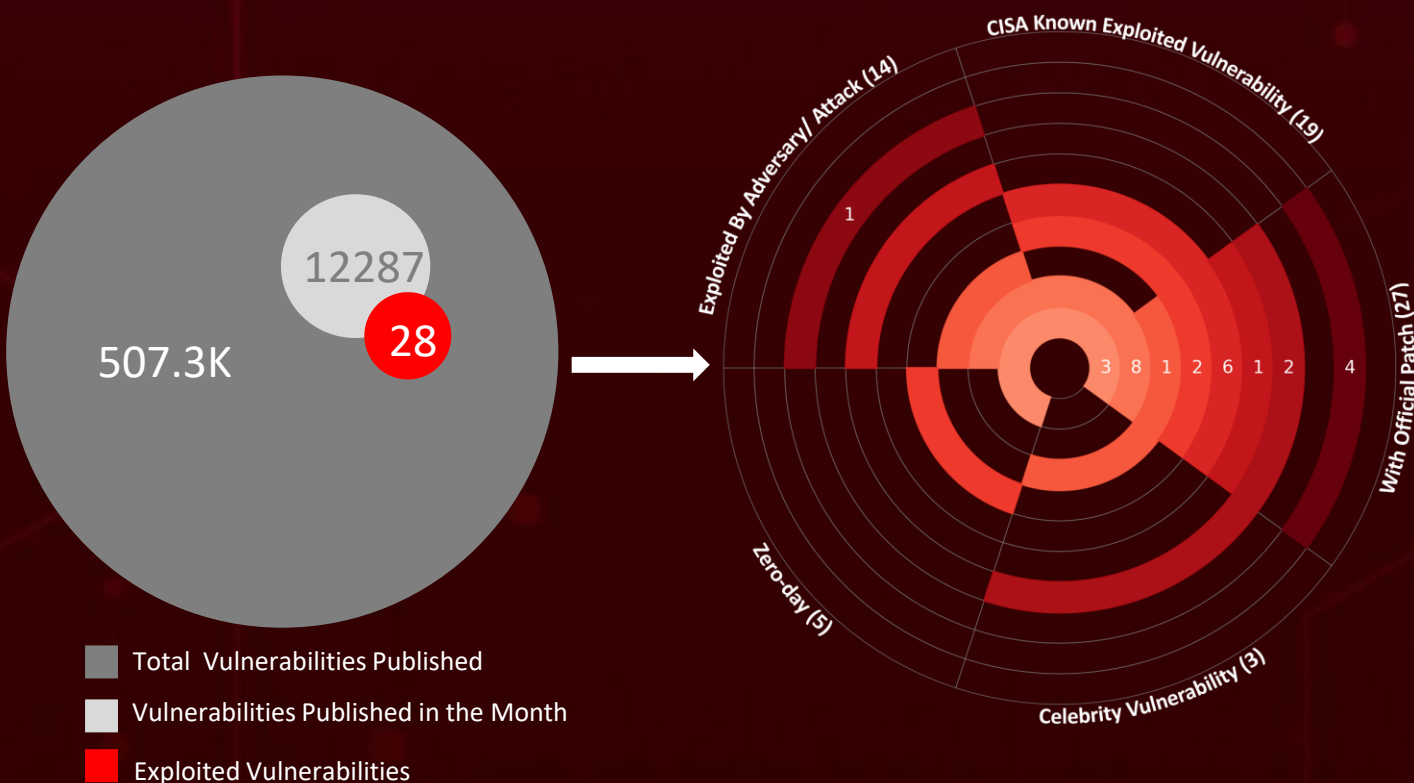
Summary

August reshaped the cybersecurity landscape with active exploitation of **5** zero-days. A rising cyber-espionage threat is gaining attention: **CI0p-linked operators** are hitting internet-facing PTC Windchill and FlexPLM servers, chaining a pre-auth FlexPLM WSDL disclosure with a Windchill login servlet flaw (**CVE-2026-12569**) for unauthenticated RCE. They then drop hex-named JSP web shells and stage engineering data for extortion.

The same hunger for quiet access drives the espionage side, only the payoff is intelligence. **Mirage Kitten**, an Iranian group also tracked as UNC1549, Smoke Sandstorm, and Nimbus Manticore, has fielded three undocumented families: the **NightLedger** backdoor plus WebSocket tunnelers **BridgeHead** and **ArcBridge**, aimed at the **Middle East, Africa, and South Asia**.

Rails has patched **CVE-2026-66066**, dubbed **KindaRails2Shell**, a critical Active Storage flaw that leaves unsafe libvips loaders on by default, so apps are vulnerable simply because nobody chose otherwise.

Head Mare weaponises trust instead. It chains **two flaws in unpatched TrueConf** servers for SYSTEM-level code execution, plants a web shell, swaps the TrueConf Client installer for a trojanized build carrying **PhantomCore**, then adds **PhantomGraph**, which hides its C2 traffic inside Microsoft OneDrive. With these increasing risks, strengthening defensive measures is more critical than ever in today's digital landscape.



In August 2026, a geopolitical cybersecurity landscape unfolds, revealing **India, Spain, Germany, Brazil, and Russia** as the top-targeted countries

Highlighted in **August 2026** is a cyber battleground encompassing the **Government, Education, Healthcare, Finance** and **Manufacturing** sectors, designating them as the top industries

ChainDrop: The npm Worm That Turned Stolen Tokens Into Fuel

Payroll Pirates: AiTM Phishing Campaign Targeting Microsoft 365 Finance Mailboxes

Killing EDR From the Kernel: Inside the DeadLock Ransomware Playbook

Fake Afghan Telecom VPN and Spoofed NIC Portal Deliver Espionage Implants

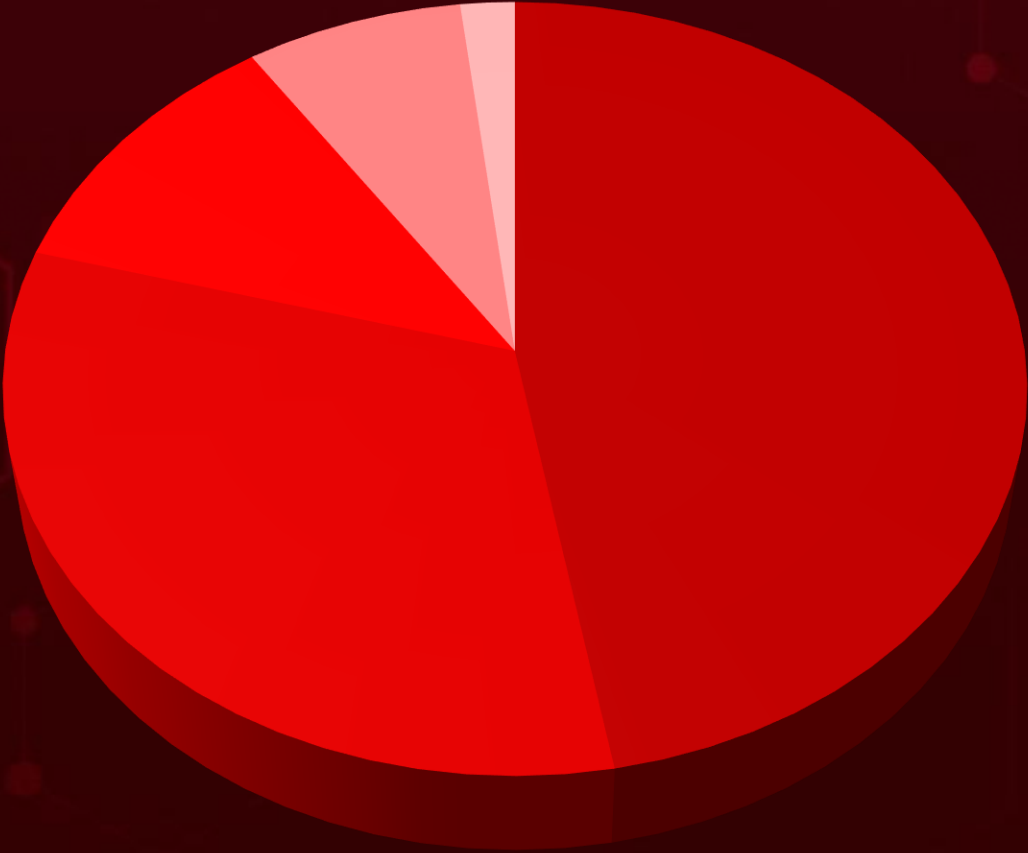
Gunra: Conti's Bloodline Returns as Ransomware-as-a-Service

StopAndProtect Hijacks Nearly 2,000 WordPress Sites for Malware Delivery and C2

Patched, Not Fixed: N-central Bypass Returns as CVE-2026-18577

Lazarus Revives Operation Dream Job Against Defense and Aerospace Targets

Threat Distribution



- Malware Attacks
- Social Engineering
- Injection Attacks
- Supply Chain Attacks
- Denial-of-Service Attack



Celebrity Vulnerabilities

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-64638</u>	XSS2Shell	WordPress Core 4.7.0 through 7.0.2, all branches; before 7.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:wordpress:*.~*~*~*~*~*~*	-
XSS2Shell (WordPress Core Pre-Auth Reflected Cross-Site Scripting Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application, T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1211: Exploitation for Defense Evasion, T1528: Steal Application Access Token	https://wordpress.org/news/2026/08/wordpress-7-0-3-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-6387</u>	regreSSHion	OpenSSH server	APT36
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:openssh:openssh:*.*.*:*.*.*.*	PATCHCORD SHEETCORD HACKERAI C2 Agent
regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362, CWE-364	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-18577	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central (Before 2026.3.1.7)			
CVE-2026-18556	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central (Before 2026.2)			
CVE-2026-66066	KindaRails2Shell (Ruby on Rails Active Storage Arbitrary File Read Vulnerability)	Ruby on Rails Active Storage			
CVE-2026-63077	JetBrains TeamCity Deserialization of Untrusted Data Vulnerability	JetBrains TeamCity On-Premises			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-64638	XSS2Shell (WordPress Core Pre-Auth Reflected Cross-Site Scripting Vulnerability)	WordPress Core			
CVE-2026-68820	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Windows Server, Windows 10- 11 26H1			
CVE-2026-62832	Windows User Profile Service Elevation of Privilege Vulnerability	Windows Server, Windows 10 - 11 26H1			
CVE-2026-72971	Windows Container Isolation FS Filter Driver (unionfs.sys) Tampering Vulnerability	Windows 11 26H1			
CVE-2025-49113	RoundCube Webmail Deserialization of Untrusted Data Vulnerability	Roundcube Webmail			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-51324	Baidu Antivirus Improper Privilege Management Arbitrary Process Termination Vulnerability	BdApiUtil driver of Baidu Antivirus			
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	FortiOS, FortiProxy			
CVE-2025-24472	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	FortiOS, FortiProxy			
CVE-2024-6387	regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)	OpenSSH server			
CVE-2026-12569	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	PTC Windchill PDMLink and FlexPLM			
CVE-2026-65400	Apple macOS Improper Authentication Vulnerability	Apple macOS Sonoma, macOS Sequoia, macOS Tahoe			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-64849	MLflow Server-Side Request Forgery Vulnerability	MLflow			
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect			
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS			
CVE-2025-10035	FortiClient EMSFortra GoAnywhere MFT Vulnerability Deserialization of Untrusted Data	FortiClient EMSFortra GoAnywhere MFT			
CVE-2026-1731	SQL Injection BeyondTrust Remote Support (RS) and Privileged BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-59310	Broadcom VMware vCenter Path Traversal Vulnerability	VMware vCenter, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure			
CVE-2026-59309	Broadcom VMware vCenter Authentication Bypass Vulnerability	VMware vCenter, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure			
CVE-2026-21962	Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in Improper Access Control Vulnerability	Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server; WebLogic Server Proxy Plug-in for Microsoft IIS			
CVE-2026-60004	Gitea Code Injection Vulnerability	Gitea			
CVE-2026-75604	Vercel Next.js Windows-Hosted Remote Code Execution Vulnerability	Vercel Next.js			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-36425	OPSWAT AppRemover Arbitrary Process Termination Vulnerability	OPSWAT AppRemover			
CVE-2026-82078	PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability	PaperCut NG and PaperCut MF			
CVE-2026-81578	PaperCut NG and PaperCut MF Authentication Bypass Vulnerability	PaperCut NG and PaperCut MF			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
NightLedger	Backdoor	-	Remote access, Data exfiltration	-	-
BridgeHead	Tunneling tool	-	Network pivoting, Traffic relay, Perimeter bypass	-	-
ArcBridge	Tunneling tool	-	Network pivoting, Traffic relay, Perimeter bypass	-	-
ChainDrop	worm	-	Credential theft, supply chain compromise	-	Malicious npm preinstall hook
FDMP	Backdoor	-	System Compromise	-	Through a compromised version of QuickFox
XCSSET	Modular	-	Information theft, Defenses disabled	-	Supply chain compromise (Xcode projects)
PhantomCore	Backdoor	-	System Compromise	-	Unpatched TrueConf video conferencing servers

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PhantomGraph	Backdoor	-	System Compromise	-	Unpatched TrueConf video conferencing servers
Troy	Backdoor	CVE-2026-68820 CVE-2025-49113	System Compromise		Phishing, Exploiting Vulnerability
FudModule	Rootkit	CVE-2026-68820 CVE-2025-49113	System Compromise		Phishing, Exploiting Vulnerability
RelayShell	Webshell	CVE-2026-68820 CVE-2025-49113	System Compromise		Phishing, Exploiting Vulnerability
MISTPEN	Downloader	CVE-2026-68820 CVE-2025-49113	Loads additional payload		Phishing, Exploiting Vulnerability
ForestTiger	Backdoor	CVE-2026-68820 CVE-2025-49113	System Compromise		Phishing, Exploiting Vulnerability
DeadLock	Ransomware	CVE-2024-51324	Data stolen, Backups disabled, Operations halted		Stolen Credentials
Gunra	Ransomware	CVE-2024-55591, CVE-2025-24472	Data encryption, extortion		Exploiting vulnerabilities
PATCHCORD	Backdoor	CVE-2024-6387	System Compromise		Phishing
SHEETCORD	Backdoor	CVE-2024-6387	System Compromise		Phishing
HACKERAI C2 Agent	Framework	CVE-2024-6387	System Compromise, persistence		Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
CoolClient	Backdoor	-	System Compromise	-	Through PlugX infection
PlugX	RAT	-	Keylogging, screen capture, system compromise	-	-
Monero	Cryptomine r	CVE-2026-65400	Data Theft		Exploiting Vulnerability
Antino	Backdoor	-	Remote access, Persistent foothold, Credential theft	-	Trojanized Installers
ClientKing	Backdoor	-	Remote access, Persistent foothold, Credential theft	-	-
XG-Web	Framework	-	Data exfiltration, Command execution	-	-
SilentDataCollector	Stealer	-	Steal Data	-	ClickFix
NetworkShareScanner	Worm	-	System disruption	-	ClickFix
SilentEncryptor	Ransomware	-	Encrypt Data, Data theft	-	ClickFix
Medusa	Ransomware	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731	Encryption, data theft/extortion		Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Babuk-derived ESXi ransomware	Ransomware	CVE-2026-59310	Data encryption, Service disruption, Log destruction		Exploiting Vulnerability
Grandoreiro	Banking Trojan	-	Banking fraud, System profiling, Payload delivery	-	Phishing
C2Looper	Backdoor	-	Foothold, recon, payload delivery	-	ClickFix chain
SynkLoader	Loader	-	Data theft	-	Phishing
QUICAgent	Backdoor	-	Remote exec, espionage	-	-
WeedHack	MaaS	-	remote-access	-	-
GoCaracal	RAT	-	Data theft, keylogging, RDP, SOCKS5	-	Phishing
Bandook	RAT	-	File theft, credential theft, keylogging	-	Phishing
Delphi loader	Loader	-	Payload delivery	-	-
SparkRAT	RAT	CVE-2026-36425	System Compromise		Phishing

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Mirage Kitten	Information theft and espionage	Iran	-	NightLedger, BridgeHead, ArcBridge	Windows
Head Mare	Information Theft, Espionage, Financial Gain	-	-	PhantomCore, PhantomGraph	TrueConf Server, TrueConf Client
Payroll Pirates	Financial Gains	-	-	-	Microsoft 365, Microsoft Outlook, Microsoft Graph API, Microsoft Entra ID
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2026-68820 CVE-2025-49113	Troy, FudModule, RelayShell, MISTPEN, ForestTiger	Microsoft Windows, Roundcube Webmail
APT36	Information theft and espionage	Pakistan	CVE-2024-6387	PATCHCORD, SHEETCORD, HACKERAI C2 Agent	OpenSSH server

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
HoneyMyte	Information theft and espionage	China	-	CoolClient , PlugX	Microsoft Windows
Jewelbug	Espionage and Financial Gains	China	-	Antino, ClientKing , XG-Web	Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers
Storm-1175	Espionage and Financial Gains	-	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731	Medusa ransomware	Windows and Linux
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	Medusa ransomware	Windows and Linux
Dark Caracal	Espionage and Information Theft	Lebanon	-	GoCaracal , Bandoock, Delphi loader	Windows



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	RMM / IT management platform (server)	N-able N-central (Before 2026.3.1.7, 2026.2)
	Web framework component / library	Ruby on Rails Active Storage, all versions before 7.2.3.2; version 8.0 and later, before 8.0.5.1; and version 8.1 and later, before 8.1.3.1.
 JETBRAINS	CI/CD build server (DevOps)	JetBrains TeamCity On-Premises (all versions before 2025.11.7 and before 2026.1.3)
	CMS / web application	WordPress Core 4.7.0 through 7.0.2, all branches; before 7.0.3
 Microsoft	Operating system	Windows Server 2012, 2016, 2019, 2022, 2025, Windows Server 2022, 2025, Windows 11 26H1, Windows 10- 11 26H1, Windows 10 - 11 26H1
	Webmail application	Roundcube Webmail before 1.5.10 and 1.6.x before 1.6.11
	Endpoint security - kernel-mode driver component	BdApiUtil driver of Baidu Antivirus v5.2.3.116083
	Network security OS (firewall) / secure web proxy	FortiOS 7.0.0 - 7.0.16; FortiProxy 7.0.0 - 7.0.19, 7.2.0 - 7.2.12
	Endpoint security management server	Fortinet FortiClient EMS

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Managed file transfer (MFT) server	Fortra GoAnywhere MFT
	Remote access service / network daemon	OpenSSH server
	PLM enterprise application	PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030
	Operating system	Apple macOS Sonoma (Before 14.8.9), macOS Sequoia (Before 15.7.9), macOS Tahoe (Before 26.6.1)
	MLOps platform / web application	MLflow (Before 3.15.0)
	Remote support / remote access software	ConnectWise ScreenConnect
	Privileged access management / remote support appliance	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)
	Virtualization management / cloud infrastructure platform	VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Web server / middleware plug-in	Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for Microsoft IIS (12.2.1.4.0)
	Git repository hosting server (DevOps)	Gitea (1.17 through 1.27.0, before 1.27.1)
	Web application framework (JavaScript/React)	Vercel Next.js (≥ 13.4 and $< 15.5.24$; ≥ 16.0 and $< 16.3.3$) on Windows filesystem hosts using Pages Router and App Router without Cache Components
	Endpoint utility - kernel-mode driver component	OPSWAT AppRemover (ardrv.sys)
	Print management server/application	All versions of PaperCut NG and PaperCut MF

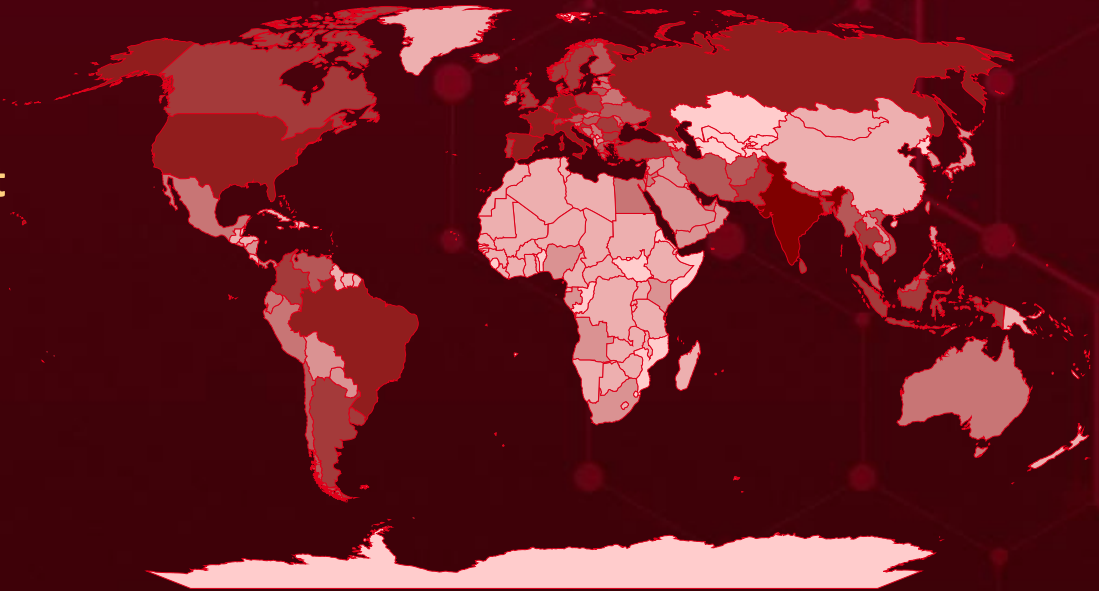


Targeted Countries

Most



Least



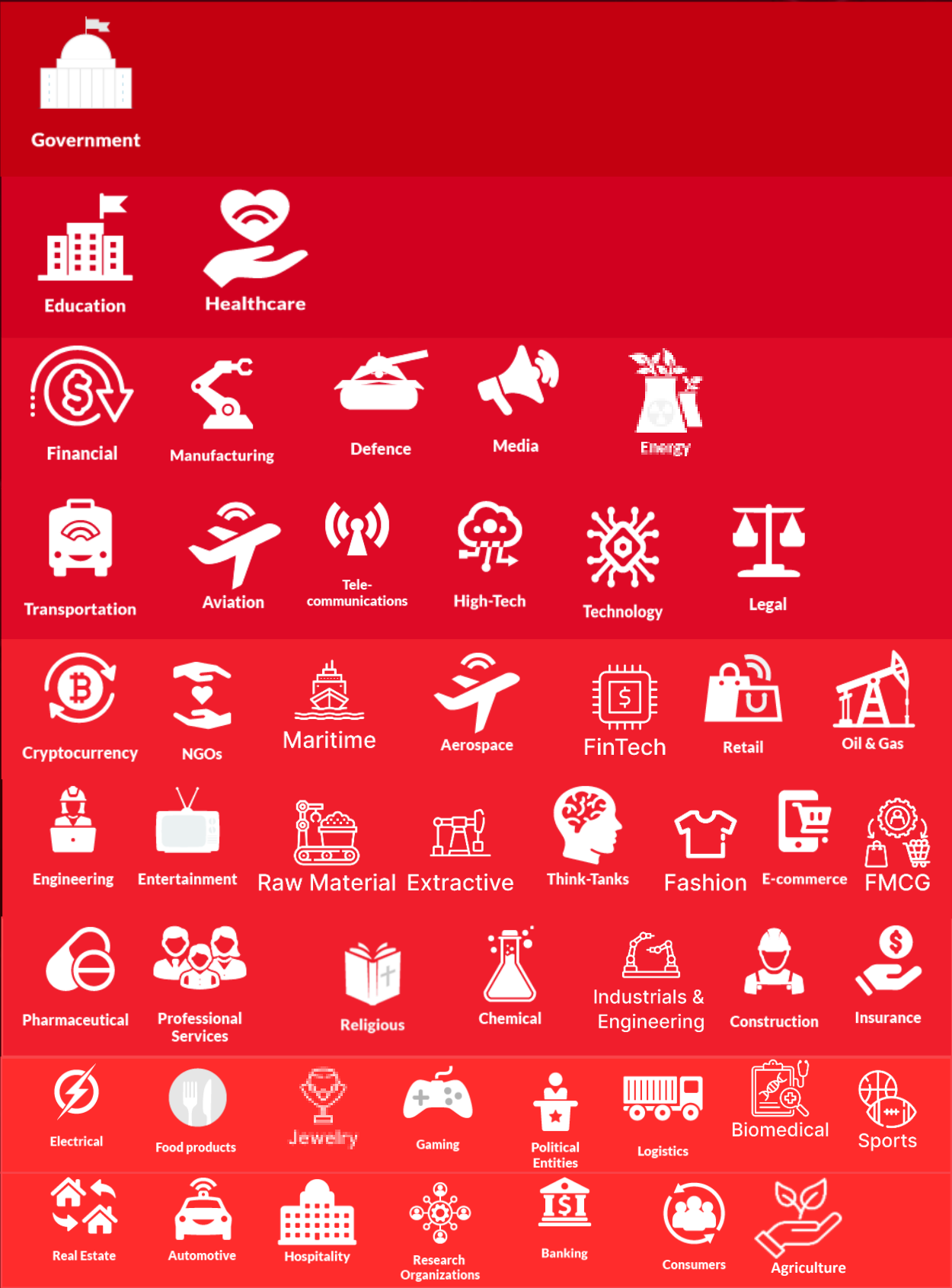
Powered by Bing

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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	India		Bulgaria		Myanmar		Moldova		Bahrain
	Spain		United Kingdom		Afghanistan		San Marino		Kenya
	Germany		Sweden		Lithuania		Monaco		Saudi Arabia
	Brazil		Netherlands		Belarus		Serbia		Syria
	Russia		Thailand		United Arab Emirates		Cambodia		Albania
	Czech Republic		Norway		Taiwan		Bosnia and Herzegovina		North Macedonia
	United States		Pakistan		Ecuador		Australia		Iraq
	France		Canada		Iceland		Slovakia		Kuwait
	Italy		Belgium		Egypt		Liechtenstein		Brunei
	Singapore		Hungary		Andorra		Akrotiri and Dhekelia		Laos
	Poland		Nepal		Panama		Oman		Gabon
	Switzerland		Finland		Mexico		Nigeria		Angola
	Colombia		Bhutan		Peru		Hong Kong		South Africa
	Romania		Iran		Montenegro		Paraguay		Holy See
	Croatia		Chile		Israel		Qatar		South Korea
	Sri Lanka		Austria		Slovenia		Nicaragua		Yemen
	Denmark		Greece		Luxembourg		Bahamas		Japan
	Turkey		Venezuela		Republic of Ireland		Timor-Leste		Lebanon
	Bangladesh		Ukraine		Cyprus		Bolivia		Tunisia
	Portugal		Vietnam		Jordan		Palestine		Senegal
	Indonesia		Malaysia		Malta		El Salvador		Zimbabwe
	Argentina		Maldives		Latvia		Philippines		Cuba
	Uruguay								Suriname

Targeted Industries

Most



Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1071

Application Layer Protocol

T1036

Masquerading

T1027

Obfuscated Files or Information

T1071.001

Web Protocols

T1190

Exploit Public-Facing Application

T1082

System Information Discovery

T1204

User Execution

T1566

Phishing

T1036.005

Match Legitimate Name or Location

T1070

Indicator Removal

T1057

Process Discovery

T1083

File and Directory Discovery

T1041

Exfiltration Over C2 Channel

T1105

Ingress Tool Transfer

T1140

Deobfuscate/Decode Files or Information

T1204.002

Malicious File

T1574

Hijack Execution Flow

T1005

Data from Local System

T1102

Web Service

T1583

Acquire Infrastructure

T1059.003

Windows Command Shell

T1033

System Owner/User Discovery

T1562.001

Disable or Modify Tools

T1588

Obtain Capabilities



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>ChainDrop</u>	SHA256	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2ca a93012b 350668 fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda 806e56 84b1eb 9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367c fc2509c f1bcc
<u>FDMTTP</u>	SHA256	795594ad5e6f2868cc4d8ed12dabf4f3999a1477c6b250527c5 ede9a98528fb9
<u>PhantomCore</u>	MD5	c5a460e4e68a088f6e51b2c6474642ec 129462164a7d52e9ea8560b60f0412c5 ec0bf4a2186a88874e9f26f07cfeb532 b348642146ea34771e5785c5857950f5 c915cb6c2aeb863ee8479238e1644217 0e79996d9483d1e44fea32b0a48c2c19 2bb75c20e778eb5c416965bd4d4259b1 b3a6fee3307f1c26841fd5c603e2b013 8fcc3e4ccbf1725d9989fb464abf3561
	SHA256	b9e4052b310f9451eca9784a4a33bf5282d1bd07e3359eba96 48be625e2e40dd
<u>PhantomGraph</u>	MD5	489f43be558b2679284ceabed7adc4f3 dd1fd2b459b97b7d59375cb8383cd19a 0e4541c3153ec5ed01497f19cf4f63d0
<u>PlugX</u>	SHA256	d9529976ce67da55a0f1a561ff4fb7e6535bfc7b607c8381827 52fd6e6732794 64b9f35206cb8ad0b79a07dad35acf024d2d429855352674f3f ecc0798b96cfd 1f8a2658aeabcfecfee2fe37978ccbcddfee8045e23ed5f069b4c 1743acad4ccd ce44171fbacb22d86c61f4c4c47ffb0fca380c96dd1894522ee4 65e39d72dcec dc4558efd0113791cbccc363a89a71b3170b71b82065b464a9 1832488e792ee3
<u>Monero</u>	SHA256	657fe4474fd1788c2910fb3fc4e2e8ed85ea4598638c4b38811 bbbf4090a3999

Attack Name	TYPE	VALUE
<u>Monero</u>	SHA256	4f4e99c6e30bc5ce997aa398ab131ecc3e969eb78211de93d3 2174575e4d998e 459655bcc84a8239a65300ea61fd44a16f4a7df3cbf011a6756 46560c2cc0d5d c20e89caf440d8b3b9b1da8c9467ab6aaea9a17a79a2169f89f 07b1a603cb422 66871e7a931ce86c90fc19cacb47a91fd fba9d3d21436965749 7ced2a77f2f4f c05a6dfee8a914f64c75dfb4fa2bae9e8aa8214b5921faa1b3c2 75c7a3b79be6 8bf1ae207338b8cd2f3ec202cef0285d09041f94ebdd5ae6c2e dfe8ad59f06b1 60033b1bda21c6d2a70d7e3829d76a44fdc45087ba27b0e6fe 01b54f0c968180
<u>Antino</u>	SHA256	09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e 9105107e5cff c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a7 1d71d71e42cc 153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0 dc22d3bb5c94e
<u>Medusa</u>	Email	key[.]medusa[.]serviceteam[@]protonmail[.]com medusa[.]support[@]onionmail[.]org mds[.]svt[.]breach[@]protonmail[.]com mds[.]svt[.]mir2[@]protonmail[.]com MedusaSupport[@]cock[.]li
	SHA256	0cefeb6210b7103fd32b996beff518c9b6e1691a97bb1cda7f5f b57905c4be96 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a 610354d672523c e57ba1a4e323094ca9d747bfb3304bd12f3ea3be5e2ee785a3 e656c3ab1e8086 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044 a68fff8496d19 56b08aa03bd8c0ea094cfefb03d5954ffd857bac42df929dc835 eea62f32b09e0 a5a3c3c4fbf5c7db808176db3242c2106995c85f8ba987472ea 0e92e59503b55 d3abd4bae082d4c9918447fe82c521567cc7f9b0e5f2d55999a 6e5c40fa7fd54 7ffce7f6d7262f214d78e6b7fd8d07119835cba4b04ce334260 665d7c8fb369a b29defbbc4ebaa243c1712ccc4943374f1b6fb864c39ed9f70fc eb17eee098db 04b13b6cd5e5291b1cde78975a140feea7fd3bc3777c53caa1a b33426c83bfcc



Vulnerabilities Exploited

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

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-68820</u>		Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10-11 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-62832</u>		Windows Server 2022, 2025, Windows 10 - 11 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Windows User Profile Service Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62832

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-72971</u>		Windows 11 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Windows Container Isolation FS Filter Driver (unionfs.sys) Tampering Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72971

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-49113</u>		Roundcube Webmail 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-2024-51324</u>		BdApiUtil driver of Baidu Antivirus v5.2.3.116083	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:baidu:baidu_antivirus:*.~*~*~*~*~*~*	-
Baidu Antivirus Improper Privilege Management Arbitrary Process Termination Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1588: Obtain Capabilities, T1105: Ingress Tool Transfer, T1036: Masquerading, T1068: Exploitation for Privilege Escalation	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-55591</u>		FortiOS 7.0.0 - 7.0.16; FortiProxy 7.0.0 - 7.0.19, 7.2.0 - 7.2.12	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*	-
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts , T1068 : Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-24472</u>		FortiOS 7.0.0 - 7.0.16; FortiProxy 7.0.0 - 7.0.19, 7.2.0 - 7.2.12	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*	-
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts , T1068 : Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

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 LINKS
	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-2026-65400</u>		Apple macOS Sonoma (Before 14.8.9), macOS Sequoia (Before 15.7.9), macOS Tahoe (Before 26.6.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*	-
Apple macOS Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1496: Resource Hijacking	https://support.apple.com/en-us/148170 , https://support.apple.com/en-us/148171 , https://support.apple.com/en-us/148172

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-64849</u>		MLflow (Before 3.15.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:mlflow:mlflow:*:*:*:*:*:*:*	-
MLflow Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://github.com/mlflow/mlflow/releases/tag/v3.15.0 , https://github.com/mlflow/mlflow/releases/tag/v3.15.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-1709</u>		ConnectWise ScreenConnect	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:connectwise:screenco nnect:*:*:*:*:*:*:*	-
ConnectWise ScreenConnect Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1072: Software Deployment Tools	https://www.screencnect.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-48788</u>		Fortinet FortiClient EMS	-
	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, T1505.003: Web Shell, T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-10035</u>		Fortra GoAnywhere MFT	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*	-
Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77, CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.fortra.com/security/advisories/product-security/fi-2025-012

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-1731</u>		BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*	-
BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Web Shell	https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-59310</u>		VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Broadcom VMware vCenter Path Traversal Vulnerability		cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1053: Scheduled Task/Job, T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-59309</u>		VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Broadcom VMware vCenter Authentication Bypass Vulnerability		cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-303	T1595: Active Scanning, T1136: Create Account, T1036: Masquerading	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-21962</u>		Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for Microsoft IIS (12.2.1.4.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:oracle:http_server:*:*:*:*:* ; cpe:2.3:a:oracle:weblogic_server_proxy_plug-in:*:*:*:*:*	-
Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpujan2026.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-60004</u>		Gitea (1.17 through 1.27.0, before 1.27.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitea:gitea:*:*:*:*:*:*:*:*	-
Gitea Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://blog.gitea.com/release-of-1.27.1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-75604</u>		Vercel Next.js (>= 13.4 and < 15.5.24; >= 16.0 and < 16.3.3) on Windows filesystem hosts using Pages Router and App Router without Cache Components	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:*	-
Vercel Next.js Windows-Hosted Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://nextjs.org/blog/august-2026-security-release

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-36425</u>		OPSWAT AppRemover (ardrv.sys)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:opswat:appremoverdriver:*:*:*:*:*:*	-
OPSWAT AppRemover Arbitrary Process Termination Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://www.opswat.com/products/oesis-framework/application-removal

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

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

Attacks Executed

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

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

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

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

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

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

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

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

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

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

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>PhantomCore</u>	PhantomCore is a backdoor used by the hacktivist group Head Mare, active since 2023 and known for consistently targeting Russia. It gathers information about the victim, including their public IP address, to build a detailed picture of the target before deploying its final-stage payload or running additional commands on the compromised system.	Unpatched TrueConf video conferencing servers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	TrueConf Server, TrueConf Client
ASSOCIATED ACTOR			PATCH LINK
Head Mare			-

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
PhantomGraph	PhantomGraph is a backdoor made up of two modules. The first, SysExcSvc.dll, receives commands from the attackers and sends back the results, using a Microsoft OneDrive account as its command-and-control (C2) server. The second, SysReadSvc.dll, reads the command passed along by the first module, executes it, and saves the result.	Unpatched TrueConf video conferencing servers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	TrueConf Server, TrueConf Client
ASSOCIATED ACTOR			PATCH LINK
Head Mare			-

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>Troy</u>	Troy backdoor is a newly identified modular remote access trojan in Lazarus' arsenal. Delivered as a 64-bit DLL, it supports 17 operator commands, giving attackers a broad range of remote access and post-exploitation capabilities. Troy is configured with three command-and-control (C2) servers, each with its own URL and port. At startup, it works through them in order, parsing each URL into its host and path, opening an HTTP connection, and sending a connection request, then validates the response against the string CONNECTED and sticks with the first server that answers successfully.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , 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>FudModule</u>	FudModule is an advanced rootkit developed by the North Korean threat actor group. It's built to gain admin-to-kernel access on Windows systems, letting attackers read and write arbitrary kernel memory. With that access, FudModule can disable a range of security monitoring features, modifying kernel variables and removing kernel callbacks, to blind products like EDRs, firewalls, and antimalware tools.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Rootkit		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , 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
RelayShell	RelayShell is a previously undocumented PHP web shell that the threat actor deployed after compromising a web server. Unlike a traditional web shell that runs commands directly, RelayShell mainly acts as a communication relay between the attacker and an infected endpoint. It operates in two distinct modes, which we call Victim mode and Operator mode, chosen based on the password supplied in the HTTP POST request.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Webshell		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , 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>MISTPEN</u>	MISTPEN is a lightweight, in-memory downloader that uses the Microsoft Graph API to reach attacker-controlled files hosted on OneDrive and pull down additional payloads. Every file exchanged through OneDrive is encrypted with AES, using separate keys for uploads and downloads. Its core capability is reflectively loading PE DLL files straight into memory, letting attackers deploy more payloads without ever touching disk. Before delivering the final backdoor, MISTPEN often runs several in-memory modules built for specific tasks; these modules have no network communication of their own, they simply do their job and hand the results back to MISTPEN, which then uploads the data to the C2.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Downloader		Loads additional payload	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , 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>ForestTiger</u>	ForestTiger is a well-documented backdoor widely attributed to the Lazarus threat group. Once deployed, it gives attackers long-term remote access to the compromised host. Its command-and-control (C2) infrastructure has historically relied mainly on compromised servers running WordPress and SharePoint, though in more recent campaigns the threat actor appears to have shifted toward using compromised Roundcube webmail servers as C2.	Phishing, Exploiting Vulnerability	CVE-2026-68820 CVE-2025-49113
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows, Roundcube Webmail
ASSOCIATED ACTOR			PATCH LINKS
Lazarus			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820 , 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>DeadLock</u>	DeadLock is a financially motivated, human-operated ransomware operation active since mid-2025 that combines double extortion with a decentralized back end. They load a legitimate Baidu antivirus driver with a known flaw (CVE-2024-51324) and use it to kill EDR from the kernel, turning a security product into the weapon that blinds the rest.	Stolen Credentials	CVE-2024-51324
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data stolen, Backups disabled, Operations halted	Baidu Antivirus
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Gunra</u>	Gunra is a Conti-derived ransomware-as-a-service, active since April 2025, now running a formal affiliate program under the alias "Golden Community." Uses double extortion with a multi-threaded ChaCha20 + RSA-4096 locker against Windows and Linux.	Exploiting vulnerabilities	CVE-2024-55591 CVE-2025-24472
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, extortion	Fortinet FortiOS, FortiProxy
ASSOCIATED ACTOR			PATCH LINK
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535

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>PATCHCORD</u>	PATCHCORD is a compiled C/C++ backdoor delivered through sector-specific lures, including fake VPN installers impersonating Afghan Telecom (AFTEL) and telecom management tools. It abuses Google Sheets for its command-and-control (C2) communication and has been actively distributed through a domain impersonating India's National Informatics Centre (NIC). Once running, PATCHCORD hides its console window, sets up persistence by hijacking browser shortcuts, fingerprints the host, registers with its C2 server, and then enters its main tasking loop.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SHEETCORD</u>	SHEETCORD is a Go-based backdoor that blends functionality from the earlier SHEETCREEP RAT with several capabilities introduced in PATCHCORD, suggesting the operator's tooling is evolving. Like PATCHCORD, it can run remote commands (via <code>main.executeShellCommand</code>) and includes a <code>main.getHostInfo</code> function that works much like PATCHCORD's registration payload builder, collecting the victim's hostname for the initial check-in. Notably, the Go variant gathers far less system information than PATCHCORD's detailed fingerprinting, which pulled hostname, username, process details, and OS version.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>HACKERAI</u> <u>C2 Agent</u>	HACKERAI C2 Agent is a previously undocumented malware framework that shares several capabilities with PATCHCORD and SHEETCORD, including system fingerprinting, remote command execution, and browser shortcut hijacking for persistence.	Phishing	CVE-2024-6387
TYPE		IMPACT	AFFECTED PLATFORM
Framework		System Compromise, persistence	OpenSSH server
ASSOCIATED ACTOR			PATCH LINKS
APT36			https://www.openssh.org/txt/release-9.8 , https://www.openssh.org/releasesnotes.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CoolClient	CoolClient is a backdoor family attributed to the HoneyMyte APT group, and it has kept evolving over time. A 2025 variant added clipboard theft and HTTP traffic interception for harvesting credentials. The newest version can deploy a signed kernel-mode driver as a Windows service and talk to it through IOCTL requests. That driver boosts the malware's stealth by hiding the CoolClient process and shielding its files and registry entries from inspection or modification. The overall design resembles the kernel-mode enhancements previously seen in ToneShell, but the CoolClient driver adds dedicated IOCTL handlers that let the user-mode backdoor communicate directly with the driver.	Through PlugX infection	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
HoneyMyte			-

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
PlugX	PlugX is a remote access trojan (RAT) that has been around since 2008, used as a backdoor to take full control of a victim's machine. Once a device is infected, the attacker can remotely run a wide range of commands, pulling machine information, capturing the screen, sending keyboard and mouse events, keylogging, rebooting the system, managing processes (creating, killing, and listing them), managing services (create, start, stop, and so on), editing Windows registry entries, opening a shell, and more. It also records its own activity in a text log file.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Keylogging, screen capture, system compromise	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
HoneyMyte			-

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>Monero</u>	Monero, a privacy- focused cryptocurrency, has become a magnet for cryptominers, both legitimate and malicious. The lure lies in its unique mining algorithm, RandomX, designed to be resistant to specialized hardware (ASICs) and favor consumer-grade CPUs and GPUs.	Exploiting Vulnerability	CVE-2026-65400
TYPE		IMPACT	AFFECTED PLATFORM
Cryptominer		Data Theft	Apple macOS Sonoma, macOS Sequoia, macOS Tahoe
ASSOCIATED ACTOR			PATCH LINKS
-			https://support.apple.com/en-us/148170 , https://support.apple.com/en-us/148171 , https://support.apple.com/en-us/148172

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
Antino	Antino is the group's Windows backdoor. It is the payload dropped by a wave of malicious HTML Application (HTA) downloaders that use current geopolitical events as lures, the activity that prompted this investigation. Antino is also delivered as a fake Adobe Flash or Adobe installer, using file names such as flashcenter_pp_ax_install_en.exe and Adobeinstall.exe, downloaded from domains the group controls.	Trojanized Installers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Persistent foothold, Credential theft	Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-

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
ClientKing	ClientKing is a Rust-based backdoor/implant, bundled with a kernel-mode rootkit and a credential-stealing authentication module. Unlike the browser tooling, ClientKing targets servers and network devices. It supports five command-and-control (C&C) transports, one of which is a custom DNS tunnel. It gives the operator a full interactive shell, SOCKS pivoting, and the ability to load kernel modules straight from memory.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Persistent foothold, Credential theft	Linux, x86-64 servers, ARM64 devices
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-

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>XG-Web</u>	XG-Web is the single control panel behind Jewelbug's espionage and cryptocurrency-fraud operations. It is built as a React front end over a Node.js backend, with a MySQL database that doubles as the rendezvous point for victim implants. Its developers describe it in their own documentation as a "penetration-testing platform," but internal function names include browser hijacking, data theft, and a man-in-the-middle attack. The framework turns a victim's browser into a full remote-control channel and reaches from there into the host and the internal network behind it.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Framework		Data exfiltration, Command execution	Windows, Google Chrome, Mozilla Firefox
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-

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
SilentDataCollector	SilentDataCollector is a stealer that builds a list of every file across all drives, fixed, removable, and network, then encrypts that list and sends it to the base command-and-control (C&C) server. The operator can steer file collection by uploading a command file to the C&C, which the stealer reads before compressing, encrypting, and exfiltrating the requested files back to the same server.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Steal Data	Windows, WordPress
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
NetworkShareScanner	NetworkShareScanner acts as an SMB/USB worm, enumerating network shares and plugged-in USB devices to spread beyond the machine it first infected.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Worm		System disruption	Windows, WordPress
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
SilentEncryptor	SilentEncryptor is the ransomware component. It downloads a command file from the base C&C that tells it whether to encrypt every infected computer or only those with specific hostnames, and it also carries the ransom message shown to the victim. Its key derivation function combines a per-file password with the machine name to produce a 32-byte key, and since both the per-file password and machine name are embedded in the encrypted file's renamed filename, decryption of the files is possible.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Encrypt Data, Data theft	Windows, WordPress
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>Medusa</u>	Medusa is a RaaS operation (since June 2021) running double/triple-extortion against critical infrastructure, distinct from MedusaLocker. Core operation dormant since mid-Feb 2026; lead affiliate has pivoted to StormEncryptor.	Exploiting Vulnerability	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Encryption, data theft/extortion	ScreenConnect, FortiClient EMS, GoAnywhere MFT, BeyondTrust RS/PRA
ASSOCIATED ACTOR			PATCH LINKS
Storm-1175, Lazarus			https://www.screencconnect.com/download , https://fortiguard.fortinet.com/psirt/FG-IR-24-007 , https://www.fortra.com/security/advisories/product-security/fi-2025-012 , https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

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>Babuk-derived ESXi ransomware</u>	This is a Babuk-derived ESXi encryptor deployed as the final stage of a global campaign against internet-facing VMware vCenter. After gaining root on the vCenter Server Appliance, the actor harvested vmdir machine credentials, created SSO administrator accounts, and pushed the encryptor to a datastore shared by all ESXi hosts.	Exploiting Vulnerability	CVE-2026-59310
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, Service disruption, Log destruction	VMware vCenter Server, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure
ASSOCIATED ACTOR			PATCH LINK
-			https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

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
Grandoreiro	Grandoreiro is a Brazilian-origin banking trojan written in Delphi, active across Latin America since at least 2016 against financial institutions and their customers. In this May 2026 campaign the operators abuse Duplicate Files Finder for DLL sideloading, so malicious code executes inside a trusted, signed application. The loader is lightweight in function but heavily defended: it hides the host application's GUI window, then runs extensive anti-analysis checks before ever contacting its C2 system uptime below three minutes, desktop shortcuts for a specific seven-application set, VMware and VirtualBox drivers, BIOS registry keywords, 49 blacklisted analyst and EDR process names, blacklisted usernames and hostnames, and analyst tool directories.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Banking Trojan		Banking fraud, System profiling, Payload delivery	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
C2Looper	C2Looper is a Rust-based backdoor identified in July 2026, used to establish a foothold for lateral movement in ransomware intrusions. Its v2 build adds GitHub-based C2 and shellcode injection, and abuses OneDrive DLL sideloading for stealth.	ClickFix chain	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Foothold, recon, payload delivery	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SynkLoader	SynkLoader is a loader distributed through Microsoft Teams phishing campaigns to steal credentials via a fake lock screen. It got its name from its unusual mix of programming languages, Python, PowerShell, C#, and C++, sometimes blending up to three of them in a single module. The loader ships with a long chain of attack tools that bridge these different languages, with some modules using as many as three at once.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Data theft	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
QUICAgent	QUICAgent is a custom 64-bit Go backdoor that performs sandbox evasion, then resolves its C2 via Cloudflare Workers and communicates over QUIC on UDP/443 with RC4 encryption. Deployed in Operation QUICSILVER.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote exec, espionage	Windows
ASSOCIATED ACTOR			PATCH LINK
China-nexus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
WeedHack	WeedHack is a Minecraft-focused Malware-as-a-Service (MaaS) that shows how SEO poisoning can drop malicious downloads straight into gamers' paths. It has also become a major catalyst for cyberbullying: many of its customers appear to be teenagers and young adults who use its remote access capabilities to threaten, harass, and monitor victims around their own age.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
MaaS		remote-access	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
GoCaracal	GoCaracal is a modular Go-based RAT and post-exploitation framework with lightweight and extended profiles. Its extended variant uses Ethereum smart contracts as a fallback C2-resolution mechanism.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Data theft, keylogging, RDP, SOCKS5	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Bandook	Bandook is a long-running C++ remote access trojan and Dark Caracal's signature malware. Its June 2026 variant adds anti-analysis via randomized command IDs and obfuscated plugin export names.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		File theft, credential theft, keylogging	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-

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>Delphi loader</u>	Delphi loader is an intermediate stager in the Dark Caracal chain that carries Bandook and the extended GoCaracal variant. It recurs across campaigns as an attribution artifact.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Payload delivery	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-

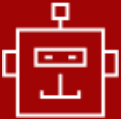
NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SparkRAT</u>	SparkRAT is an open-source, cross-platform remote access trojan written in Go and developed by XZB-1248. It runs on Windows, macOS, and Linux, and offers extensive remote access capabilities, including file and process management, file transfer, remote desktop monitoring, system information collection, and command execution through terminal access.	Phishing	CVE-2026-36425
TYPE		IMPACT	AFFECTED PLATFORM
RAT		System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			https://www.opswat.com/products/oesis-framework/application-removal

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

Adversaries in Action

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Head Mare	-	Instrumentation, Electronics, Transportation, Energy, IT, Software Development	Russia
	MOTIVE		
	Information Theft, Espionage, Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	PhantomCore, PhantomGraph	TrueConf Server, TrueConf Client
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0011: Command and Control, TA0010: Exfiltration, T1190: Exploit Public-Facing Application, T1199: Trusted Relationship, T1566: Phishing, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1505: Server Software Component, T1505.003: Web Shell, T1543: Create or Modify System Process, T1543.003: Windows Service, T1546: Event Triggered Execution, T1546.015: Component Object Model Hijacking, T1068: Exploitation for Privilege Escalation, T1027: Obfuscated Files or Information, T1036: Masquerading, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1102: Web Service, T1102.002: Bidirectional Communication, T1572: Protocol Tunneling, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Payroll Pirates</u> <u>(aka Storm-2755)</u>	-	Healthcare, Education, Manufacturing, Government, Professional Services	United States, Canada, Europe
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Microsoft 365, Microsoft Outlook, Microsoft Graph API, Microsoft Entra ID
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0006: Credential Access, TA0005: Defense Evasion, TA0011: Command and Control, TA0007: Discovery, TA0009: Collection, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.002: Spearphishing Link, T1557: Adversary-in-the-Middle, T1111: Multi-Factor Authentication Interception, T1539: Steal Web Session Cookie, T1550: Use Alternate Authentication Material, T1550.004: Web Session Cookie, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1684: Social Engineering, T1684.001: Impersonation, T1090: Proxy, T1090.002: External Proxy, T1087: Account Discovery, T1087.004: Cloud Account, T1114: Email Collection, T1114.002: Remote Email Collection			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>APT36 (aka</u> <u>Transparent</u> <u>Tribe, ProjectM,</u> <u>TEMP.Lapis,</u> <u>Mythic Leopard,</u> <u>Copper</u> <u>Fieldstone, Earth</u> <u>Karkaddan,</u> <u>STEPPY-KAVACH,</u> <u>Green Havildar,</u> <u>APT-C-56,</u> <u>Storm-0156,</u> <u>Opaque Draco)</u>	Pakistan	Defense, Aerospace, and Aviation	Europe (France, Germany), India, and South America (Brazil)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2024-6387	Troy, FudModule, RelayShell, MISTPEN, ForestTiger	OpenSSH server
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0006: Credential Access, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1566: Phishing, T1566.001: Spearphishing Attachment, T1566.002: Spearphishing Link, T1190: Exploit Public-Facing Application, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1059.001: PowerShell, T1059.005: Visual Basic, T1620: Reflective Code Loading, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1547.009: Shortcut Modification, T1564: Hide Artifacts, T1564.003: Hidden Window, T1497: Virtualization/Sandbox Evasion, T1497.001: System Checks, T1622: Debugger Evasion, T1140: Deobfuscate/Decode Information, T1057: Process Discovery, T1082: System Information Discovery, T1555: Credentials from Password Stores, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1102.002: Bidirectional Communication, T1132: Data Encoding, T1132.001: Standard Encoding, T1571: Non-Standard Port, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>HoneyMyte (aka Mustang Panda, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)</u>	China	Government	Myanmar, Mongolia, Pakistan, Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	CoolClient, PlugX	Microsoft Windows
TTPs			
TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0009: Collection, TA0007: Discovery, TA0011: Command and Control, T1569: System Services, T1569.002: Service Execution, T1106: Native API, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1543: Create or Modify System Process, T1543.003: Windows Service, T1548: Abuse Elevation Control Mechanism, T1548.002: Bypass User Account Control, T1134: Access Token Manipulation, T1134.004: Parent PID Spoofing, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1014: Rootkit, T1055: Process Injection, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1553: Subvert Trust Controls, T1553.002: Code Signing, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1112: Modify Registry, T1564: Hide Artifacts, T1070: Indicator Removal, T1070.004: File Deletion, T1056: Input Capture, T1056.001: Keylogging, T1115: Clipboard Data, T1005: Data from Local System, T1057: Process Discovery, T1082: System Information Discovery, T1071: Application Layer Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Jewelbug (Earth Alux, REF7707, CL-STA-0049, Ink Dragon)	China	Government, Military, Defense, Law Enforcement, Telecommunications, Aerospace, Industrial Manufacturing, Web Hosting Services, Cryptocurrency	Middle East, Southeast Asia, South Asia, Taiwan, United States
	MOTIVE		
	Espionage and Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Antino, ClientKing, XG-Web	Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers
TTPs			
TA0043: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1587: Develop Capabilities; T1608: Stage Capabilities; T1189: Drive-by Compromise; T1566: Phishing; T1078: Valid Accounts; T1204: User Execution; T1059: Command and Scripting Interpreter; T1176: Software Extensions; T1556: Modify Authentication Process; T1547: Boot or Logon Autostart Execution; T1112: Modify Registry; T1014: Rootkit; T1027: Obfuscated Files or Information; T1036: Masquerading; T1218: System Binary Proxy Execution; T1539: Steal Web Session Cookie; T1056: Input Capture; T1185: Browser Session Hijacking; T1217: Browser Information Discovery; T1082: System Information Discovery; T1550: Use Alternate Authentication Material; T1114: Email Collection; T1113: Screen Capture; T1115: Clipboard Data; T1557: Adversary-in-the-Middle; T1074: Data Staged; T1102: Web Service; T1071: Application Layer Protocol; T1572: Protocol Tunneling; T1090: Proxy; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1583.001: Domains; T1583.006: Web Services; T1584.004: Server; T1587.001: Malware; T1608.001: Upload Malware; T1608.004: Drive-by Target; T1608.006: SEO Poisoning; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204.001: Malicious Link; T1059.007: JavaScript; T1059.003: Windows Command Shell; T1176.001: Browser Extensions; T1556.003: Pluggable Authentication Modules; T1547.006: Kernel Modules and Extensions; T1027.013: Encrypted/Encoded File; T1036.005: Match Legitimate Resource Name or Location; T1218.005: Mshta; T1056.003: Web Portal Capture; T1550.004: Web Session Cookie; T1114.002: Remote Email Collection; T1074.002: Remote Data Staging; T1102.001: Dead Drop Resolver; T1102.002: Bidirectional Communication; T1071.001: Web Protocols; T1071.004: DNS; T1090.001: Internal Proxy			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Storm-1175</u>	-	Healthcare, education, professional services, finance, legal, insurance, technology, manufacturing	Global
	MOTIVE		
	Espionage and Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731	Medusa ransomware	Windows and Linux
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0010: Exfiltration, TA0011: Command and Control, TA0040: Impact, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1569: System Services, T1072: Software Deployment Tools, T1505: Server Software Component, T1484: Domain or Tenant Policy Modification, T1562: Impair Defenses, T1036: Masquerading, T1003: OS Credential Dumping, T1555: Credentials from Password Stores, T1046: Network Service Discovery, T1018: Remote System Discovery, T1021: Remote Services, T1570: Lateral Tool Transfer, T1105: Ingress Tool Transfer, T1572: Protocol Tunneling, T1219: Remote Access Software, T1567: Exfiltration Over Web Service, T1486: Data Encrypted for Impact, T1490: Inhibit System Recovery, T1489: Service Stop, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1569.002: Service Execution, T1505.003: Web Shell, T1484.001: Group Policy Modification, T1562.001: Disable or Modify Tools, T1003.001: LSASS Memory, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1567.002: Exfiltration to Cloud Storage			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, G0032)</u>	North Korea	Healthcare, education, professional services, finance, legal, insurance, technology, manufacturing	Global
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Medusa ransomware	Windows and Linux
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1584: Compromise Infrastructure, T1584.004: Server, T1608: Stage Capabilities, T1608.001: Upload Malware, T1608.006: SEO Poisoning, T1586: Compromise Accounts, T1586.002: Email Accounts, T1566: Phishing, T1566.003: Spearphishing via Service, T1566.001: Spearphishing Attachment, T1190: Exploit Public-Facing Application, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1505: Server Software Component, T1505.003: Web Shell, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1014: Rootkit, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1055: Process Injection, T1055.001: Dynamic-link Library Injection, T1684: Social Engineering, T1684.001: Impersonation, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, T1070: Indicator Removal, T1070.004: File Deletion, T1078: Valid Accounts, T1057: Process Discovery, T1082: System Information Discovery, T1113: Screen Capture, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Dark Caracal</u> <u>(aka ATK 27,</u> <u>TAG-CT3)</u>	Lebanon	Communications, Government, Military, Businesses, Journalists, Activists, Legal, Healthcare, Education	Venezuela, Brazil, Ecuador, Chile, Colombia, El Salvador, Uruguay
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	GoCaracal, Bandoock, Delphi loader	Windows
TTPs			
TA0042:Resource Development, T1583:Acquire Infrastructure, T1583.001:Domains, T1583.003:Virtual Private Server, T1608:Stage Capabilities, T1608.001:Upload Malware, TA0001:Initial Access, T1566:Phishing, T1566.001:Spearphishing Attachment, TA0002:Execution, T1204:User Execution, T1204.002:Malicious File, T1059:Command and Scripting Interpreter, T1059.003:Windows Command Shell, TA0003:Persistence, T1547:Boot or Logon Autostart Execution, T1547.001:Registry Run Keys / Startup Folder, TA0005:Defense Evasion, T1112:Modify Registry, T1055:Process Injection, T1027:Obfuscated Files or Information, T1140:Deobfuscate/Decode Files or Information, T1564:Hide Artifacts, T1564.001:Hidden Files and Directories, T1070:Indicator Removal, T1070.004:File Deletion, T1036:Masquerading, T1036.005:Match Legitimate Name or Location, TA0006:Credential Access, T1555:Credentials from Password Stores, T1555.003:Credentials from Web Browsers, T1539:Steal Web Session Cookie, T1056:Input Capture, T1056.001:Keylogging, TA0007:Discovery, T1082:System Information Discovery, T1057:Process Discovery, T1083:File and Directory Discovery, T1518:Software Discovery, T1518.001:Security Software Discovery, T1010:Application Window Discovery, TA0009:Collection, T1005:Data from Local System, TA0011:Command and Control, T1105:Ingress Tool Transfer, T1573:Encrypted Channel, T1573.001:Symmetric Cryptography, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1102:Web Service, T1102.001:Dead Drop Resolver, T1090:Proxy, T1090.001:Internal Proxy, T1219:Remote Access Tools, T1219.002:Remote Desktop Software, TA0010:Exfiltration, T1041:Exfiltration Over C2 Channel			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
		T1195.002: Compromise Software Supply Chain
	T1199: Trusted Relationship	
	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell

Tactic	Technique	Sub-technique
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1559: Inter-Process Communication	T1559.001: Component Object Model
	T1569: System Services	T1569.001: Launchctl
		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
		T1078.003: Local Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account

Tactic	Technique	Sub-technique
TA0003: Persistence	T1136: Create Account	T1136.003: Cloud Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.002: Systemd Service
		T1543.003: Windows Service
		T1543.004: Launch Daemon
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
		T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification
	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.004: Parent PID Spoofing
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
		T1543.004: Launch Daemon
	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
		T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
		T1548.004: Elevated Execution with Prompt
TA0005: Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
	T1006: Direct Volume Access	
	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.003: Steganography

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.004: Compile After Delivery
		T1027.009: Embedded Payloads
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.004: Parent PID Spoofing
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.014: MMC
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1480: Execution Guardrails	

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.003: Sudo and Sudo Caching
		T1548.004: Elevated Execution with Prompt
		T1548.006: TCC Manipulation
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
		T1550.003: Pass the Ticket
		T1550.004: Web Session Cookie
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
		T1553.002: Code Signing
	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
		T1556.006: Multi-Factor Authentication
	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
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.012 : File/Path Exclusions

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1647: Plist File Modification	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
		T1003.003: NTDS
		T1003.005: Cached Domain Credentials
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	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
		T1552.002: Credentials in Registry
		T1552.005: Cloud Instance Metadata API

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1552: Unsecured Credentials	T1552.007: Container API
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
		T1556.006: Multi-Factor Authentication
	T1557: Adversary-in-the-Middle	
	T1558: Steal or Forge Kerberos Tickets	
TA0007: Discovery	T1606: Forge Web Credentials	T1606.001: Web Cookies
	T1007: System Service Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1087: Account Discovery	T1087.001: Local Account
		T1087.002: Domain Account
	T1120: Peripheral Device Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust 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	
	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
	T1072: Software Deployment Tools	
	T1080: Taint Shared Content	
	T1091: Replication Through Removable Media	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
		T1550.003: Pass the Ticket
		T1550.004: Web Session Cookie

Tactic	Technique	Sub-technique
TA0008: Lateral Movement	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.002: Remote Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.002: Remote Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1530: Data from Cloud Storage Object	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository
		T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1090: Proxy	T1090.002: External Proxy
	T1102: Web Service	T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	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
	T1496: Resource Hijacking	
	T1499: Endpoint Denial of Service	
	T1529: System Shutdown/Reboot	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
	T1657: Financial Theft	

Tactic	Technique	Sub-technique
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.004: Server
		T1583.006: Web Services
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.004: Drive-by Target
		T1608.006: SEO Poisoning
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	
	T1590: Gather Victim Network Information	T1590.002: DNS
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.001: Spearphishing Service
		T1598.002: Spearphishing Attachment

Top 5 Takeaways

#1

In **August 2026**, **5 zero-day vulnerabilities** surfaced. These zero-days were found across products from **Fortinet, Windows, Apple, Fortra, and PaperCut**

#2

Newly identified malware active in August included a broad mix of **Backdoors, Ransomware, and RAT**. Key discoveries were **NightLedger, FDMTP, PhantomCore, PhantomGraph, Troy, ForestTiger, PATCHCORD, SHEETCORD, CoolClient, Antino, ClientKing, C2Looper, and QUICAgent**, each representing distinct capabilities ranging from stealthy persistence to large-scale compromise.

#3

Cyberattacks concentrated heavily on **India, Spain, Germany, Brazil, and Russia**, which absorbed most 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, Education, Healthcare, Finance, and Manufacturing 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 **Lazarus, APT36, and Storm-1175**, 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 **28 significant vulnerabilities** and block the indicators related to the **10 active threat actors**, **38 active malware**, and **255 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 **28 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>NightLedger</u>	SHA256	24771d0a69e442b9493ab1406e0253be1acd31d83f593177fd736f7f6d629ed9
	MD5	A239E655709A2518DD0B7BDBED163679
<u>BridgeHead</u>	SHA256	d80c6f338ecf4997d5dfce92bde9303578982fa6d20e49d3538a269d7f7a048d 78e1d5640936f65071dba0e99abfe85b61a7b1156bfca266edb55585cecf0a3 f0c0357b12b5e6125bf97f6806f91e9183cac133600b2d9c46a7a0a2da997754
	MD5	5FA15EF96808EA82F0A6176F0BB4B386 42F847597109DA2A220391BB09D00676 AFB1C1583606599C7272CFB33CC6F498
<u>ArcBridge</u>	SHA256	0258c24048532e2c6dcd20f15162406e71f9e78763fb256772e4b9c336339fe2 f714881161b8249ceb480da57d9f5ed461157d8ccc6080588af7c6a9a9428f6d 87fa75eaa5d538826570ac7d4f0bcf58879183bac90c068f1b7477883296c416 e0e98bde358a6cf02c36a794021dfd921a7f55c5c7a0a4cd241e9568ed4a4016 2592f40a2ee9dde24eb966c5b0b1afe7ddbc8e80aee4662e68295ad1608a79ee
	MD5	6038D42AF0AFFD1FB263F470C0956F6B AE628EFA305387B633DCE82F9364875B F7D36CC5904A53252D2BB3D21615134F C90F0EFADBF322E5EB1C4103A38C30E6 D09B14A2FE01C7363ECC56F5D046162C
<u>XCSSET</u>	SHA256	ac3467a04eeb552d92651af1187bdc795100ea77a7a1ac755b4681c654b54692

Attack Name	TYPE	VALUE
XCSSET	SHA256	d11a549e6bc913c78673f4e142e577f372311404766be8a3153792de9f00f6c1 172eb05a2f72cb89e38be3ac91fd13929ee536073d1fe576bc8b8d8d6ec6c262 a238ed8a801e48300169afae7d27b5e49a946661ed91fab4f792e99243fbc28d
	Domains	accapple[.]ru adschecks[.]ru adschecks.ru adsmobi[.]ru adsmorein[.]in adsmoreme[.]in amdcdn[.]ru amzndev[.]in amzndev[.]ru amznprod[.]in applecdn[.]ru appledisk[.]ru appledns[.]ru applehosts[.]ru appletime[.]in bulksec[.]ru cdnamz[.]in cdnamz[.]ru cdnapple[.]in cdnatapple[.]ru cdnroute[.]ru checkcdn[.]ru chromeads[.]ru cnmag[.]ru devnetaps[.]ru dnsapple[.]ru

Attack Name	TYPE	VALUE
<u>XCSSET</u>	Domains	dnsrelays[.]ru explorecdn[.]ru fiddlejoy[.]ru figmacat[.]ru figmanets[.]in funchats[.]ru gironetcdn[.]ru goalmate[.]ru googlenets[.]ru greencn[.]ru icloudsnet[.]ru imails[.]ru legalads[.]in littleads[.]in littledns[.]ru maganet[.]ru mindelgate[.]ru netapsdev[.]ru netcdnads[.]in netcdnamz[.]ru netcdndev[.]in netcorps[.]ru netsprot[.]in netsproto[.]in networkads[.]in rigacdn[.]in rigmajoy[.]in rigmanet[.]ru rigmanets[.]in sahusuzuki[.]in stuffdns[.]in testjoys[.]ru timewebnet[.]in

Attack Name	TYPE	VALUE
<u>XCSSET</u>	Domains	vigmanet[.]ru whitead[.]in whiteads[.]ru wincdn[.]ru windsecure[.]ru
<u>ChainDrop</u>	SHA256	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2caa93012b350668fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda806e5684b1eb9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367cfc2509cf1bcc
<u>FDFTP</u>	SHA256	795594ad5e6f2868cc4d8ed12dabf4f3999a1477c6b250527c5ede9a98528fb9
<u>PhantomCore</u>	MD5	c5a460e4e68a088f6e51b2c6474642ec129462164a7d52e9ea8560b60f0412c5ec0bf4a2186a88874e9f26f07cfefb532b348642146ea34771e5785c5857950f5c915cb6c2aeb863ee8479238e16442170e79996d9483d1e44fea32b0a48c2c192bb75c20e778eb5c416965bd4d4259b1b3a6fee3307f1c26841fd5c603e2b0138fcc3e4ccbf1725d9989fb464abf3561
	SHA256	b9e4052b310f9451eca9784a4a33bf5282d1bd07e3359eba9648be625e2e40dd
<u>PhantomGraph</u>	MD5	489f43be558b2679284ceabed7adc4f3dd1fd2b459b97b7d59375cb8383cd19a0e4541c3153ec5ed01497f19cf4f63d0

Attack Name	TYPE	VALUE
<u>PhantomGrap</u> <u>h</u>	MD5	12d4e8f5295f2ef7e0f9bfc0f4830939 7f267006cac10f341c356b62fe493527 ee2861d5965e8730708cd1da8a93fa4c
	SHA256	0fce4b732ce10c72093587e82ca9747a885430e366934ddc27e4 37443ff0cc0e
<u>Troy</u>	SHA256	590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6 d115e1615d6 68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac93303 0a68faac0bb a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf59434 41b9cc99075
<u>FudModule</u>	SHA256	3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8 347b2637c245d
<u>RelayShell</u>	SHA256	21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21e b47c9e22762 cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e 132963d2e222
<u>MISTPEN</u>	SHA256	2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87 bd7232e141eb 5278ee922838352f1480a73e971161017d643a80b7ec22bf7258 97dfd088696d b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c623 5e458d21afb fb3fc5626f68677fb1269a2fefbe70e719211b4065e836ab92e06a 8210139a2d ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac25 04db2c619 13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad34 0dacbcdef79

Attack Name	TYPE	VALUE
<u>MISTPEN</u>	SHA256	4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d 4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7
<u>ForestTiger</u>	SHA256	72dcae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289 231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858 6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d 82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943
<u>DeadLock</u>	SHA256	a1fdf65020ce4a0f0940c793c6425baf8a0b994ec48b9baaf72788661a9d29f4 3c1b9df801b9abbb3684670822f367b5b8cda566b749f457821b6481606995b3 3cd5703d285ed2753434f14f8da933010ecfdc1e5009d0e438188aaf85501612 c9cc95ff8f2998229394dfd31c2bd6b723e826a3ca5e008d2b5be19ba419ae2c 2d89fb7455ff3ebf6b965d8b1113857607f7fbda4c752ccb591dbc1dc14ba0da
	TOR Address	deadblogdbdu5wprek7wa2o4ce7rnt6u6ntqeud3hzjjcveosgpsqqd[.]onion
<u>Gunra</u>	SHA256	75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e

Attack Name	TYPE	VALUE
<u>Gunra</u>	SHA256	25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48 2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751 834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1 91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0 a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
<u>PATCHCORD</u>	SHA256	d46ee94d6a27ff9f02cff6fb57780acac2833ce48c95e63042a6274e24a040bb 50fc220347f9e281037e831c3755dc70a8ba7f663025aea35b301226918b016b 0f4073d3c866bc3daf55b25f71250b96ec120db94a4f9cc8fe85b7c9f9d346b3
<u>SHEETCORD</u>	SHA256	959bbb09cd86ce3930406bf1cf32776ca477dfefe3fd63e90bf0017fccd90587
<u>HACKERAI C2 Agent</u>	SHA256	74d347785dc47f8cda3876826cdd3fb3935ac55dc8e9e0c0f96d5ef4e00089a2
<u>CoolClient</u>	SHA256	ee72ae4cc869affddab11647e95bab9c5691c9fc76dcb4b31650ff504da29156
<u>PlugX</u>	SHA256	d247570da6646a9d66d094090d71a59e6b06e0c31c7346d3d4fbadddef90a887 25c2e47b5663f4b414c02671bfe849bca588d8992cd643af8a411557fa5e3f1e f2f0d2062eb1a181e1669456f077ef4e913750cb5b2a97c3c7668afedcaa6961 91753cefea41f924951a6d441179a0f97b902ae30b7b1fd04b601d266dba435e

Attack Name	TYPE	VALUE
<u>PlugX</u>	SHA256	d9529976ce67da55a0f1a561ff4fb7e6535bfc7b607c838182752fd6e6732794 64b9f35206cb8ad0b79a07dad35acf024d2d429855352674f3fec c0798b96cfd 1f8a2658aeabcfecce2fe37978ccbcddfee8045e23ed5f069b4c17 43acad4ccd ce44171fbacb22d86c61f4c4c47ffb0fca380c96dd1894522ee465 e39d72dcec dc4558efd0113791cbccc363a89a71b3170b71b82065b464a918 32488e792ee3
<u>Monero</u>	SHA256	657fe4474fd1788c2910fb3fc4e2e8ed85ea4598638c4b38811bb bf4090a3999 4f4e99c6e30bc5ce997aa398ab131ecc3e969eb78211de93d321 74575e4d998e 459655bcc84a8239a65300ea61fd44a16f4a7df3cbf011a675646 560c2cc0d5d c20e89caf440d8b3b9b1da8c9467ab6aaea9a17a79a2169f89f07 b1a603cb422 66871e7a931ce86c90fc19cacb47a91fdgba9d3d214369657497c ed2a77f2f4f c05a6dfee8a914f64c75dfb4fa2bae9e8aa8214b5921faa1b3c275 c7a3b79be6 8bf1ae207338b8cd2f3ec202cef0285d09041f94ebdd5ae6c2edfe 8ad59f06b1 60033b1bda21c6d2a70d7e3829d76a44fdc45087ba27b0e6fe01 b54f0c968180
<u>Antino</u>	SHA256	09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e91 05107e5cff c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d 71d71e42cc 153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0dc 22d3bb5c94e

Attack Name	TYPE	VALUE
<u>Antino</u>	SHA256	297413a3e49e7353bf484a3eb15ec647de729211059df8fc68678d2378b6f561 30f5122cc199b9c2e524503b343a9ee13a6f9773dcbc1df82c8b25ad20bca61d 430f12970f8d58f12edccee9019a1aa90fa232c961449bdcc69c8d348a52cf55 5ccdf53881f6c758af8d94fe67066af209b4bc0a3cb80b6a4c724fa d86eb97ef 5edb8d1023b8babf302871b68fa2b26d5ca57633f64951922998e8f1d6c8f7ac 6d5fe6b6a34eeb470798b970b70f41a07ccf59b22f49ad9b3dfff7aa3256f3c2 97c3a6be1711c5340d8806e4a54f7297f3f763d0aa4240b667f1e4e1f98f2aad ac3d453d3c9b0310ebb8a67cef35e2ac954d4acdf70cf497fe43a02c7a510813 e782a6d4919f194d41e524ebd6df5894197043cf772fcf60455127b246f302c0 ea893abf20b00d9bfc042a88fbf7b4bd42e68ce07c116d3e3b002e5b4a853877 ed96e7f1085a50251eb8967ac53777272a617831084f0edad8a769c583a18869
<u>SilentDataCollector</u>	SHA256	23cbabfe3ca3a7f1eb365f772d6a4ed8095cb8f7755622cc82e804478259dc70
<u>NetworkShare Scanner</u>	SHA256	8d1e23630a6695fa9c793d73832f59436c98bba30ed81c16d01b549bd17feab4 10babb15e08f9fbd72cce11713a273b971c910dd5bdb989a3f6ff4d9c8e372c0 f042240c3de00c46dee625916bf246b7e87481e4081a6a97208b091409766e41
<u>SilentEncryptor</u>	SHA256	b79b9b027f76579555069a7506d946648a8cb3126c0dda837dc9fee0e5c79489

Attack Name	TYPE	VALUE
<u>SilentEncrypt</u> <u>or</u>	SHA256	65550f6d0ffec8421f703cdc7273d9c0563b3d480fe6702bad294a18afe72143 0080d0dd72eda4850a02e51c0e5c6f768423dfe970cafae2ab52ceee75972b40
<u>Medusa</u>	Email	key[.]medusa[.]serviceteam[.]protonmail[.]com medusa[.]support[.]onionmail[.]org mds[.]svt[.]breach[.]protonmail[.]com mds[.]svt[.]mir2[.]protonmail[.]com MedusaSupport[.]cock[.]li
	SHA256	0cefeb6210b7103fd32b996beff518c9b6e1691a97bb1cda7f5fb57905c4be96 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c e57ba1a4e323094ca9d747bfb3304bd12f3ea3be5e2ee785a3e656c3ab1e8086 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19 56b08aa03bd8c0ea094cfef03d5954ffd857bac42df929dc835eea62f32b09e0 a5a3c3c4fbf5c7db808176db3242c2106995c85f8ba987472ea0e92e59503b55 d3abd4bae082d4c9918447fe82c521567cc7f9b0e5f2d55999a6e5c40fa7fd54 7ffce7f6d7262f214d78e6b7fd8d07119835cba4b04ce334260665d7c8fb369a b29defbbc4ebaa243c1712ccc4943374f1b6fb864c39ed9f70fceb17eee098db 04b13b6cd5e5291b1cde78975a140feea7fd3bc3777c53caa1ab33426c83bfcc
<u>Grandoreiro</u>	SHA256	1b2fe30c5bf57f9623efb34688580fe5bbb2c55351c5a07a6c4313bb6faa29f1

Attack Name	TYPE	VALUE
<u>Grandoreiro</u>	SHA256	1fe5a72aefc38afeeee72d8a939f9db50800a447b7313f4d8c504771bb7fa2de 2820a2e36f1cb537a7853fde2313a5158d1e3696ff81c3066ec8fe274358c22d 368246eb503585f26e0151431909792b8d9be0edc229bb207be882bfb374c005 37492ecd9deb8591ea7e179ebb8e13c6b486cdacae18a6a482d9dd18f08453a3 47d5a73b220813299f753ef0a96582a8d08b853391864128a1f15271dbb42e65 609755a8c73e53f332428786c366323b3979850aaa0e075d946e6c05aa62f867 65db035f79db85ad66fb3e0365e478f95f8f648545b18360d850a7ed179c9dab 684f5eb157ef2ba3ea17335d6c8c9c801f93e6eb3aa08ecbfaf5806a4b5e3b80 a91c7cb932301454df4b0feed58082cae7f2d0e4078d7e6df3f53d806ed04f1d 90254c3baec79cf9b448836293d3864ee273c30de374933296c6e8e3bcaefdbd ad5762fa98da2aff24d9d6b55be5dae21d07c54679ead67252a19c2521162a87 c019cfa9b50a69ff07e98bd78b3a6fc489110e5db1c0d79ada716605a2320951 ca33f5608b72ecca64a002074a4103c7cb83de902ecf5c69949eecb7eef03b5a cc238813ab277cbb4324d37875c37985ca5baeaf8c412b4c85aa8ec5faec7096 e0491eddb45425a674e479b2590517ffef2f108add431761bb89791fc208b6e9 e99416ff71e4574de4fceeabdc34f3b9a6e0610f36b77b735b231bd39edb7a0a1
<u>C2Looper</u>	SHA256	f96ff2f3abbff7f382ace509b90e54853b4b61c402ecde27d82f1c17b414867b
<u>SynkLoader</u>	SHA256	d150c70d2732df17aa77991b9ebf4c896f044445e900978581d9598dfa5dc98c

Attack Name	TYPE	VALUE
<u>QUICAgent</u>	SHA256	cd147efe37003399e174951927e5fe727a4481756b116f0204a14a64cc62b059
<u>WeedHack</u>	SHA256	3951533d56803cd5d708014b4eed7e30349b4c4ba43f7d843133b3a5e2992ce6
<u>GoCaracal</u>	IPv4	109[.]120[.]187[.]217 109[.]172[.]95[.]121 138[.]124[.]112[.]213 138[.]124[.]14[.]130 176[.]124[.]220[.]153 185[.]125[.]101[.]181 185[.]96[.]80[.]110 185[.]96[.]80[.]54 193[.]233[.]245[.]52 193[.]233[.]245[.]45 193[.]233[.]245[.]0 62[.]60[.]237[.]22 77[.]110[.]104[.]98 77[.]110[.]105[.]244 77[.]110[.]105[.]56 77[.]110[.]105[.]59 77[.]110[.]98[.]66 80[.]71[.]224[.]30 82[.]117[.]87[.]138 82[.]117[.]87[.]192 85[.]192[.]30[.]211 79[.]137[.]192[.]38 46[.]226[.]162[.]68 45[.]152[.]198[.]108
	SHA256	1E499C815146124C4A6D2B48C99068B980AD74E1A2CFD16013F8D75A9425A0CA77F7AD29F4A8037EE5F38D3D87FB91CFD97CB8F7FA7883EDF3FCE506DF5200C0
<u>Bandook</u>	IPv4	91[.]208[.]197[.]80

Attack Name	TYPE	VALUE
<u>Bandook</u>	IPv4	91[.]208[.]184[.]45 91[.]208[.]206[.]88 91[.]208[.]184[.]130 176[.]123[.]1[.]174
	SHA256	a2cdf2fe741de4b13ad2298b387a6c32da4a94da180ae75bf8547386aee7376b
<u>Delphi loader</u>	SHA256	0A6DA70548F14834ACB8960689A589B48FF422F8385AE445A281AAB77045FE22
<u>SparkRAT</u>	SHA256	c1a8556741564c3698b56419f66cc27ad50be9148ef483f92866d4edabc46624 f949d967355578cb6a34a678b6e8683b21e58e2ea6b6d5e0cdd4f59af2e37f19 d56c6513a8b25b1883ef33a95d4ece591eabbe17a58f7e3d0fc77c6f29344148 a2c1b858c1d4788e87bb699e3775e851cda95488979b15f4d676f6e1915d8bc8

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

September 03, 2026 • 7:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com