

Date of Publication
June 2, 2025



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

MAY 2025

Table Of Contents

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

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

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

[Celebrity Vulnerabilities](#) 06

[Vulnerabilities Summary](#)..... 07

[Attacks Summary](#)..... 11

[Adversaries Summary](#)..... 14

[Targeted Products](#)..... 16

[Targeted Countries](#)..... 19

[Targeted Industries](#)..... 20

[Top MITRE ATT&CK TTPs](#)..... 21

[Top Indicators of Compromise \(IOCs\)](#)..... 22

[Vulnerabilities Exploited](#)..... 25

[Attacks Executed](#)..... 48

[Adversaries in Action](#)..... 68

[MITRE ATT&CK TTPs](#)..... 82

[Top 5 Takeaways](#)..... 86

[Recommendations](#)..... 87

[Appendix](#)..... 88

[Indicators of Compromise \(IoCs\)](#)..... 89

[What Next?](#)..... 98

Summary

In **May**, the cybersecurity landscape saw heightened activity with the exploitation of 27 zero-day vulnerabilities. One of the most critical among them was **CVE-2025-31324** a flaw in SAP NetWeaver that is being actively exploited to drop web shells and execute malicious code on vulnerable servers. Several cybercriminal groups, including the Russian ransomware gang **BianLian** and the operators behind **RansomExx**, have shown significant interest in leveraging this vulnerability.

Ransomware activity surged during the same period, with threat actors deploying aggressive variants such as **DragonForce**, **Agenda**, **Interlock**, **Nitrogen**, **Qilin**, **BianLian**, and **RansomExx**. As these attacks become more sophisticated, organizations are urged to strengthen their defenses. This includes implementing robust backup and disaster recovery plans, alongside employee training programs focused on recognizing and mitigating phishing attempts.

In parallel, **Operation RoundPress** a stealthy espionage campaign conducted by Russian state-sponsored group **APT28** targeted webmail platforms including **Roundcube**, **Horde**, and **Zimbra**. By exploiting unpatched vulnerabilities, the attackers gained unauthorized access to communications. This operation underscores the risks of outdated webmail infrastructure, where even a single missed patch can lead to serious security breaches.

Moreover, at least **15** known threat actors were active throughout May, each conducting various cyber campaigns. Notably, **Void Blizzard** a Russian-backed espionage group operational since 2024 continued its relentless targeting of NATO members, Ukraine, and sectors such as defense, aviation, and government. Rather than relying on advanced exploits, Void Blizzard primarily leverages stolen credentials to breach systems, highlighting the persistent threat posed by credential theft. As the threat landscape continues to evolve, organizations must remain vigilant, prioritize patch management, and adopt proactive threat detection and response strategies to stay ahead of emerging threats.



In May 2025, a geopolitical cybersecurity landscape unfolds, revealing **United States, United Kingdom, Germany** and **Italy** as the top-targeted countries.

Highlighted in **May 2025** is a cyber battleground encompassing the **Government, Finance, Defence** and **Media** sectors, designating them as the top industries.

Mimo Strikes Fast: Threat Actor Exploits Craft CMS RCE (CVE-2025-32432) to Drop XMRig and Proxyware, Chaining Yii Flaw for Persistence

Void Blizzard Intensifies Attacks:

Russia-Linked Espionage Group Hits NATO and Key Sectors by Exploiting Stolen Credentials Over Sophisticated Exploits

AI-Generated TikToks Push Malware:

Fake Activation Tutorials Drop Vidar and StealC via PowerShell Tricks

PoisonSeed

Phishing Campaign Hijacks Emails to Push Crypto Scams, Steals Wallets via Seed Phrase Poisoning

CVE-2025-47577: flaw in TI WooCommerce Wishlist No patch - disable now

SideWinder Leverages Old **Microsoft Office** Vulnerabilities to Strike Military and Government Targets

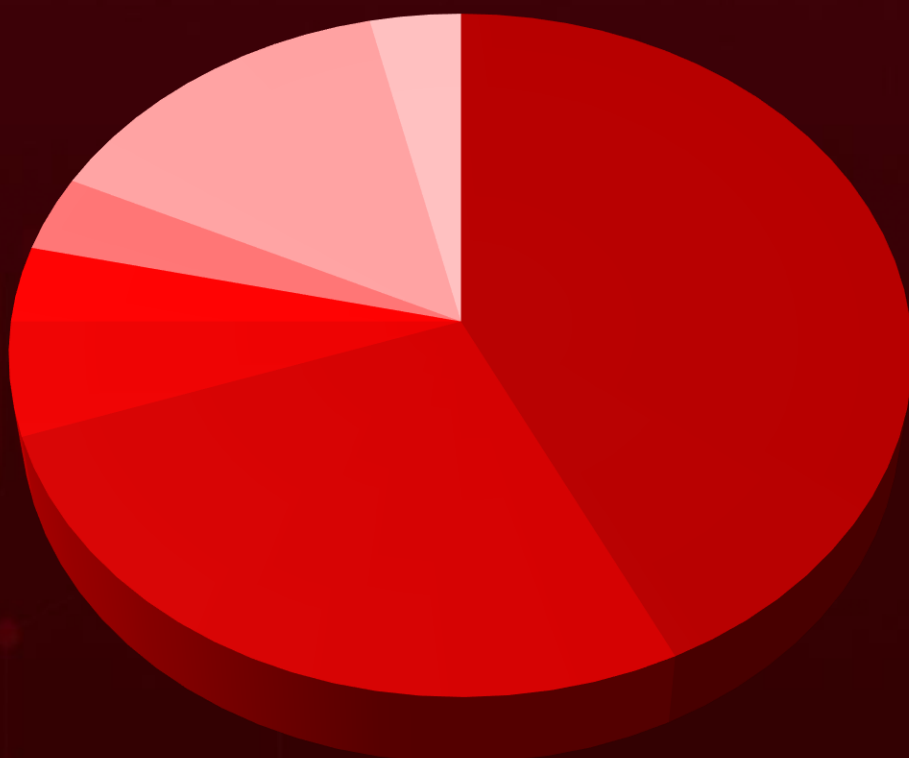
Zero-Day Unleashed

CVE-2025-29824
Exploited with Custom Grixba Infostealer for Stealthy Data Theft and Deep System Intrusion

APT41's

TOUGHPROGRESS malware turns Google Calendar into a covert control hub - slipping past defenses by hiding in plain sight within trusted cloud services

Threat Landscape



- Malware Attacks
- Supply Chain Attacks
- Denial-of-Service Attack
- Password Attack
- Social Engineering
- Man-in-the-Middle Attack
- Injection Attacks


































































Celebrity Vulnerabilities
















CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>	Log4shell	Apache Log4j2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*: *.*.*.*.*.*.*	DragonForce
Apache Log4j2 Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/security.html

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-44221	SonicWall SMA100 Appliances OS Command Injection Vulnerability	SMA 100 Series			
CVE-2024-38475	Apache HTTP Server Improper Escaping of Output Vulnerability	SMA 100 Series			
CVE-2025-3248	Langflow Missing Authentication Vulnerability	Langflow			
CVE-2025-29824	Microsoft Windows Common Log File System (CLFS) Driver Use-AfterFree Vulnerability	Microsoft Windows			
CVE-2025-2857	Mozilla Firefox Sandbox Escape Vulnerability	Mozilla Firefox			
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2			
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure			
CVE-2024-21412	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows Internet Shortcut Files			
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure			
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons ServerSide Request Forgery (SSRF) Vulnerability	Pulse Connect Secure, ZTA gateways, Pulse Policy Secure			
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-27920	Srimax Output Messenger Directory Traversal Vulnerability	Srimax Output Messenger			
CVE-2024-11120	GeoVision Devices OS Command Injection Vulnerability	GeoVision			
CVE-2024-6047	GeoVision Devices OS Command Injection Vulnerability	GeoVision			
CVE-2025-32756	Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	Fortinet Multiple Products			
CVE-2025-4632	Samsung MagicINFO 9 Server Path Traversal Vulnerability	Samsung MagicINFO 9 Server			
CVE-2025-4427	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile			
CVE-2025-4428	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile			
CVE-2025-30400	Microsoft Windows DWM Core Library Use-After-Free Vulnerability	Microsoft Windows			
CVE-2025-32701	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Microsoft Windows			
CVE-2025-32706	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability	Microsoft Windows			
CVE-2025-32709	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Microsoft Windows			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-30397	Microsoft Windows Scripting Engine Type Confusion Vulnerability	Microsoft Windows			
CVE-2025-4664	Google Chromium Loader Insufficient Policy Enforcement Vulnerability	Google Chromium			
CVE-2023-43770	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube			
CVE-2020-35730	Roundcube Webmail CrossSite Scripting (XSS) Vulnerability	Roundcube			
CVE-2017-11882	MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	MDaemon			
CVE-2024-27443	Synacor Zimbra Collaboration Suite (ZCS) CrossSite Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)			
CVE-2025-4918	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Mozilla Firefox			
CVE-2025-4919	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Mozilla Firefox			
CVE-2017-0199	Microsoft Office and WordPad Remote Code Execution Vulnerability	Microsoft Office and WordPad			
CVE-2024-11182	Microsoft Office Memory Corruption Vulnerability	Microsoft Office			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-0994	Trimble Cityworks Deserialization Vulnerability	Trimble Cityworks			
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver			
CVE-2025-32432	Craft CMS Remote Code Execution Vulnerability	Craft CMS			
CVE-2024-58136	Yiiframework Yii Improper Protection of Alternate Path Vulnerability	Yiiframework Yii			
CVE-2025-47577	TemplateInvaders TI WooCommerce Wishlist Plugin Unrestricted File Type Upload Vulnerability	TemplateInvaders TI WooCommerce Wishlist Plugin			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
StealC V2	Information Stealer	-	-	-	-
More_eggs	Backdoor	-	-	-	Phishing
Grixba	Information Stealer	CVE-2025-29824	Microsoft Windows		Exploiting Vulnerability
DragonForce	Ransomware	CVE-2021-44228, CVE-2023-46805, CVE-2024-21412, CVE-2024-21887, CVE-2024-21893, CVE-2022-26134	Apache Log4j2, Ivanti Connect Secure and Policy Secure, Microsoft Windows Internet Shortcut Files, Pulse Connect Secure, ZTA gateways, Pulse Policy Secure, Atlassian Confluence Server and Data Center		Exploiting Vulnerabilities, Phishing
NOOPDOOR	Backdoor	-	-	-	Phishing
ANEL	Backdoor	-	-	-	Phishing
ROAMINGMOUSE	Dropper	-	-	-	Phishing
Agenda (aka Qilin, Water Galura)	Ransomware	-	-	-	Phishing
SmokeLoader	Loader	-	-	-	Phishing
NETXLOADER	Loader	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Crimson	RAT	-	Linux	-	Phishing
Poseidon	Backdoor	-	Linux	-	Kavach 2FA tool
ElizaRAT	RAT	-	Windows	-	Phishing
PupkinStealer	Infostealer	-	Windows	-	-
Mirai	Botnet	CVE-2024-11120 CVE-2024-6047	GeoVision Devices		Exploiting vulnerabilities
LZRD	Botnet	CVE-2024-11120 CVE-2024-6047	GeoVision Devices		Exploiting vulnerabilities
TransferLoade	Loader	-	-	-	-
SpyPress	Information Stealer	CVE-2023-43770 CVE-2020-35730 CVE-2024-11182 CVE-2024-27443	Roundcube Webmail, MDAemon Email Server, Zimbra Collaboration (ZCS)		Loaded by the XSS Vulnerabilities
LOSTKEYS	Information Stealer	-	-	-	Phishing Emails
StealerBot	Credential Stealer	CVE-2017-0199 CVE-2017-11882	Microsoft Office and WordPad		Spearphishing Attachment
Interlock	Ransomware	-	-	-	Phishing
Nitrogen	Ransomware	-	Windows	-	Malvertising Campaigns
PureHVNC	RAT	-	-	-	Malvertising Campaigns
PureRAT	RAT	-	-	-	Phishing Emails
PureLogs	Stealer	-	-	-	Phishing Emails
PureCrypter	Loader	-	-	-	Phishing Emails

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
TetraLoader	Loader	CVE-2025-0994	Trimble Cityworks		Exploiting Vulnerability
KrustyLoader	Loader	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability
Qilin	Ransomware	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability
BianLian	Ransomware	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability
RansomExx	Ransomware	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability
PipeMagic	Trojan	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability
Vidar	Stealer	-	-	-	Social Engineering via AI-generated TikTok videos
StealC	Stealer	-	-	-	Social Engineering via AI-generated TikTok videos
Dero crypto miner	Crypto miner	-	-		Social Engineering
XMRig	Crypto miner	CVE-2025-32432 CVE-2024-58136	Craft CMS Yiiframework Yii		Exploiting Vulnerabilities
TOUGHPROGRESS	Framework	-	-	-	Spear-phishing Attachment


Adversaries Summary










ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
RomCom	Information theft and espionage, Financial gain	Russia	-	-	-
Venom Spider	Financial Gain	Russia	-	More_eggs	-
Earth Kasha	Information theft and espionage	China	-	NOOPDOOR, ANEL, ROAMINGMOUSE	-
APT36	Information Theft and Espionage	Pakistan	-	Crimson RAT, Poseidon, ElizaRAT	Windows, Linux, Android
Marbled Dust	Information theft and espionage	Turkey	CVE-2025-27920	-	Output Messenger
APT28	Information theft and espionage	Russia	CVE-2023-43770 CVE-2020-35730 CVE-2024-11182 CVE-2024-27443	SpyPress	Roundcube Webmail, MDAemon Email Server, Zimbra Collaboration (ZCS)
COLDRIVER	Information theft and espionage	Russia	-	LOSTKEYS	-
SideWinder	Information theft and espionage	India	CVE-2017-0199 CVE-2017-11882	StealerBot	Microsoft Office and WordPad






ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UAT-6382	Information theft and espionage	Chinese-speaking	CVE-2025-0994	TetraLoader	Trimble Cityworks
UNC5221	Information theft and espionage	China	CVE-2025-31324	KrustyLoader	SAP NetWeaver
UNC5174	Espionage, Financial Gains	China	CVE-2025-31324	-	SAP NetWeaver
CL-STA-0048	Espionage	China	CVE-2025-31324	-	SAP NetWeaver
Void Blizzard	Information theft, Espionage	Russia	-	-	-
Mimo (aka Hezb)	Financial Gains	-	CVE-2025-32432 CVE-2024-58136	XMRig	Craft CMS, Yiiframework k Yii
APT41	Financial crime, Information theft and espionage	China	-	TOUGHPROGRESS	Spear-phishing emails



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Web Server	Apache SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions
		Apache Log4j2
	Network Security Appliance	SonicWall SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions
	Low-Code AI Application Builder	Langflow versions prior to 1.3.0
	Server	Microsoft Windows: 10 - 11 24H2, Windows Server: 2008 - 2025
	Operating System File Format	Microsoft Windows Internet Shortcut Files
	Server	Microsoft Windows: 10 21H2 - 11 24H2 Windows Server: 2008 – 2025 Microsoft Internet Explorer: 11
	Application	Microsoft Office and WordPad
	Browser	Mozilla Firefox versions prior to 136.0.4 Firefox ESR versions prior to 128.8.1 Firefox ESR versions prior to 115.21.1
	Browser	Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1
	Secure Remote Access Appliance	Ivanti Connect Secure and Policy Secure, Pulse Connect Secure, ZTA gateways, Pulse Policy Secure
	Unified Endpoint Management (UEM) Solution	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
 Confluence	Server	Atlassian Confluence Server and Data Center
	Application	Output Messenger before 2.0.63
	Video Surveillance Software (VMS)	GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3
	Network Video Surveillance System	FortiCamera Version 2.1.0 through 2.1.3 FortiCamera 2.0 All Versions FortiCamera 1.1 All Versions FortiMail Version 7.6.0 through 7.6.2 FortiMail Version 7.4.0 through 7.4.4 FortiMail Version 7.2.0 through 7.2.7 FortiMail Version 7.0.0 through 7.0.8 FortiNDR Version 7.6.0 FortiNDR Version 7.4.0 through 7.4.7 FortiNDR Version 7.2.0 through 7.2.4 FortiNDR 7.1 All Versions FortiNDR Version 7.0.0 through 7.0.6 FortiNDR 1.1 – 1.5 All Versions FortiRecorder Version 7.2.0 through 7.2.3 FortiRecorder Version 7.0.0 through 7.0.5 FortiRecorder Version 6.4.0 through 6.4.5 FortiVoice Version 7.2.0 FortiVoice Version 7.0.0 through 7.0.6 FortiVoice Version 6.4.0 through 6.4.10
	Server	Samsung MagicInfo 9 Server Versions prior to 21.1052
	Browser	Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76
	Web-based Email Client (Webmail)	Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3 Roundcube: 1.2.0 - 1.4.9
	Email Server Software	MDaemon Email Server before version 24.5.1c
	Collaborative Software Suite	Zimbra Collaboration (ZCS) 9.0 and 10.0

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	GIS-Centric Asset Lifecycle Management System	Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10
	Enterprise Application Platform	SAP NetWeaver Version 7.50
	Content Management System	Craft CMS
	Web Application Framework	Yii framework Yii
	Plugin	TemplateInvaders TI WooCommerce Wishlist Plugin

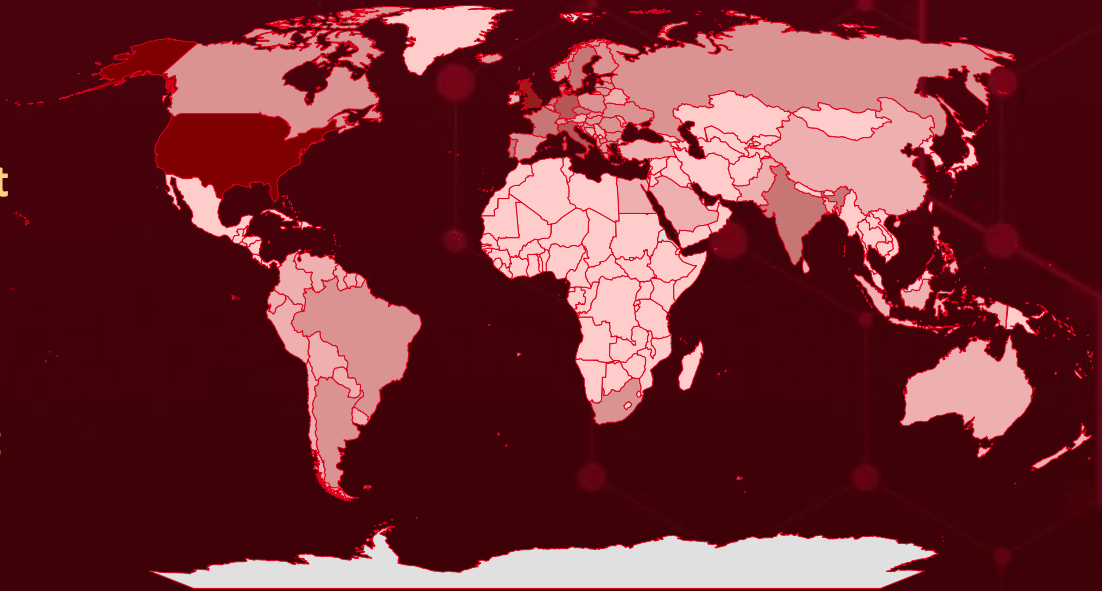


Targeted Countries

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
	United States		Hungary		Monaco		Philippines		Niger
	United Kingdom		North Macedonia		Chile		Bangladesh		Grenada
	Germany		Iceland		Bosnia and Herzegovina		Republic of Ireland		Bonaire
	Italy		Poland		China		Indonesia		Guadeloupe
	France		Spain		Turkey		San Marino		Scotland
	Netherlands		Romania		Colombia		Israel		Guam
	Sweden		Bulgaria		Pakistan		Serbia		Burundi
	Czech Republic		Slovakia		Ecuador		Liechtenstein		Guatemala
	Portugal		Ukraine		Bolivia		Andorra		Cambodia
	Denmark		South Africa		Egypt		Belarus		Guernsey
	India		Brazil		Saudi Arabia		Suriname		Northern Cyprus
	Estonia		Montenegro		Australia		Uruguay		Guinea
	Canada		Switzerland		Sri Lanka		Venezuela		Cape Verde
	Slovenia		Argentina		French Guiana		Malta		Guinea-Bissau
	Croatia		Belgium		Moldova		Tokelau		Faroe Islands
	Norway		Lithuania		Austria		Saint Eustatius		Congo-Brazzaville
	Albania		Luxembourg		New Zealand		Chad		Saint Vincent and the Grenadines
	Russia		Latvia		Guyana		Azerbaijan		Haiti
	Greece		Singapore		Paraguay		Brunei		Sierra Leone
	Finland		Peru		Holy See		Greenland		Costa Rica
									Niger
									Grenada

Targeted Industries

Most



Government



Financial



Defence



Media



Banking



Technology



Education



Tele-communications



Retail



Manufacturing



Legal



Energy



Professional Services



Logistics



Utilities



Construction



Electrical



Aerospace



Hospitality



Automotive



Transportation



Healthcare



Oil & Gas



Engineering



Real Estate



Gaming



NGOs



Food products



Political Entities



Cryptocurrency



Chemical



Insurance



Think-Tanks



E-commerce



Religious



Agriculture



Travel



Aviation



Research Organizations



Entertainment



Pharmaceutical

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1588.006

Vulnerabilities

T1566

Phishing

T1204

User Execution

T1036

Masquerading

T1041

Exfiltration Over C2 Channel

T1071

Application Layer Protocol

T1082

System Information Discovery

T1071.001

Web Protocols

T1005

Data from Local System

T1547

Boot or Logon Autostart Execution

T1588.005

Exploits

T1204.002

Malicious File

T1059.001

PowerShell

T1547.001

Registry Run Keys / Startup Folder

T1140

Deobfuscate/Decode Files or Information

T1083

File and Directory Discovery

T1203

Exploitation for Client Execution

T1068

Exploitation for Privilege Escalation

T1566.002

Spearphishing Link

T1486

Data Encrypted for Impact

T1057

Process Discovery



Top Indicators of Compromise (IOCs)




Attack Name	TYPE	VALUE
<u>KrustyLoader</u>	SHA256	f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec, 47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04, 3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce, 91f66ba1ad49d3062afdcc80e54da0807207d80a1b539edcbbd6e1bf99e7a2ca, c71da1dfea145798f881afd73b597336d87f18f8fd8f9a7f524c6749a5c664e4, b8e56de3792dbd0f4239b54cfaad7ece3bd42affa4fbbdd7668492de548b5df8, 0c2c8280701706e0772cb9be83502096e94ad4d9c21d576db0bc627e1e84b579, 5f3d1f17033d85b85f3bd5ae55cb720e53b31f1679d52986c8d635fd1ce0c08a
	Domains	brandnav-cms-storage[.]s3[.]amazonaws[.]com, abode-dashboard-media[.]s3[.]ap-south-1.amazonaws[.]com, applr-malbbal[.]s3[.]ap-northeast-2[.]amazonaws[.]com
<u>Qilin</u>	URL	hxxp[:]//184[.]174[.]96[.]70
	IPv4	180[.]131[.]145[.]73
<u>BianLian</u>	IPv4:Port	64[.]190[.]113[.]215[:]:443, 15[.]237[.]93[.]235[:]:443, 94[.]198[.]40[.]6[:]:20033, 94[.]198[.]40[.]6[:]:20007, 139[.]162[.]1[.]232[:]:8443, 49[.]232[.]6[.]238[:]:443, 170[.]64[.]148[.]46[:]:443
<u>RansomExx</u>	SHA256	bb12b7c4169e2a86a67a86f03048baa282688d36ef0ae3251bc1ace317c26af9, 6b667bb7e4f3f2cb6c6f2d43290f32f41ae9f0d6ed34b818d78490050f7582a1, 78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d, 08113ca015468d6c29af4e4e4754c003dacc194ce4a254e15f38060854f18867, cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849, 843b8434ab69089970530b0d1a9865a89d25aed88bc98d91845bfe41a6dfc31b




Attack Name	TYPE	VALUE
<u>PipeMagic</u>	SHA256	945a02cdbbd8772f5b0a30f047ae6450ee77a14fef5046af252565a9b524c88f, d9cb912e6ca4dc22515b9dfddced01a96f6de2fd51169597d437d390d5d868f1, 2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe
<u>Grixba</u>	SHA256	6030c4381b8b5d5c5734341292316723a89f1bdbd2d10bb67c4d06b1242afd05
<u>DragonForce</u>	SHA1	343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c, 229e073dbcb72bdfec2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4, 577b110a8bfa6526b21bb728e14bd6494dc67f71, 7db52047c72529d27a39f2e1a9ffb8f1f0ddc774, 81185dd73f2e042a947a1bf77f429de08778b6e9, a4bdd6cef0ed43a4d08f373edc8e146bb15ca0f9, b571e60a6d2d9ab78da1c14327c0d26f34117daa, e1c0482b43fe57c93535119d085596cd2d90560a, eada05f4bfd4876c57c24cd4b41f7a40ea97274c, fc75a3800d8c2fa49b27b632dc9d7fb611b65201
<u>Crimson</u>	MD5	026e8e7acb2f2a156f8afff64fd54066, fb64c22d37c502bde55b19688d40c803, 70b8040730c62e4a52a904251fa74029, 3efec6ffcbfe79f71f5410eb46f1c19e, b03211f6feccd3a62273368b52f6079d
	SHA256	d1a1eaefe6bd2e245bba369e966d7a8eab9ed6ad1fa827321e5889cc8d43f976
<u>Poseidon</u>	SHA256	541cefaad8d9554bdc5ce9cde24e4556c2444111ea13bd9965bd4a50e60f9265, 682d5e53a456668f15809d9ab499651e1342fc602e7f5bc85e30fe29933f7634, 7e2020c4a838bd7463478188bfaa97e66cf3365d3aef03f1b4398eaddacfc6b9
<u>ElizaRAT</u>	SHA256	b30a9e31b0897bfe6ab80aebcd0982eecf68e9d3d3353c1e146f72195cef0ef5, 263f9e965f4f0d042537034e33699cf6d852fb8a52ac320a0e964ce96c48f5e5




Attack Name	TYPE	VALUE
<u>SpyPress</u>	SHA1	41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C, 1078C587FE2B246D618AF74D157F941078477579, F95F26F1C097D4CA38304ECC692DBAC7424A5E8D, B6C340549700470C651031865C2772D3A4C81310, 65A8D221B9ECED76B9C17A3E1992DF9B085CECD7, 8E6C07F38EF920B5154FD081BA252B9295E8184D, AD3C590D1C0963D62702445E8108DB025EEBEC70, EBF794E421BE60C9532091EB432C1977517D1BE5, F81DE9584F0BF3E55C6CF1B465F00B2671DAA230
<u>TetraLoader</u>	SHA256	14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64 c4f4611f, 4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67 d1850a9
<u>Dero</u>	SHA256	e4aa649015b19a3c3350b0d897e23377d0487f9ea265fe94e71 61fed09f283cf
	Wallet Address	dero1qyy8xjrdjcn2dvr6pwe40jrl3evv9vam6tpx537vux60xxkx6 hs7zqgde993y
	Domains	d[.]windowsupdatesupport[.]link, h[.]wiNdowsupdatesupport[.]link
<u>XMRig</u>	SHA256	3a71680ffb4264e07da4aaca16a3f8831b9a30d444215268e82 b2125a98b94aa
<u>TOUGHPROGR ESS</u>	SHA256	3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2f a302791c2c4fb









Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38475</u>		SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*	-
Apache HTTP Server Improper Escaping of Output Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-116	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://httpd.apache.org/download.cgi




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-44221</u>		SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*	-
SonicWall SMA100 Appliances OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-3248</u>		Langflow versions prior to 1.3.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:langflow-ai:langflow:*:*:*:*:*:*	-
Langflow Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006: Python	https://github.com/langflow-ai/langflow/releases/tag/1.3.0




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-29824</u>		Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	Grixba
Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-2857</u>		Firefox versions prior to 136.0.4 Firefox ESR versions prior to 128.8.1 Firefox ESR versions prior to 115.21.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*	-
Mozilla Firefox Sandbox Escape Vulnerability		*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion, T1611: Escape to Host	https://www.mozilla.org/en-US/security/advisories/mfsa2025-19/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46805</u>		Ivanti Connect Secure and Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*	DragonForce
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.iva nti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21412</u>		Microsoft Windows Internet Shortcut Files	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*	DragonForce
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204: User Execution T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21887</u>		Ivanti Connect Secure and Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*	DragonForce
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US







CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21893</u>		Pulse Connect Secure, ZTA gateways, Pulse Policy Secure	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*.:.:.:.:.*	DragonForce
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-26134</u>		Atlassian Confluence Server and Data Center	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*.:.:.:.:.* cpe:2.3:a:atlassian:confluence_server:*.:.:.:.:.*	DragonForce
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://jira.atlassian.com/browse/CONFSERVER-79016




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-27920</u>		Output Messenger before 2.0.63	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:output_messenger:out_put_messenger:-:*:*:*:*:*	-
Srimax Output Messenger Directory Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://www.outputmessenger.com/cve-2025-27920/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-11120</u>		GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*	Mirai, LZRD
GeoVision Devices OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32756</u>		FortiCamera Version 2.1.0 through 2.1.3 FortiCamera 2.0 All Versions FortiCamera 1.1 All Versions FortiMail Version 7.6.0 through 7.6.2 FortiMail Version 7.4.0 through 7.4.4 FortiMail Version 7.2.0 through 7.2.7 FortiMail Version 7.0.0 through 7.0.8 FortiNDR Version 7.6.0 FortiNDR Version 7.4.0 through 7.4.7 FortiNDR Version 7.2.0 through 7.2.4 FortiNDR 7.1 All Versions FortiNDR Version 7.0.0 through 7.0.6 FortiNDR 1.1 – 1.5 All Versions FortiRecorder Version 7.2.0 through 7.2.3 FortiRecorder Version 7.0.0 through 7.0.5 FortiRecorder Version 6.4.0 through 6.4.5 FortiVoice Version 7.2.0 FortiVoice Version 7.0.0 through 7.0.6 FortiVoice Version 6.4.0 through 6.4.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortivoice:*:*:*:*:*:* cpe:2.3:a:fortinet:fortirecorder:*:*:*:*:*:* *.* cpe:2.3:a:fortinet:fortindr:*:*:*:*:*:* cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:* cpe:2.3:a:fortinet:forticamera:*:*:*:*:*:* *	-
Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation; T1053.003: Scheduled Task/Job: Cron	https://fortiguard.fortinet.com/p/sirt/FG-IR-25-254




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4632</u>		Samsung MagicInfo 9 Server Versions prior to 21.1052	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:samsung:magicinfo_9_server:*.~.*.*.*.*.*.*	-
Samsung MagicINFO 9 Server Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://eu.community.samsung.com/t5/samsung-solutions/update-magicinfo-server-v9-21-1052-0-setup-file/ta-p/11374265
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4427</u>		Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_mobile:*.~.*.*.*.*.*.*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4428</u>		Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:endpoint_manager_mobile:*.~.*.*.*.*.*	-
Ivanti Endpoint Manager Mobile (EPM) Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPM




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-30400</u>		Windows: 10 21H2 - 11 24H2 Windows Server: 2012 Gold - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*.~.*.*.*.*.*.* cpe:2.3:o:microsoft:windows_server:-.*.*.*.*.*.*.*	-
Microsoft Windows DWM Core Library Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32701</u>		Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability		cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32701







CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32706</u>		Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability		cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32706




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32709</u>		Windows: 10 21H2 - 11 24H2 Windows Server: 2012 - 2025	-
	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	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-327069

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-30397</u>		Windows: 10 - 11 Windows Server: 2008 - 2025	-
	ZERO-DAY	Microsoft Internet Explorer: 11	
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Scripting Engine Type Confusion Vulnerability		cpe:2.3:o:microsoft:windows_server-*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter; T1204.001: User Execution: Malicious Link; T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30397




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4664</u>		Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chromium Loader Insufficient Policy Enforcement Vulnerability		cpe:2.3:a:microsoft:edge:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-346	T1528: Steal Application Access Token; T1189 : Drive-by Compromise; T1204: User Execution	https://www.google.com/intl/en/chrome/?standalone=1




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-43770</u>		Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	SpyPress
Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1588.006: Vulnerabilities, T1204: User Execution	https://roundcube.net/news/2023/09/15/security-update-1.6.3-released




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-35730</u>		Roundcube: 1.2.0 - 1.4.9	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	SpyPress
Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1059.007: JavaScript/JScript, T1557: Man-in-the-Browser, T1189: Drive-by Compromise, T1204: User Execution, T1204.001: Malicious Link	https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-11182</u>		MDaemon Email Server before version 24.5.1c	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:mdaemon:mdaemon:*:*:*:*:*:*	SpyPress
MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204: User Execution	https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-27443</u>		Zimbra Collaboration (ZCS) 9.0 and 10.0	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*:*	SpyPress
Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204: User Execution	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4918</u>		Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*	-
Mozilla Firefox Out-of-Bounds Read or Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-125	T1059: Command and Scripting Interpreter, T1059.007: JavaScript	https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/ https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/ https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-4919</u>		Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*	-
Mozilla Firefox Out-of-Bounds Read or Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787 CWE-125	T1203: Exploitation for Client Execution, T1055: Process Injection	https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/ https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/ https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-0199</u>		Microsoft Office and WordPad	SideWinder
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:microsoft_office:*.:.:.:.:.:.:.*	StealerBot
Microsoft Office and WordPad Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows:*.:.:.:.:.:.:.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199





CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-11882</u>		Microsoft Office	SideWinder
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:office:-*.:.:.:.*.*	StealerBot
Microsoft Office Memory Corruption Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID	T1203: Exploitation for Client Execution, T1190: Exploit Public-Facing Application, T1055: Process Injection	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882
	CWE-119		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-0994</u>		Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10	UAT-6382
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:trimble:cityworks:*.~*~*~*~*~*~*	TetraLoader
Trimble Cityworks Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-502	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	Trimble Cityworks version 15.8.9 and Cityworks with office companion version 23.10

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-31324</u>		SAP NetWeaver Version 7.50	UNC5221, UNC5174, CL-STA-0048
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sap:sap_netweaver:7.50.*~*~*~*~*~*~*	KrustyLoader, Qilin ransomware, BianLian, RansomExx, PipeMagic
SAP NetWeaver Unrestricted File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1505: Server Software Component, T1505.003: Web Shell	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32432</u>		Craft CMS	Mimo (aka Hezb)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:craftcms:craft_cms:*.*.*.*.*.*.*.*	XMRig
Craft CMS Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-58136</u>		Yiiframework Yii	Mimo (aka Hezb)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:yiiframework:yii:*.*.*.*.*.*.*.*	XMRig
Yiiframework Yii Improper Protection of Alternate Path Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1068: Exploitation for Privilege Escalation	https://github.com/yiisoft/yii2/pull/20232

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-47577</u>		TemplateInvaders TI WooCommerce Wishlist Plugin versions upto 2.9.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:templateinvaders:ti_woocommerce_wishlist_plugin:*:*:*:*:*	-
TemplateInvaders TI WooCommerce Wishlist Plugin Unrestricted File Type Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-434	T1059: Command and Scripting Interpreter, T1485: Data Destruction, T1190: Exploit Public-Facing Application	

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StealC V2	<p>StealC V2 is an enhanced version of the popular StealC information stealer, first observed in March 2025. This updated variant introduces a streamlined command-and-control (C2) protocol using a JSON-based format, with recent versions incorporating RC4 encryption to secure communication. It features a versatile loader capable of delivering payloads via Microsoft Software Installer (MSI) packages and PowerShell scripts. StealC V2 expands its data theft capabilities with multi-monitor screenshot capture and a unified file grabber that targets a wide array of applications, including cryptocurrency wallets, gaming platforms, messaging apps, email clients, VPNs, and browsers. Additionally, it supports server-side brute-force functionality for credential harvesting.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Data Theft	-
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 CVEs
<u>More_eggs</u>	More_eggs, also known as SpicyOmelette, is a versatile backdoor malware designed to give attackers remote access to compromised systems. Its modular nature allows threat actors to use it for a range of malicious activities, such as data theft, system surveillance, and delivering additional malware. More_eggs enables attackers to craft highly customized lures and payloads that align closely with the intended victim, increasing the chances of successful compromise.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Venom Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Grixba</u>	Grixba is an infostealer tool used by attackers to scan networks and enumerate all users and computers within a targeted domain. Typically employed in the early stages of an attack, Grixba helps adversaries map out the environment, identify potential targets, and gather valuable information that can facilitate lateral movement, privilege escalation, or data theft.	Exploiting Vulnerability	CVE-2025-29824
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Steal Data	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

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 CVEs
<u>DragonForce</u>	<p>DragonForce ransomware is a financially motivated extortion tool designed to encrypt victims' files and demand payment for their recovery. Once a system is compromised, the ransomware appends encrypted files with extensions such as .dragonforce_encrypted or .cyberbears, signaling successful infection.</p> <p>Victims receive a ransom note stating that their data has been both stolen and encrypted, with attackers emphasizing their monetary intent rather than any political agenda. The note directs victims to contact the group via a Tor website or TOX ID, where they are offered a list of exfiltrated files and a free decryption of one file as proof of the attackers' capabilities.</p>	Exploiting Vulnerabilities, Phishing	CVE-2021-44228, CVE-2023-46805, CVE-2024-21412, CVE-2024-21887, CVE-2024-21893, CVE-2022-26134
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data, Data Theft	<p>Apache Log4j2, Ivanti Connect Secure and Policy Secure, Microsoft Windows Internet Shortcut Files, Pulse Connect Secure, ZTA gateways, Pulse Policy Secure, Atlassian Confluence Server and Data Center</p>
ASSOCIATED ACTOR			<p>PATCH LINK</p> <p>https://logging.apache.org/security.html , https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412 , https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US , https://jira.atlassian.com/browse/CONFSERVER-79016</p>

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 CVEs
<u>NOOPDOOR</u>	<p>NOOPDOOR is a stealthy and sophisticated backdoor that has been exclusively used by the threat group Earth Kasha since at least 2021. Engineered for covert command-and-control (C&C) communication, NOOPDOOR leverages the DNS-over-HTTPS (DoH) protocol to obscure IP address lookups, making its network activity harder to detect. It comes pre-configured with public DoH-compatible DNS servers like Google and Cloudflare, allowing it to bypass traditional DNS monitoring and blend in with normal encrypted web traffic, significantly enhancing its stealth and persistence within compromised environments.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Earth Kasha			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ANEL</u>	<p>ANEL, also known as UPPERCUT, is a backdoor that exists solely in an encrypted form on disk. Its decrypted DLL is only loaded into memory after being decrypted by a loader in preparation for execution. ANEL communicates with its command-and-control (C&C) server over HTTP, using encryption to protect transmitted data from potential interception. It supports basic commands for file manipulation, payload execution, and screenshot capture.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATE D ACTOR			PATCH LINK
Earth Kasha			-

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 CVEs
<u>ROAMINGMOUSE</u>	ROAMINGMOUSE is a macro-enabled malicious Excel dropper used by Earth Kasha as the initial infection vector. It employs a simple sandbox evasion technique that requires user interaction to activate its malicious routine, helping it avoid detection in automated analysis environments. Once executed, ROAMINGMOUSE decodes an embedded ZIP archive encoded in Base64, drops it onto the disk, and extracts its contents to deploy ANEL malware components, paving the way for further compromise and persistence.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Dropper		Drops another malware	-
ASSOCIATED ACTOR			PATCH LINK
Earth Kasha			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Agenda (aka Qilin, Water Galura)</u>	The Agenda ransomware group, also known as Qilin, has been an active and evolving cyber threat since it was first identified in July 2022. Initially developed in the Go programming language, the ransomware has since transitioned to Rust, a move that enhances its performance, stealth, and resistance to reverse engineering. The newer Rust-based variants include advanced capabilities such as remote execution, improved spread within virtualized environments, and evasion techniques specifically designed to bypass modern security defenses	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data, Data Theft	-
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 CVEs
<u>SmokeLoader</u>	SmokeLoader is a versatile malware loader designed to deploy additional threats on infected systems while offering optional modules for information stealing. It frequently obscures its C2 traffic by generating requests to legitimate websites, making detection more challenging. Once installed, SmokeLoader can deliver various payloads, including cryptominers, ransomware, and password stealers. Beyond deploying malware, it may also exfiltrate sensitive data, corrupt files, and disrupt system operations, posing a significant risk to compromised devices.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft, System compromise and Espionage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>NETXLOADER</u>	NETXLOADER is a stealthy, .NET-compiled loader designed to deliver additional malicious payloads such as Agenda ransomware and SmokeLoader. Operating discreetly in the background, it attempts to load assemblies by name, enabling the execution of follow-on malware without raising immediate suspicion. Its use of the .NET framework allows for flexible payload delivery and evasion of traditional detection mechanisms, making it a valuable tool in multi-stage attack chains.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Loads another malwares	-
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 CVEs
Crimson	Crimson Malware is a remote access trojan used by APT36 to spy on Indian government and military entities. It steals data, monitors activity, and spreads via phishing emails with malicious attachments.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote Control, Data Theft	Linux
ASSOCIATED ACTOR			PATCH LINK
APT36			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Poseidon	Poseidon is a powerful Linux backdoor used by APT36 to infiltrate Indian government and defense networks, steal sensitive data, and maintain remote control over compromised systems, often delivered through trojanized versions of the Kavach authentication tool.	Kavach 2FA tool	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data theft, Compromise systems	Linux
ASSOCIATED ACTOR			PATCH LINK
APT36			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ElizaRAT	ElizaRAT is a remote access trojan (RAT) targeting Windows systems, first identified in 2024. It is primarily spread through phishing emails and malicious attachments. The malware enables attackers to steal credentials, capture screenshots, and remotely control infected devices.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote Control, 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
PupkinStealer	PupkinStealer is a lightweight but dangerous malware that quietly steals browser passwords, Telegram and Discord session data, desktop files, and screenshots. Once executed, it zips up the stolen info and exfiltrates it via a Telegram bot, making it a stealthy threat aimed at quick data theft and account hijacking.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Infostealer		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mirai	Mirai is a well-known malware that targets Internet of Things (IoT) devices by exploiting weak or default passwords. Once infected, these devices are added to a botnet to carry out large-scale Distributed Denial of Service (DDoS) attacks. Its open-source release has led to the creation of several variants.	Exploiting vulnerabilities	CVE-2024-11120 CVE-2024-6047
TYPE		IMPACT	AFFECTED PRODUCT
Botnet		Network Overload, Compromise systems	GeoVision Devices
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>LZRD</u>	LZRD is a Mirai-based malware botnet variant that actively exploits vulnerabilities in GeoVision IoT devices and other platforms to infect and control large numbers of devices. It uses command injection attacks to download and execute its payload, enabling a range of DDoS attack methods.	Exploiting vulnerabilities	CVE-2024-11120 CVE-2024-6047
TYPE		IMPACT	AFFECTED PRODUCT
Botnet		Network Overload, Compromise systems	GeoVision Devices
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TransferLoader</u>	TransferLoader is a sophisticated malware loader active since at least February 2025, featuring embedded components like a downloader, backdoor, and backdoor loader. It enables attackers to execute arbitrary commands, deploy additional payloads such as ransomware, and evade detection through advanced anti-analysis techniques.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Loader		Malware execution, Data theft	-
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 CVEs
SpyPress	SpyPress is a collection of JavaScript payloads designed to target various webmail platforms. Each version connects to a group of hardcoded command-and-control (C2) servers, using obfuscated JavaScript and standard HTTP POST requests to stealthily extract sensitive data.	Loaded by the XSS Vulnerabilities	CVE-2023-43770 CVE-2020-35730 CVE-2024-11182 CVE-2024-27443
		IMPACT	AFFECTED PRODUCTS
TYPE Information Stealer		Sensitive Data Exfiltration	Roundcube Webmail, MDAemon Email Server, Zimbra Collaboration (ZCS)
ASSOCIATED ACTOR APT28			PATCH LINKS https://roundcube.net/news/2023/09/15/security-update-1.6.3-released , https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13 , https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html , https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes

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 CVEs
<u>LOSTKEYS</u>	LOSTKEYS can steal files from specific directories and file types defined in its code. It also sends system information and a list of running processes back to the attacker.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Targeted File Theft	-
Information Stealer			PATCH LINK
ASSOCIATED ACTOR			
COLDRIVER			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>StealerBot</u>	StealerBot is a credential stealer that collects system information, checks for antivirus software, and exfiltrates data to attackers. It uses techniques like Base64 encoding, XOR encryption, and hides in DLLs loaded by trusted Windows applications, blending classic espionage tactics with cybercrime-driven credential theft.	Spearphishing Attachment	CVE-2017-0199 CVE-2017-11882
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, System Profiling, and Security Evasion	Microsoft Office and WordPad
Credential Stealer			PATCH LINKS
ASSOCIATED ACTOR			
SideWinder			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

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 CVEs
<u>Interlock</u>	INTERLOCK is an emerging ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. While the Windows variant is most common, INTERLOCK stands out for its rare focus on FreeBSD. The group employs refined double-extortion tactics and runs a leak site called “Worldwide Secrets Blog” to publish stolen data and pressure victims into negotiations.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Financial Loss, Data Encryption, and Operational Disruption	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nitrogen</u>	The Nitrogen ransomware group runs a highly active and aggressive campaign. Similar to the earlier LukaLocker ransomware, it uses a double-extortion model. Its threat comes from both encrypting critical data and using legitimate system tools to bypass defenses and evade detection.	Malvertising Campaigns	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Financial Loss, Data Encryption, and Operational Disruption	Windows
Ransomware			PATCH LINK
ASSOCIATED ACTOR			
-			-

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 CVEs
<u>PureHVNC</u>	PureHVNC is a customized Remote Access Trojan (RAT) that gives attackers full control over infected systems. Often obfuscated with .NET Reactor, it enables keylogging, data theft, and remote desktop access for surveillance and system control.	Malvertising Campaigns	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Full Remote Control, Information Theft	-
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PureRAT</u>	PureRAT is a remote access trojan that communicates with its command-and-control (C2) servers using encrypted, protobuf-formatted data. It collects detailed system information such as OS version, antivirus status, device IDs, and IP address. Built for stealth and persistence, PureRAT can execute commands to self-delete, restart, or shut down the host. It also monitors active applications for specific keywords like “password,” “bank,” or “WhatsApp,” making it especially invasive.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Full System Surveillance, Data Collection and Exfiltration	-
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-

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 CVEs
<u>PureLogs</u>	PureLogs is a potent information stealer that extracts sensitive data from browsers, email clients, messaging apps, VPNs, and cryptocurrency wallets. In addition to data theft, it functions as a downloader, allowing attackers to deploy additional payloads after infection. This dual capability increases its threat level, especially in enterprise environments, where it can enable long-term access and follow-up attacks.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Extensive Data Theft, Payload Deployment	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PureCrypter</u>	PureCrypter functions as a loader, downloading disguised payloads often masked as harmless media files then decrypting and executing them directly in memory to evade disk-based detection. It maintains persistence by copying itself to %AppData% as "Action.exe" and adding a startup script to run automatically at each reboot.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Malware Deployment, Persistent Access	-
Loader			PATCH LINK
ASSOCIATED ACTOR			
-			-

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>TetraLoader</u>	TetraLoader is a custom loader built on the MaLoader framework, written in Simplified Chinese. It allows attackers to package shellcode and other payloads within Rust-based binaries, enabling stealthy deployment of advanced tools while avoiding detection.	Exploiting Vulnerability	CVE-2025-0994
TYPE		IMPACT	AFFECTED PRODUCT
Loader		Payload Delivery	Trimble Cityworks
ASSOCIATED ACTOR			PATCH DETAILS
UAT-6382			Trimble Cityworks version 15.8.9 and Cityworks with office companion version 23.10

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>KrustyLoader</u>	KrustyLoader is a Rust-based malware loader designed to deliver backdoors during post-exploitation. It focuses on evading detection and maintaining persistence on compromised Linux systems. Upon execution, it performs anti-analysis and environment checks to avoid discovery.	Exploiting Vulnerability	CVE-2025-31324
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Backdoor Deployment, Persistent Access	SAP NetWeaver
ASSOCIATED ACTOR			PATCH LINK
UNC5221			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.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>Qilin</u>	Qilin ransomware was originally developed in Go but has since transitioned to Rust, improving its performance, stealth, and resistance to reverse engineering. The Rust-based variants feature advanced capabilities like remote execution, enhanced propagation in virtualized environments, and sophisticated evasion techniques to bypass modern security defenses.	Exploiting Vulnerability	CVE-2025-31324
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data Encryption and Operational Disruption	SAP NetWeaver
ASSOCIATED ACTOR			PATCH LINK
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>BianLian</u>	BianLian is a ransomware group steadily expanding its victim base, demonstrating advanced operational security and expertise in network infiltration. Notably, it has shifted its focus from encrypting files to leveraging data-leak extortion.	Exploiting Vulnerability	CVE-2025-31324
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data Theft and Exposure	SAP NetWeaver
ASSOCIATED ACTOR			PATCH LINK
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.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>RansomExx</u>	RansomExx is a ransomware variant operating under a ransomware-as-a-service (RaaS) model, recently redeveloped in Rust to enhance stealth and reduce detection by antivirus solutions.	Exploiting Vulnerability	CVE-2025-31324
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware			SAP NetWeaver
ASSOCIATED ACTOR			PATCH LINK
-		Data Encryption and Operational Disruption	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>PipeMagic</u>	PipeMagic is an advanced backdoor Trojan crafted in Rust. It employs encrypted communication via named pipes, granting attackers remote access and facilitating subsequent infections such as ransomware deployment or data exfiltration.	Exploiting Vulnerability	CVE-2025-31324
TYPE		IMPACT	AFFECTED PRODUCT
Trojan			SAP NetWeaver
ASSOCIATED ACTOR			PATCH LINK
-		Remote Control, Data Exfiltration and Data Theft	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.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>Vidar</u>	Vidar is a variant of the Arkei malware, designed to exploit legitimate platforms like Steam and Telegram as Dead Drop Resolvers (DDR) to hide its command-and-control (C&C) server details. It harvests sensitive data from web browsers and digital wallets, making it a serious threat by enabling the theft of personal information and cryptocurrency.	Social Engineering via AI-generated TikTok videos	-
TYPE		IMPACT	AFFECTED PRODUCT
Stealer		Data Theft, C&C Obfuscation	TikTok
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>StealC</u>	Stealc is developed in C and leverages WinAPI functions. It primarily targets data from web browsers, browser extensions, desktop cryptocurrency wallets, and other applications.	Social Engineering via AI-generated TikTok videos	-
TYPE		IMPACT	AFFECTED PRODUCT
Stealer		Credential Theft, Data Exposure	TikTok
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>Dero</u>	The Dero cryptocurrency miner, developed in Golang and packed with UPX, is part of an ongoing mining campaign that targets exposed Docker APIs. It hijacks vulnerable environments, converting containers into botnet nodes to propagate the infection and mine cryptocurrency.	Exploit Public-Facing Application	-
TYPE		IMPACT	AFFECTED PRODUCT
Cryptominer		Resource Drain, Infrastructure Hijacking, Reputation Damage	Windows, Linux
ASSOCIATED ACTOR			PATCH LINK
-			-


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XMRIg</u>	XMRIg is an open-source cryptocurrency miner commonly used to mine Monero (XMR). Cybercriminals frequently leverage it in cryptojacking attacks, covertly exploiting victims’ computing resources to generate cryptocurrency.	Exploiting Vulnerabilities	CVE-2025-32432 CVE-2024-58136
TYPE		IMPACT	AFFECTED PRODUCT
Crypto miner		Operational Disruption, Financial Loss	Craft CMS, Yiiframework Yii
ASSOCIATED ACTOR			PATCH LINK
Mimo			https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47 , https://github.com/yiisoft/yii2/pull/20232


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>TOUGHPROGRESS</u>	TOUGHPROGRESS is an advanced malware framework focused on stealth, persistence, and control. It uniquely uses Google Calendar as a command-and-control (C2) channel by embedding encrypted payloads in event descriptions. With a modular design, it deploys three sequential payloads, each performing specific functions and employing evasion techniques like memory-resident execution, encryption, compression, process hollowing, and control flow obfuscation.	Spear-phishing Attachment	-
TYPE		IMPACT	AFFECTED PRODUCT
Framework		Persistent System Compromise, Data Theft and Espionage	-
ASSOCIATED ACTOR			PATCH LINK
APT41			-


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 COUNTRIES
 <u>RomCom (aka Storm-0978, Tropical Scorpis, Void Rabisu, DEV-0978, UNC2596, UAC-0180)</u>	Russia	Retail, Hospitality, and CNI (Critical National Infrastructure) sectors	UK
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; T1036: Masquerading; T1036.008: Masquerade File Type; T1199: Trusted Relationship; T1497: Virtualization/Sandbox Evasion; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1566: Phishing; T1566.002: Spearphishing Link; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1585: Establish Accounts; T1585.002: Email Accounts; T1587: Develop Capabilities; T1587.002: Code Signing Certificates; T1588: Obtain Capabilities; T1588.007: Artificial Intelligence; T1656: Impersonation; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Venom Spider (aka Golden Chickens, badbullz, badbullzvenom)</u>	Russia	Hiring Managers	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	More_eggs	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.007: JavaScript; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1027.013: Encrypted/Encoded File; T1027.014: Polymorphic Code; T1105: Ingress Tool Transfer; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1518: Software Discovery; T1518.001: Security Software Discovery; T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Earth Kasha (aka MirrorFace, Operation LiberalFace)</u></p>	China	Government and Public Sector organizations	Taiwan and Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	NOOPDOOR, ANEL, ROAMINGMOUSE	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1047: Windows Management Instrumentation; T1071: Application Layer Protocol; T1071.004: DNS; T1547: Boot or Logon Autostart Execution; T1036: Masquerading; T1204: User Execution; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1574: Hijack Execution Flow; T1574.001: DLL; T1497: Virtualization/Sandbox Evasion; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1113: Screen Capture; T1057: Process Discovery; T1572: Protocol Tunneling; T1637: Dynamic Resolution; T1637.001: Domain Generation Algorithms			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u>APT36 (alias Mythic Leopard, Transparent Tribe, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156)</u></p>	Pakistan	Government, Military, Defense, Aerospace, Education, Media, Energy, Telecommunications	India
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Crimson RAT, Poseidon, ElizaRAT	Windows, Linux, Android


TTPs


TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1598: Phishing for Information; T1070: Indicator Removal; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1430: Location Tracking; T1409: Stored Application Data; T1115: Clipboard Data; T1573: Encrypted Channel; T1071: Application Layer Protocol; T1598.003: Spearphishing Link; T1583.001: Domains; T1566.001: Spearphishing Attachment; T1204.001: Malicious Link; T1059.005: Visual Basic; T1547.001: Registry Run Keys /Startup Folder; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1005: Data from Local: System; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel; T1218.005: Mshta; T1071.001: Web Protocols; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1036.005: Match Legitimate Name or Location; T1070.004: File Deletion; T1056.001: Keylogging; T1583: Acquire Infrastructure; T1027.013: Encrypted/Encoded File; T1566.002: Spearphishing Link; T1608.004: Drive-by Target; T1608: Stage Capabilities


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Marbled Dust (alias Silicon, Cosmic Wolf, Sea Turtle, Teal Kurma, UNC1326)</u></p>	Turkey	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2025-27920	-	Output Messenger
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA0042: Resource Development; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1037: Boot or Logon Initialization Scripts; T1036: Masquerading; T1212: Exploitation for Credential Access; T1046: Network Service Discovery; T1071.004: DNS; T1041: Exfiltration Over C2 Channel; T1082: System Information Discovery; T1027: Obfuscated Files or Information; T1587.004: Exploits; T1574: Hijack Execution Flow; T1587: Develop Capabilities			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>APT28 (aka Sednit group, Sofacy, Fancy Bear, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)</u></div>	Russia	Governmental Entities, Defense Companies, Telecommunication, Academic, Military, Transport	Eastern Europe, Governments in Africa, Europe, and South America
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2023-43770 CVE-2020-35730 CVE-2024-11182 CVE-2024-27443	SpyPress	Roundcube Webmail, MDaemon Email Server, Zimbra Collaboration (ZCS)
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1587: Develop Capabilities; T1587.004: Exploits; T1587.001: Malware; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1027: Obfuscated Files or Information; T1187: Forced Authentication; T1556: Modify Authentication Process; T1556.006: Multi-Factor Authentication; T1087: Account Discovery; T1087.003: Email Account; T1056: Input Capture; T1056.003: Web Portal Capture; T1119: Automated Collection; T1114: Email Collection; T1114.002: Remote Email Collection; T1114.003: Email Forwarding Rule; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1071.003: Mail Protocols; T1132: Data Encoding; T1132.001: Standard Encoding; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1566: Phishing; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpreter; T1059.007: JavaScript			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <p><u>COLDRIVER (aka Star Blizzard, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, UNC4057)</u></p>	Russia	Governments, Militaries, Journalists, Think Tanks, NGOs	Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine, United Kingdom, United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANS OMWARE	AFFECTED PRODUCTS
	-	LOSTKEYS	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1027: Obfuscated Files or Information; T1497.001: System Checks; T1497: Virtualization/Sandbox Evasion; T1082: System Information Discovery; T1057: Process Discovery; T1005: Data from Local System; T1119: Automated Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <p><u>SideWinder (aka Rattlesnake, Razor Tiger, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)</u></p>	India	Government Institutions, Military Institutions, Banking	Sri Lanka, Bangladesh and Pakistan
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	TARGETED CVE		
	CVE-2017-0199 CVE-2017-11882	StealerBot	Microsoft Office and WordPad
TTPs			
TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1036: Masquerading; T1656: Impersonation; T1590: Gather Victim Network Information; T1218.011: Rundll32; T1140: Deobfuscate/Decode Files or Information; T1082: System Information Discovery; T1132: Data Encoding; T1132.001: Standard Encoding; T1518: Software Discovery; T1518.001: Security Software Discovery; T1027: Obfuscated Files or Information; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <u>UAT-6382</u>	Chinese-speaking	Government	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2025-0994	TetraLoader	Trimble Cityworks
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1505: Server Software Component; T1505.003: Web Shell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1074: Data Staged; T1041: Exfiltration Over C2 Channel; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1588.005: Exploits; T1505.004: IIS Components; T1588.006: Vulnerabilities			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 UNC5221 (aka UTA0178, Red Dev 61)	China	Government, Finance, Oil and Gas	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2025-31324	KrustyLoader	SAP NetWeaver
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0003: Persistence; TA0011: Command and Control; T1068: Exploitation for Privilege Escalation; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1588.005: Exploits; T1588.006: Vulnerabilities; T1070.004: File Deletion; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1204: User Execution; T1059: Command and Scripting Interpreter			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 UNC5174 (aka Uteus)	China	Government, Finance, Oil and Gas	Worldwide
	MOTIVE		
	Espionage, Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2025-31324	-	SAP NetWeaver
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; T1105: Ingress Tool Transfer; T1136: Create Account; T1059: Command and Scripting Interpreter; T1531- Account Access Removal; T1190: Exploit Public-Facing Application; T1082: System Information Discovery; T1083: File and Directory Discovery			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>CL-STA-0048</u>	China	Government, Finance, Oil and Gas	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-31324	-	SAP NetWeaver

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1204: User Execution; T1059: Command and Scripting Interpreter; T1547: Boot or Logon Autostart Execution; T1548: Abuse Elevation Control Mechanism; T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1562: Impair Defenses; T1003: OS Credential Dumping; T1552: Unsecured Credentials; T1083: File and Directory Discovery; T1057: Process Discovery; T1570: Lateral Tool Transfer; T1021: Remote Services; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1048: Exfiltration Over Alternative Protocol; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>Void Blizzard (aka Laundry Bear)</u></div>	Russia	Aviation, Defense, Education, Government, Healthcare, IT, Law Enforcement, Media, NGO, Telecommunications, Transportation	North America, Europe, NATO Members
	MOTIVE		
	Information theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1557: Adversary-in-the-Middle; T1204: User Execution; T1204.002: Malicious File; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.002: Tool; T1110.003: Password Spraying; T1550.004: Web Session Cookie; T1552.001: Credentials In Files; T1087: Account Discovery; T1087.004: Cloud Account; T1018: Remote System Discovery; T1082: System Information Discovery; T1114: Email Collection; T1114.002: Remote Email Collection; T1530: Data from Cloud Storage; T1119: Automated Collection; T1071.001: Web Protocols			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div>Mimo (aka Hezb)</div>	-	Finance	Worldwide
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-32432 CVE-2024-58136	XMRig	Craft CMS, Yiiframework Yii
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0003: Persistence; TA0011: Command and Control; TA0005: Defense Evasion; TA0040: Impact; T1588: Obtain Capabilities; T1588.005: Exploits; T1543: Create or Modify System Process; T1588.006: Vulnerabilities; T1204: User Execution; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1564: Hide Artifacts; T1070: Indicator Removal; T1071: Application Layer Protocol; T1496: Resource Hijacking; T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u>APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)</u></p>	China	Governments, Shipping, Logistics, Media, Technology, Automotive	Worldwide
	MOTIVE		
	Financial crime, Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	TOUGHPROGRESS	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1036.008: Masquerade File Type; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1005: Data from Local System; T1027.005: Indicator Removal from Tools; T1620: Reflective Code Loading; T1055: Process Injection; T1055.012: Process Hollowing; T1102: Web Service; T1001: Data Obfuscation; T1041: Exfiltration Over C2 Channel			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	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
		T1078.004: Cloud Accounts
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1106: Native API	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	
	T1133: External Remote Services	
	T1136: Create Account	
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.013: PowerShell Profile
		T1053.003: Cron
		T1078.001: Default Accounts

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	
	T1068: Exploitation for Privilege Escalation	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1611: Escape to Host	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.005: Indicator Removal from Tools
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.009: Clear Persistence
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1127: Trusted Developer Utilities Proxy Execution	
	T1134: Access Token Manipulation	T1134.002: Create Process with Token
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1553: Subvert Trust Controls	
	T1556: Modify Authentication Process	T1556.006: Multi-Factor Authentication
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.009: Safe Mode Boot
	T1564: Hide Artifacts	
	T1574: Hijack Execution Flow	
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	T1110.003: Password Spraying
	T1187: Forced Authentication	
	T1212: Exploitation for Credential Access	
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.007: Container API
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
TA0007: Discovery	T1007: System Service Discovery	
	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	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.003: Email Account
		T1087.004: Cloud Account
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1614: System Location Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1072: Software Deployment Tools	
	T1210: Exploitation of Remote Services	
TA0009: Collection	T1005: Data from Local System	
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.002: Remote Email Collection
		T1114.003: Email Forwarding Rule
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	
	T1056: Input Capture	T1056.003: Web Portal Capture

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1001: Data Obfuscation	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.003: Mail Protocols
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
TA0040: Impact	T1573: Encrypted Channel	
		T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1491: Defacement	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
TA0042: Resource Development	T1529: System Shutdown/Reboot	
	T1531: Account Access Removal	
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.004: Server
		T1583.008 : Malvertising
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1585: Establish Accounts	
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.003: Code Signing Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
TA0043: Reconnaissance	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.004: Drive-by Target
	T1590: Gather Victim Network Information	T1590.002: DNS
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1598.003: Spearphishing Link

Top 5 Takeaways

#1

In May 27 zero-day vulnerabilities were observed, with so-called “Celebrity Vulnerabilities” taking center stage. Among them was **Log4Shell**, which continues to be exploited to deploy ransomware such as **DragonForce**.

#2

Ransomware attacks are on the rise, driven by aggressive variants like **DragonForce**, **Agenda**, **Interlock**, **Nitrogen**, **Qilin**, **BianLian**, and **RansomExx**. As these threats grow more sophisticated, organizations must act swiftly by strengthening defenses, securing backups, and refining disaster recovery plans, to stay ahead of the threat landscape.

#3

Cyberattacks were reported across **222** countries in May, with the **United States**, **United Kingdom**, **Germany**, and **Italy** bearing the brunt. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region remained untouched as adversaries expanded their global reach.

#4

The **Government**, **Financial**, **Defense**, and **Media** sectors were prime targets, enduring waves of ransomware attacks, data theft, and cyber espionage. As threat actors continue to refine their tactics, organizations in these industries must adopt proactive and adaptive security strategies.

#5

A wide range of malware families has also been observed actively targeting victims in real-world environments. These include **Grixba**, **PipeMagic**, **Poseidon**, **ElizaRAT**, **SpyPress**, **LOSTKEYS**, and **StealerBot**.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **37 significant vulnerabilities** and block the indicators related to the **15 active threat actors**, **37 active malware**, and **191 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 **37 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>StealC V2</u>	SHA256	0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c, e205646761f59f23d5c8a8483f8a03a313d3b435b302d3a37061840b5cc084c3, a1b2aecdd1b37e0c7836f5c254398250363ea74013700d9a812c98269752f385, 27c77167584ce803317eab2eb5db5963e9dfa86450237195f5723185361510dc, 87618787e1032bbf6a6ca8b3388ea3803be20a49e4afaba1df38a6116085062f
	URLs	hxxp[:]//45[.]93[.]20[.]64/c090b39aa5004512[.]php, hxxp[:]//45[.]93[.]20[.]28/3d15e67552d448ff[.]php, hxxp[:]//88[.]214[.]48[.]93/ea2cb15d61cc476f[.]php
<u>More_eggs</u>	MD5	ec103191c61e4c5e55282f4ffb188156, ebb5fb96bf2d8da2d9f0f6577766b9f1, 2da2f53ffd9969aa8004d0e1060d2ed1, 17158538b95777541d90754744f41f58, 46f142198eeeadc30c0b4ddfbf0b3ffd, b1e8602e283bbddf52df642dd460a2a2
	SHA256	f7a405795f11421f0996be0d0a12da743cc5aaf65f79e0b063be6965c8fb8016, 2fef6c59fbf16504db9790fcc6759938e2886148fc8acab84dbd4f1292875c6c,
<u>More_eggs</u>	SHA256	0af266246c905431e9982deab4ad38aaa63d33a725ff7f7675eb23dd75ca4d83, f873352564a6bd6bd162f07eb9f7a137671054f7ef6e71d89a1398fb237c7a7b, 184788267738dfa09c82462821b1363dbec1191d843da5b7392ee3add19b06fb, ccb05ca9250093479a6a23c0c4d2c587c843974f229929cd3a8acd109424700d
<u>Grixba</u>	SHA256	6030c4381b8b5d5c5734341292316723a89f1bdbd2d10bb67c4d06b1242afd05
<u>DragonForce</u>	SHA1	343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c,

Attack Name	TYPE	VALUE
<u>DragonForce</u>	SHA1	229e073dbcb72bdfee2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4, 577b110a8bfa6526b21bb728e14bd6494dc67f71, 7db52047c72529d27a39f2e1a9ffb8f1f0ddc774, 81185dd73f2e042a947a1bf77f429de08778b6e9, a4bdd6cef0ed43a4d08f373edc8e146bb15ca0f9, b571e60a6d2d9ab78da1c14327c0d26f34117daa, e1c0482b43fe57c93535119d085596cd2d90560a, eada05f4bfd4876c57c24cd4b41f7a40ea97274c, fc75a3800d8c2fa49b27b632dc9d7fb611b65201
	TOR Address	3pktcrbcmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion, , ljbw7iiodqzpg6ooewbgn6mv2pinoer3k5pzdecoejsw5nyoe73zvad[.]onion, n, Kfgjwkho24xiwckcf53x7qyruobbkhx4eqn2c6oe4hprbn23rcp6qcqd[.]onion, n, Rnc6scfbqslz5aqxfg5hrjel5qomxsclltc6jvhahi6qwt7op5qc7iad[.]onion, rrrbay3nf4c2wxmhprc6eotjlpqeowfuobodic4x4nzqtosx3ebirid[.]onion,rr rbayguhgtgxdg5myxkdc2cxei25u6brknfqkl3a35nse7f2arblyd[.]onion, rrrbaygxp3f2qtgvf6ffhdm24ucxvbr6mhmhsga4faefqyd77w7tqd[.]onion, Z3wqggtxft7id3ibr7sriuv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion
	Tox ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA5 5F4A856D90A65E99D20, 258C79F73CCC1E56863030CD02C2C7C4347F80CAD43DD6A5B219A618F D17853C7BB1029DAE31
	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd6002 50a9
<u>NOOPDOOR</u>	SHA256	7fb4c9f041d4411311437e12427aaf09d369bc384faa2de4b5bc8ae36a42 190e, 4f3ec89d5ea0a513afa3f49434f67b7e1540a4a8a93d078def950bd94d444 723
<u>ANEL</u>	SHA256	362b0959b639ab720b007110a1032320970dd252aa07fc8825bb48e8fdd 14332, 78f7b98b1e6f089f5789019dab23ac38f77c662fd651ee212d8451ee61b2f c0c
<u>ROAMINGMO USE</u>	SHA256	1e0a7737a484699d035c0568771c4834c0ff3fb9ba87aded3c86705e10e9 bb0e, 2110b9a4c74d1c8be1aed6ebcff2351cad3d16574026fe4697a9c70810fb1 d9e, 488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e5 8dd2,

Attack Name	TYPE	VALUE
<u>ROAMINGMO USE</u>	SHA256	517ef26be8b9fb1af0e9780b244827af4937ad2fa4778a0bd2d9c65502ce54e1, 63e813b5bf94bdec9ce35c9d7311f76c3a35728d158ade0a6487fc99c73dcf31, 69e2a259e0136b61a3acad3f8fad2c012c75c9d8e26e66a3f0af1e7c23506b5c, 6edf72495e03ca757fa55beb2ea02492f2e7a4b85ca287a9d08bbe60e390c618, 705e5f1245e59566895b1d456aee32d4bff672a6a00f2cd390d7d50c12316dee, 712b81f1a82b9ea9a304220ed87c47c329392c2ce040ed3bff936fe33456acff, 72ece359a3c6f286d174b9cccc7c963577749e38e28f5ecf00dd4c267478a693, 75d6f82962f380f7726142490068879240c3c507427f477cf25268b524c30339, 7b61ed1049ba5f5b8d9725f32cff1ef1e72ef46e2a1dd87bd2b33e73e7333f44, 8cdcd674a0269945dd4c526b5868efb6df8854a127fd5449e57e89905511391d, 9569c4044f8cf32bc9a0513ed7c4497bb6ab71b701c53e58719ef259b3716751, 9c24b60574f39b0565442a79a629a2944672f56acca555e81275e5079382d98b, 9e4c155f4d096d9a0529e83fd21197f3dba20cc4eef48045fd018334384dd513, a12a34d329ccc305dca2306e2d698945f1413c013fe99d4bb069db2127f47806, a14c9ae22ca8bdb4971a03f61b2bcc5f140abb51c6922ab7c92ea09ee14dd3bd, a347e1efbfca3722c9e8cc86eba3b288f7e4fae9d386f2a8969faffb125a74c5, ac8c36075ac0085c7d1e96b3fc08c15a151373186e564486dd91d2e49b2dd287, ad050545b65ecbb2178f678c654d84d14986a77051897927e56b5c2893c33608, b56aa48721cd1119a9e06ed9c2f923a1dda5f9aa079dc0e4fd66ab37e33649e8, cb0848d79d2eef76e1d4ff602e0844d03b614d4c25a1b5e3f0ae5c33ea5500b9, cf6ed83d7dcc13f500486044d1af606ceb12c387568ccbb498e01cc7d8005dbd, e123fa2abf1a2f12af9f1828b317d486d1df63aff801d591c5e939eb06eb4cfc, e5b99572581df7a5116511be3f03b9f1a90611235b8288d9f59141876adb1ef1, eeec3a94500ecd025ecdd559e15e4679e26c1347e534944721abe416b49f3871, f502102c5c598d5b9e24f689a3b09b1d2f6702226049a573c421b765867391b3, Fc8c574088af4f74cf84c5c04d522bb1665f548cb17c6192552eb9b783401009

Attack Name	TYPE	VALUE
<u>Agenda</u>	SHA1	f995ec5d88afab30f9efb62ea3b30e1e1b62cdc3,05bf016c137230bfdc6eaae95b75a56aff76799d
	SHA256	8518d0342196772a9e34447484ac5f4944d649f8aa96d36e9e6d47db3f041a78
<u>SmokeLoader</u>	SHA1	4684aa8ab09a70d0e25139286e1178c02b15920b,Bdf33e2ba85f35ea86fb016620371fe80855fe68
	URL	hxxp[:]//serverlogs295[.]xyz/statweb255/index[.]php, hxxp[:]//servblog475[.]cfd/statweb255/index[.]php, hxxp[:]//demblog797[.]xyz/statweb255/index[.]php, hxxp[:]//admlogs457[.]cfd/statweb255/index[.]php, hxxp[:]//blogmstat599[.]xyz/statweb255/index[.]php, hxxp[:]//bloglogs757[.]cfd/statweb255/index[.]php, hxxp[:]//pzh1966[.]com/statweb255/index[.]php, hxxp[:]//mxblog77.cfd/777/
<u>NETXLOADER</u>	SHA1	16b776ff80f08105b362f9bc76c73a21c51664c2,1399e63d4662076eed3b4498c2f958c611a4387
	SHA256	53895523bf8d64b4f8f10d0b38972ceaaed52d9c0486b34ad7cb53b5af017ac4
<u>Crimson</u>	MD5	026e8e7acb2f2a156f8afff64fd54066,fb64c22d37c502bde55b19688d40c803,70b8040730c62e4a52a904251fa74029,3efec6ffcbfe79f71f5410eb46f1c19e,b03211f6feccd3a62273368b52f6079d
	SHA256	d1a1eaefe6bd2e245bba369e966d7a8eab9ed6ad1fa827321e5889cc8d43f976
<u>Poseidon</u>	SHA256	541cefaad8d9554bdc5ce9cde24e4556c2444111ea13bd9965bd4a50e60f9265,682d5e53a456668f15809d9ab499651e1342fc602e7f5bc85e30fe29933f7634,7e2020c4a838bd7463478188bfaa97e66cf3365d3aef03f1b4398eaddacfc6b9
<u>ElizaRAT</u>	SHA256	b30a9e31b0897bfe6ab80aebcd0982eecf68e9d3d3353c1e146f72195cef0ef5,263f9e965f4f0d042537034e33699cf6d852fb8a52ac320a0e964ce96c48f5e5
<u>PupkinStealer</u>	MD5	fc99a7ef8d7a2028ce73bf42d3a95bce
	SHA256	9309003c245f94ba4ee52098dadbaa0d0a4d83b423d76c1bfc082a1c29e0b95f
<u>TransferLoader</u>	SHA256	b55ba0f869f6408674ee9c5229f261e06ad1572c52eaa23f5a10389616d62efe

Attack Name	TYPE	VALUE
Mirai	SHA256	f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714, 11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114, 8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e, ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516, 03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3, 0333c6ac43c6e977e9a1c5071194d3cf8aa01222194c6e7f2fd13e631d03522d, 7a8a46ace3b9261c2c7a399dcae037ce4f185f52f94b893d5bc00cd1228fb13a, 50c5b6c971c503240b91787d31f9314ded38d4f2700ff90deb032478b30aa0c5, bb2ab0879282c5c7f92a51e6482d3eb60a84ab184eca258ea550d9ed04bc5eda, 074a261bf281da36cc91cd13f86c7a8f75fdf96807d525c24b22c48fe01584a3, 5e721c013a6e8b2246aae86974f2163d3b57a7e6608a318ab84c44b1650e650a, de3c9ecb51564e4298ce7e4ff749be0a42d37824d2fd3d5b7fbab86a04105b88, aaba1ce1f182122a7ea05683623ab2d9bd05a3507e0dfc95e8e4165f629f80a8, 3f465182b5c594784e406a6a5de2f398bcc2e2ffc92d049a7990f37c267550a6, 3d6a544b1f03df23e734a65b9f1e808ff513ad881f09745a3959d696075c057e, 5180e3050a4a5cff52dcd8e8bb39fb6cf59a264a8fb6ddcc239615b340f1b99a, 2cc4d952856a8f2e1dd73b175d730d9cc7a04c73cf6452c8d0411eedf3aed5d5, dc21419b73566651b4c1e85879c0c98a4dcff8f7d206d9a97882200503658e9c, 866b2dbbd1978be007460835e8f3d2e02c1b321f856a18ba3e53030d4effe69a, 64ca8dd1a2702e0463bab19a0b826f79c55cfd46e4e1b41c6c33d7e7aa2c7530, 9f05425478d03e4a2fd5b990fe5625d93c468b80a3880bb52475aa7561548582, bf6984ccc9fb21beba3f492420901be0b0bace8d4530e6d2850f039622f1b96f, 58f7d61e3e474d5f5eccbba79556070220f52fa011b7cd24bdd96c23c338cd4b

Attack Name	TYPE	VALUE
<u>SpyPress</u>	SHA1	41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C, 1078C587FE2B246D618AF74D157F941078477579, F95F26F1C097D4CA38304ECC692DBAC7424A5E8D, B6C340549700470C651031865C2772D3A4C81310, 65A8D221B9ECED76B9C17A3E1992DF9B085CECD7, 8E6C07F38EF920B5154FD081BA252B9295E8184D, AD3C590D1C0963D62702445E8108DB025EEBEC70, EBF794E421BE60C9532091EB432C1977517D1BE5, F81DE9584F0BF3E55C6CF1B465F00B2671DAA230
	IPv4	185[.]225[.]69[.]223, 193[.]29[.]104[.]152, 45[.]137[.]222[.]24, 91[.]237[.]124[.]164, 185[.]195[.]237[.]106, 91[.]237[.]124[.]153, 146[.]70[.]125[.]79, 89[.]44[.]9[.]74, 111[.]90[.]151[.]167
	Domains	sqj[.]fr, tgh24[.]xyz, tuo[.]world, lsjb[.]digital, jiaw[.]shop, hfuu[.]de, raxia[.]top, rnl[.]world, hijx[.]xyz, ikses[.]net
	SHA256	335b1cd7708284fc1c2c6678f2f8d6737d68935ec992d680ff540f2 e72774665
<u>LOSTKEYS</u>	SHA256	13f7599c94b9d4b028ce02397717a1282a46f07b9d3e2f8f2b3213f a8884b029, 4c7accba35edd646584bb5a40ab78f963de45e5fc816e62022cd7a b1b01dae9c, 6b85d707c23d68f9518e757cc97adb20adc8accb33d0d68faf1d8d 56d7840816, 3233668d2e4a80b17e6357177b53539df659e55e06ba49777d0d5 171f27565dd, 6bc411d562456079a8f1e38f3473c33ade73b08c7518861699e986 3540b64f9a, 28a0596b9c62b7b7aca9cac2a07b067109f27d327581a60e8cb4fa b92f8f4fa9, b55cdce773bc77ee46b503dbd9430828cc0f518b94289fbfa70b5fb b02ab1847, 02ce477a07681ee1671c7164c9cc847b01c2e1cd50e709f7e861ea ab89c69b6f, 8af28bb7e8e2f663d4b797bf3ddbee7f0a33f637a33df9b31fbb4c1 ce71b2fee

Attack Name	TYPE	VALUE
<u>Interlock</u>	IPv4	23[.]95[.]182[.]59, 195[.]201[.]21[.]34, 159[.]223[.]46[.]184, 23[.]227[.]203[.]162, 65[.]109[.]226[.]176, 65[.]38[.]120[.]47, 216[.]245[.]184[.]181, 212[.]237[.]217[.]182, 168[.]119[.]96[.]41, 216[.]245[.]184[.]170, 65[.]108[.]80[.]58, 84[.]200[.]24[.]41, 206[.]206[.]123[.]65, 49[.]12[.]102[.]206, 193[.]149[.]180[.]158, 85[.]239[.]52[.]252, 5[.]252[.]177[.]228, 80[.]87[.]206[.]189, 65[.]108[.]80[.]58, 212[.]104[.]133[.]72, 140[.]82[.]14[.]117, 64[.]94[.]84[.]85, 49[.]12[.]69[.]80, 96[.]62[.]214[.]11, 177[.]136[.]225[.]153, 188[.]34[.]195[.]44, 45[.]61[.]136[.]202
<u>Nitrogen</u>	SHA256	5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac 7a71d321, 9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdafbede830 51692e63, ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d 8507ffe2c, c94b70dff50e69639b0ef1e828621c5fddcf144fea93e27520f48264d dd33273, 0db5c55ef52e89401a668f59bf4f69391f4632447c51483bb64749d7f 2123916, 779576719a9c400a7a4abed0386e2111eb331160572c91a2fd8eaa1 a7d6e6c63, e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85 bda2bff6, 55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47 c18c88be, fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5 d2afa2
<u>PureHVNC</u>	SHA256	b33e162a78b7b8e7dbbab5d1572d63814077fa524067ce79c37f524 41b8bd384, 0c9228983fbd928ac94c057a00d744d6be4bd4c1b39d1465b7d955b 7d35bf496, 839371cd5a5d66828ac9524182769371dede9606826ad7c22c3bb18 fb2ee91cb,

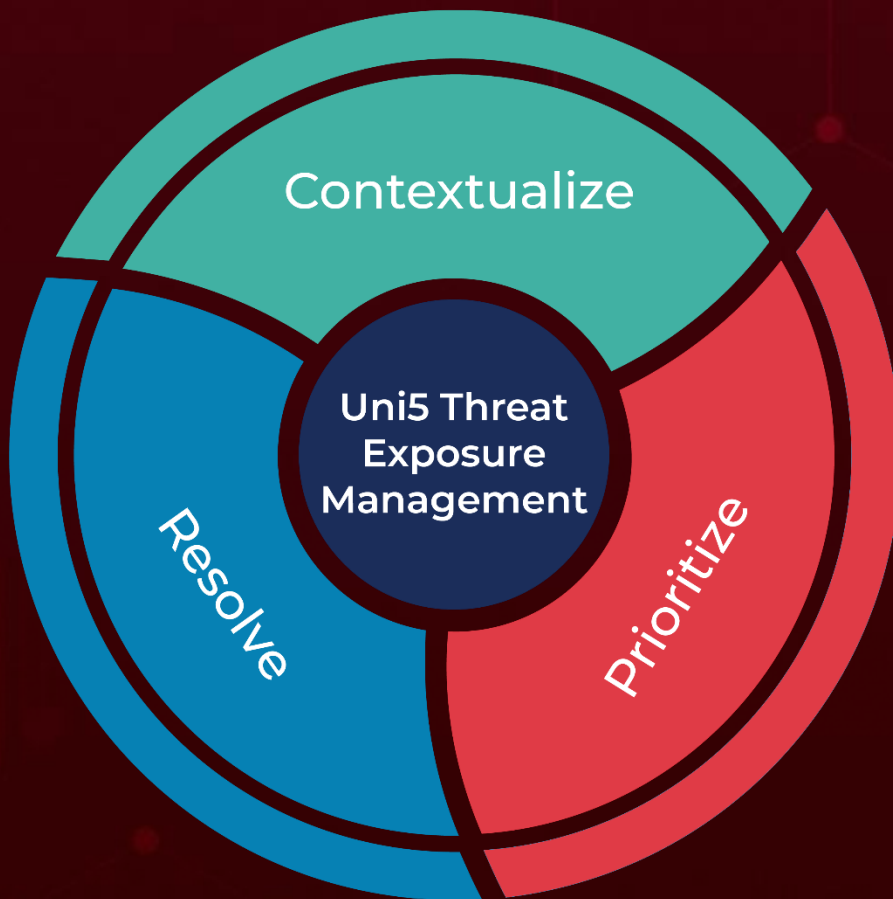
Attack Name	TYPE	VALUE
<u>PureHVNC</u>	SHA256	9dab2badfdae86963b2f13ce8942fe78dd66ec497f8d82dd40c0cb5bec4fb2a7, cee3f98b5f175219d025a92eddec4fd8bcaae31e6ad99321ae7c00b822063fc3, a5baceb97a2be17dd0c282292ebb0b5a56a555013a4c8fffc2335c504780fb, 3fba4a0942244e9c3ad25a57a21f91b06f8732a2ca36da948ae5f0afa51dc72b, 557becfcc7eccaa5a7368a6d5583404af26aadede2c345d6070e6e9fab44a641
PureRAT	IPv4:Port	195[.]26[.]227[.]209[:]56001
PureLogs	IPv4:Port	195[.]26[.]227[.]209[:]23075
	SHA256	df38f29f1f511ac9a5ecae5d4734732c039c17ec06137fade7b1e2b48899c681
PureCrypter	URL	hxxps[:]//apstori[.]ru/panel/uploads/Bghwwhmlr[.]wav
<u>TetraLoader</u>	SHA256	14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64c4f4611f, 4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9
<u>KrustyLoader</u>	SHA256	f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec, 47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04, 3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce, 91f66ba1ad49d3062afdcc80e54da0807207d80a1b539edcdbc6e1bf99e7a2ca, c71da1dfea145798f881afd73b597336d87f18f8fd8f9a7f524c6749a5c664e4, b8e56de3792dbd0f4239b54cfaad7ece3bd42affa4fbbdd7668492de548b5df8, 0c2c8280701706e0772cb9be83502096e94ad4d9c21d576db0bc627e1e84b579, 5f3d1f17033d85b85f3bd5ae55cb720e53b31f1679d52986c8d635fd1ce0c08a
	Domains	brandnav-cms-storage[.]s3[.]amazonaws[.]com, abode-dashboard-media[.]s3[.]ap-south-1.amazonaws[.]com, applr-malbbal[.]s3[.]ap-northeast-2[.]amazonaws[.]com
<u>Qilin</u>	URL	hxxp[:]//184[.]174[.]96[.]70
	IPv4	180[.]131[.]145[.]73

Attack Name	TYPE	VALUE
<u>BianLian</u>	IPv4:Port	64[.]190[.]113[.]215[:]443, 15[.]237[.]93[.]235[:]443, 94[.]198[.]40[.]6[:]20033, 94[.]198[.]40[.]6[:]20007, 139[.]162[.]1[.]232[:]8443, 49[.]232[.]6[.]238[:]443, 170[.]64[.]148[.]46[:]443
<u>RansomExx</u>	SHA256	bb12b7c4169e2a86a67a86f03048baa282688d36ef0ae3251bc1ace3 17c26af9, 6b667bb7e4f3f2cb6c6f2d43290f32f41ae9f0d6ed34b818d78490050 f7582a1, 78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f 1fafc13d, 08113ca015468d6c29af4e4e4754c003dacc194ce4a254e15f380608 54f18867, cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331 bb3c5849, 843b8434ab69089970530b0d1a9865a89d25aed88bc98d91845bfe4 1a6dfc31b
<u>PipeMagic</u>	SHA256	945a02cdbbd8772f5b0a30f047ae6450ee77a14fef5046af252565a9 b524c88f, d9cb912e6ca4dc22515b9dfddced01a96f6de2fd51169597d437d390 d5d868f1, 2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa 5b6ebe
<u>Vidar</u>	SHA256	3bb81c977bb34fadb3bdeac7e61193dd009725783fb2cf453e1 5ced70fc39e9b, b8d9821a478f1a377095867aeb2038c464cc59ed31a4c7413ff 768f2e14d3886
<u>StealC</u>	SHA256	afc72f0d8f24657d0090566ebda910a3be89d4bdd68b029a99a 19d146d63adc5
<u>Dero</u>	SHA256	e4aa649015b19a3c3350b0d897e23377d0487f9ea265fe94e71 61fed09f283cf
	Wallet Address	dero1qyy8xjrdjcn2dvr6pwe40jrl3evv9vam6tpx537vux60xxkx6 hs7zqgde993y
	Domains	d[.]windowsupdatesupport[.]link, h[.]wiNdowsupdatesupport[.]link
<u>XMRig</u>	SHA256	3a71680ffb4264e07da4aaca16a3f8831b9a30d444215268e82 b2125a98b94aa
<u>TOUGHPROGRES S</u>	SHA256	3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2f a302791c2c4fb

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 2, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com