

Date of Publication
August 5, 2025



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JULY 2025

Table Of Contents

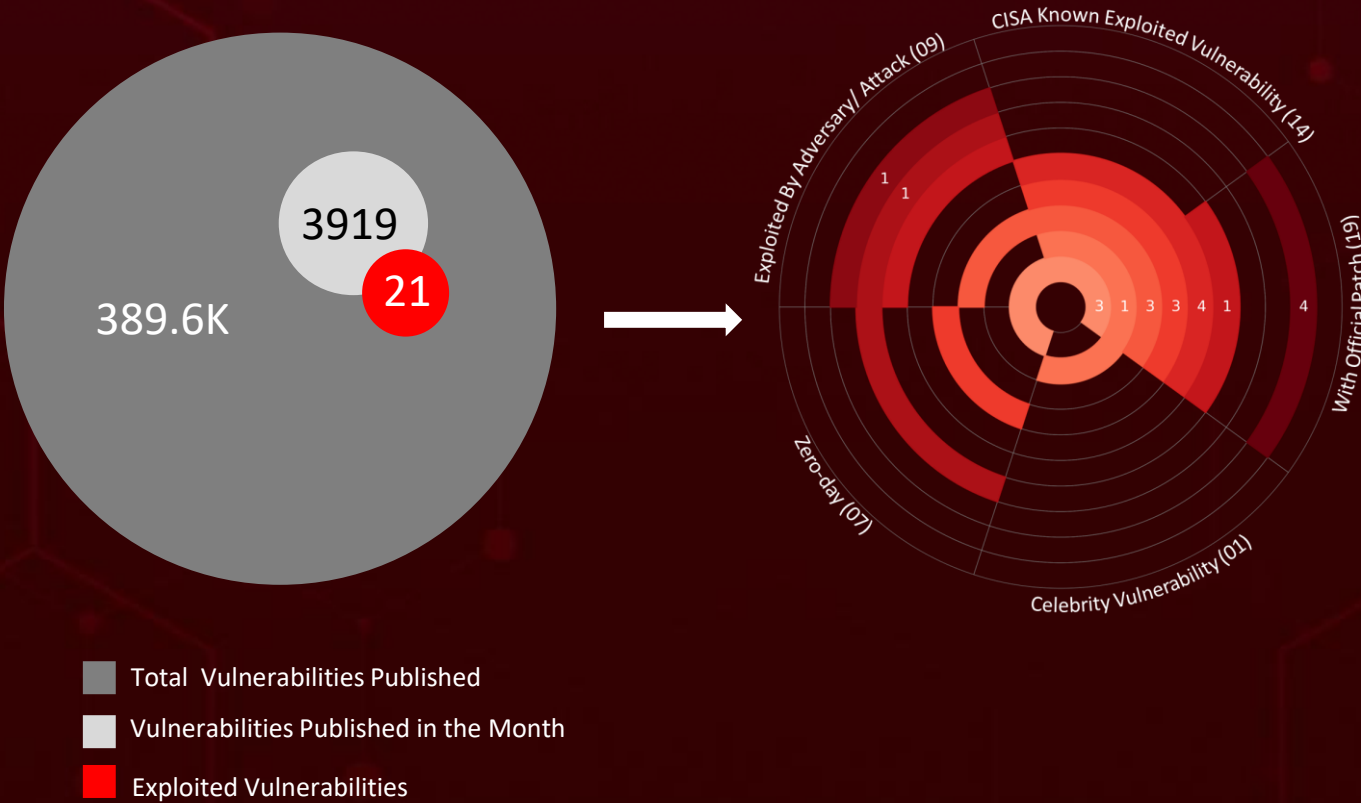
<u>Summary</u>	03
<u>Insights</u>	04
<u>Threat Landscape</u>	05
<u>Celebrity Vulnerabilities</u>	06
<u>Vulnerabilities Summary</u>	07
<u>Attacks Summary</u>	09
<u>Adversaries Summary</u>	12
<u>Targeted Products</u>	14
<u>Targeted Countries</u>	16
<u>Targeted Industries</u>	17
<u>Top MITRE ATT&CK TTPs</u>	18
<u>Top Indicators of Compromise (IOCs)</u>	19
<u>Vulnerabilities Exploited</u>	22
<u>Attacks Executed</u>	34
<u>Adversaries in Action</u>	49
<u>MITRE ATT&CK TTPS</u>	60
<u>Top 5 Takeaways</u>	66
<u>Recommendations</u>	67
<u>Appendix</u>	68
<u>Indicators of Compromise (IoCs)</u>	69
<u>What Next?</u>	75

Summary

In **July**, the cybersecurity arena drew significant attention due to the active exploitation of **seven zero-day** vulnerabilities. Among them, Google Chrome patched a **zero-day vulnerability (CVE-2025-6554)**. It is a critical flaw in Chrome's V8 engine that allows memory corruption and remote code execution, and was actively exploited in the wild before a patch was released.

During this period, ransomware attacks surged, with variants such as **DEVMAN, Dire Wolf, Interlock, GLOBAL, and Bert** aggressively targeting victims. Among the key developments, **Dire Wolf**, a sophisticated ransomware group first identified in May 2025, is targeting sectors across 13 countries using double extortion tactics. **Interlock ransomware** now leverages a PHP-based RAT delivered via fake CAPTCHA lures and Cloudflare Tunnel, enabling stealthy system access and advanced intrusion techniques.

Concurrently, **eleven** threat actors have engaged in various campaigns. The financially motivated group **Scattered Spider** launched a campaign in mid-2025 targeting VMware vSphere environments, using social engineering to infiltrate Active Directory and subsequently exploiting vCenter and ESXi for credential theft and ransomware deployment. In Latin America, the cybercriminal group **Blind Eagle** is deploying banking-themed phishing emails laced with remote access tools such as **Remcos** and **AsyncRAT**. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



In July 2025, a geopolitical cybersecurity landscape unfolds, revealing **United States, Turkey, Germany, Russia, and India**, as the top-targeted countries.

Highlighted in **July 2025** is a cyber battleground encompassing the **Technology, Government, Manufacturing, Retail, and Financial** sectors, designating them as the top industries.

Operation GhostChat and Operation PhantomPrayers Tailored malware disguised behind fake apps puts Tibetan users in the crosshairs.

APT36 Targets BOSS Linux
in Stealthy Cyber Attack Against India's Defense Networks

NordDragonScan is a .NET info-stealer using malicious HTA scripts and deceptive links to steal data.

Flaws in Cisco ISE and ISE-PIC CVE-2025-20281, -20282, and -20337 could undermine enterprise security controls if left unpatched.

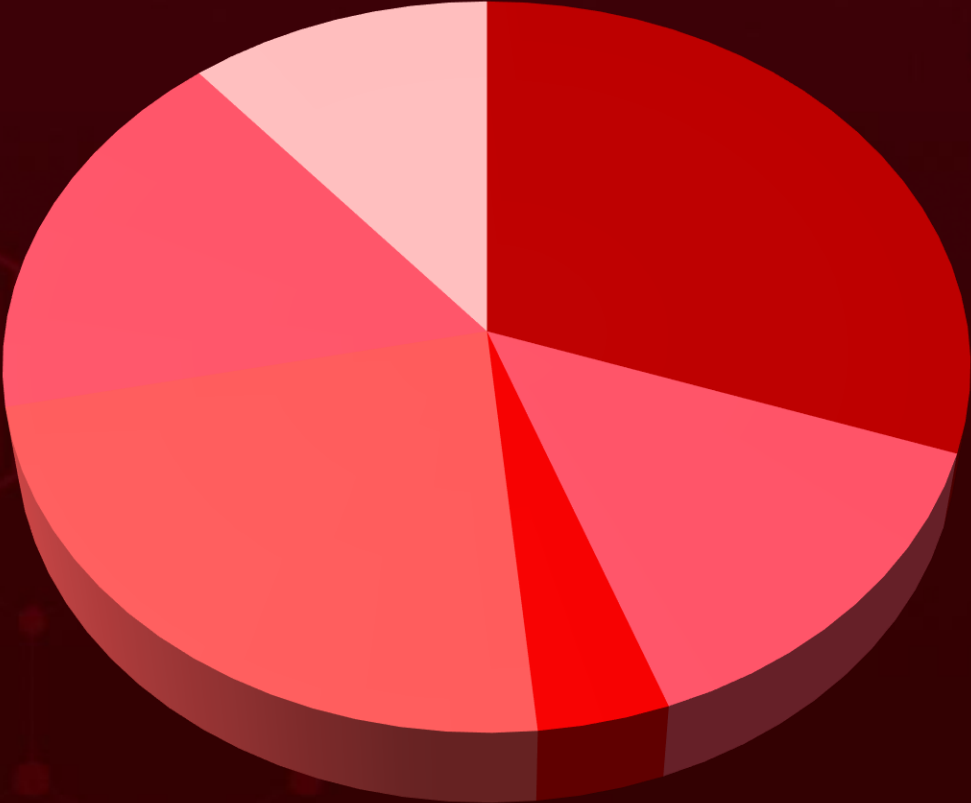
Critical Zero-Day vulnerability in Google Chrome (CVE-2025-6558) under active exploitation, immediate patch required to prevent full system compromise.

CitrixBleed 2
Vulnerability Now Weaponized in Active Campaigns

CVE-2025-6463: A critical flaw in Forminator Forms lets attackers delete server files - 600K+ sites at risk.

APT41 Expands Its Reach: China-linked group exploits misconfigurations to exfiltrate sensitive credentials.



Threat Landscape






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



Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-5777</u>	CitrixBleed 2	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID	T1190: Exploit Public-Facing Application, T1059: Command and Scripting, T1068: Exploitation for Privilege Escalation	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

Vulnerabilities Summary


CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-6463	WordPress Forminator Plugin Unauthenticated Arbitrary File Deletion Vulnerability	WordPress Forminator Plugin			
CVE-2025-49719	Microsoft SQL Server Information Disclosure Vulnerability	Microsoft SQL Server			
CVE-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chromium			
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR OS			
CVE-2024-12856	Four-Faith OS Command Injection Vulnerability	Four-Faith OS			
CVE-2025-5777	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway			
CVE-2025-47812	Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability	Wing FTP Server			
CVE-2025-25257	Fortinet FortiWeb SQL Injection Vulnerability	Fortinet FortiWeb			
CVE-2025-6558	Google Chrome Insufficient Validation of Untrusted Input in ANGLE and GPU Vulnerability	Google Chrome			
CVE-2020-0688	Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability	Microsoft Exchange Server			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-54309	CrushFTP Unprotected Alternate Channel Vulnerability	CrushFTP			
CVE-2025-53770	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server			
CVE-2025-53771	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server			
CVE-2025-49706	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server			
CVE-2025-49704	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint Server			
CVE-2025-20281	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability	Cisco ISE			
CVE-2025-20282	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability	Cisco ISE			
CVE-2025-20337	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability	Cisco ISE			
CVE-2025-21590	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability	Juniper Junos OS			
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver			
CVE-2025-5394	WordPress Alone Theme Remote Code Execution Vulnerability	WordPress Alone Theme Plugin			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Remcos	RAT	-	-	-	Phishing
AsyncRAT	RAT	-	-	-	Phishing
NimDoor	Backdoor	-	macOS	-	Social Engineering
DEVMAN	Ransomware	-	Windows	-	-
Hpingbot	Botnet	-	Windows, Linux, IoT	-	-
Dire Wolf	Ransomware	-	Windows (cross-platform capability via Golang)	-	-
RondoDox	Botnet	CVE-2024-3721 CVE-2024-12856	TBK DVR-4104 and DVR-4216 devices, Four-Faith F3x24 and F3x36	-	Exploiting Critical Vulnerabilities in TBK DVRs and Four-Faith devices
Batavia	Spyware	-	Window	-	Multi-Stage Phishing Campaign
Lumma	Stealer	-	Window	-	Social Engineering via Github
NordDragonScan	Infostealer	-	Windows	-	-
INTERLOCK	Ransomware	-	Windows	-	Phishing
INTERLOCK PHP	RAT	-	Windows	-	FileFix phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Octalyn Stealer	Stealer	-	Windows	-	-
GLOBAL	Ransomware	-	-	-	Via Initial Access Brokers
GhostContainer	Backdoor	CVE-2020-0688	Microsoft Exchange Server		Exploiting vulnerabilities
Voldemort	Backdoor	-	-	-	Phishing
HealthKick	Backdoor	-	-	-	Phishing
PureRAT	RAT	-	-	-	Phishing
Ghost Crypt	Tool	-	-	-	Phishing
AllaKore RAT	RAT	-	-	-	Phishing
SystemBC	RAT	-	-	-	Phishing
EAGLET	RAT	-	Windows		Phishing
TINYSHELL	Backdoor	CVE-2025-21590	Juniper Junos OS		Exploiting Vulnerability
NailaoLocker	Ransomware	CVE-2024-24919	Check Point Security Gateway		Exploiting Vulnerability
Auto-color	Backdoor	CVE-2025-31324	SAP NetWeaver		Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BERT	Ransomware	-	Windows, Linux	-	Phishing
Gh0st RAT	RAT	-	-	-	Social Engineering
PhantomNet	Backdoor	-	-	-	Social Engineering

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Blind Eagle	Information theft and espionage, Financial crime	Colombia	-	Remcos, AsyncRAT	-
APT36	Information theft and espionage	Pakistan	-	-	BOSS (Bharat Operating System Solutions) Linux
Gold Melody	Financial Gain, Information theft, and espionage	-	-	-	-
Linen Typhoon	Information theft and espionage	China	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
Violet Typhoon	Information theft and espionage	China	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
Storm-2603	Information theft and espionage	China	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
APT41	Financial crime, Information theft and espionage	China	-	-	Windows

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Greedy Sponge	Financial crime	-	-	AllaKore RAT, SystemBC	-
UNG0901	Information theft and espionage	-	-	EAGLET	Windows
UNC3886	Information theft and espionage	China	CVE-2025-21590	TINYSHELL	Juniper Junos OS
Scattered Spider	Financial gain	-	-	-	VMware vSphere, Windows



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
 Microsoft	Mail server	Microsoft Exchange Server
	SQL Server	Microsoft SQL Server
	SharePoint Server	Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition
	Plugin	WordPress Forminator Forms plugin versions prior to 1.44.3 WordPress Alone Theme Version 7.8.3 and below
	Browser	Google Chromium
 CrushFTP	Secure file transfer server	CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23
	Embedded DVR OS	TBK DVR-4104 and DVR-4216 up to 20240412

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating system	Four-Faith F3x24 and F3x36
	FTP Server	Wing FTP Server before 7.4.4
	Web application firewall	Fortinet FortiWeb versions: 7.6.0 - 7.6.3 7.4.0 - 7.4.7 7.2.0 - 7.2.10 7.0.0 - 7.0.10
	Network Access Control	Cisco ISE and ISE-PIC releases 3.3 and 3.4
	Network operating system	Juniper Junos OS
	Application server and integration platform	SAP NetWeaver

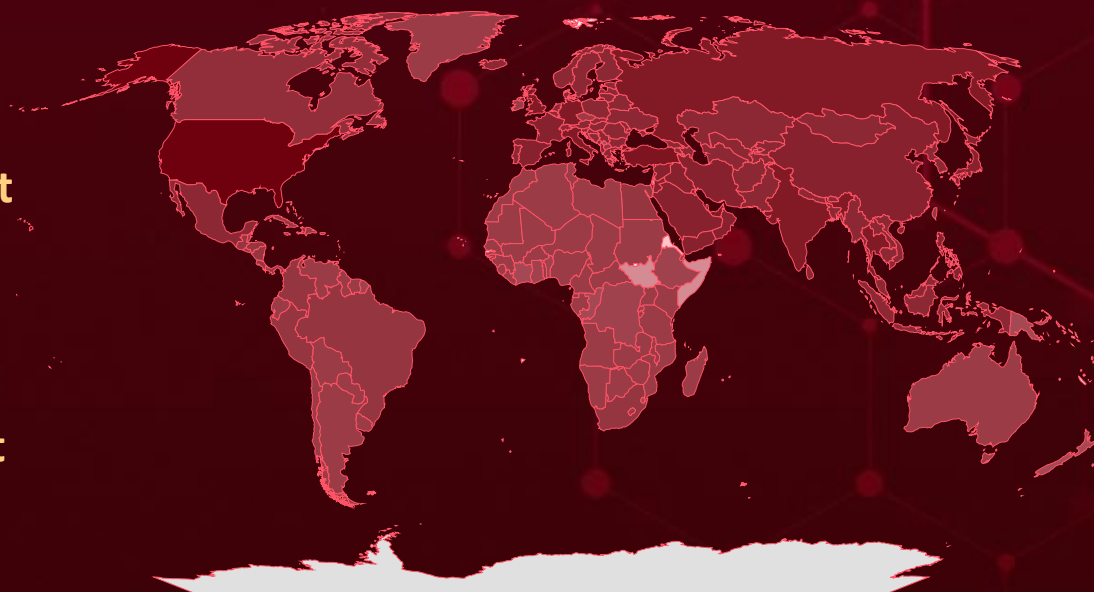


Targeted Countries

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		China		Cyprus		Kazakhstan		Haiti
	Turkey		Qatar		Montenegro		Pakistan		Canada
	Germany		France		Denmark		Kyrgyzstan		Armenia
	Russia		Iraq		North Korea		Poland		Norway
	India		Jordan		Estonia		Laos		Mexico
	Bahrain		Yemen		Azerbaijan		Romania		Vietnam
	Singapore		Kuwait		Finland		Latvia		Moldova
	Thailand		Lebanon		San Marino		Bangladesh		Maldives
	United Arab Emirates		Monaco		Georgia		Afghanistan		Cuba
	Italy		Serbia		Slovenia		Slovakia		South Africa
	United Kingdom		Austria		Greece		Liechtenstein		Peru
	Israel		Brunei		Sweden		South Korea		El Salvador
	Japan		Belgium		Holy See		Lithuania		Taiwan
	Syria		Bulgaria		Timor-Leste		Sri Lanka		Martinique
	Iran		Nepal		Hungary		Luxembourg		Panama
	Saudi Arabia		Cambodia		Uzbekistan		Switzerland		Dominican Republic
	Oman		Portugal		Iceland		Malaysia		Egypt
	Spain		Albania		Mongolia		Tajikistan		Honduras
	Philippines		Belarus		Andorra		Bosnia and Herzegovina		Colombia
			Croatia		Myanmar		Turkmenistan		Nicaragua
			Ukraine		Indonesia		Malta		Costa Rica
					Mexico		Bhutan		
					Vietnam				
					Moldova				

Targeted Industries

Most



Technology



Government



Manufacturing



Retail



Financial



Healthcare



Transportation



Defence



Aerospace



Professional Services



Energy



Education



Media



Real Estate



Construction



Legal



Engineering



Food products



Insurance



Banking



Aviation



Oil & Gas



Pharmaceutical



Gaming



Cryptocurrency



Telecommunications



Utilities



Think-Tanks



Agriculture



E-commerce



Logistics



Business Services



Critical Infrastructure

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1027

Obfuscated Files or Information

T1071

Application Layer Protocol

T1082

System Information Discovery

T1204

User Execution

T1041

Exfiltration Over C2 Channel

T1059.001

PowerShell

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1036

Masquerading

T1083

File and Directory Discovery

T1070

Indicator Removal

T1566

Phishing

T1071.001

Web Protocols

T1105

Ingress Tool Transfer

T1190

Exploit Public-Facing Application

T1005

Data from Local System

T1140

Deobfuscate/Decode Files or Information

T1068

Exploitation for Privilege Escalation

T1543

Create or Modify System Process

T1486

Data Encrypted for Impact

T1547.001

Registry Run Keys / Startup Folder

T1562

Impair Defenses

T1203

Exploitation for Client Execution

T1562.001

Disable or Modify Tools



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>RondoDox</u>	SHA256	0a9ebbecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9, 9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd, 6c81fd73b4bef6fef379cbefdcce7f374ea7e6bf1bf0917cf4ca7b72d4cee788, a55a3859a203ca2bae7399295f92aeae61d845ffa173c1938f938f5c148eef99, 57573779f9a62eecb80737d41d42165af8bb9884579c50736766abb63d2835ba, 3daa53204978b7797bd53f5c964eed7a73d971517a764785ce3ab65a9423c2e7, 8bf8928bc255e73e0b5b0ce13747c64d82d5f2647da129f189138773733ac21f, 20a24b179bdbbdcc0053838c0484ea25eff6976f2b8cb5630ab4efb28b0f06b5, 42aa715573c7d2fca01914504cb7336db715d73d1e20d23e4bd37f2e4f4fe389
<u>GhostContainer</u>	MD5	01d98380dfb9211251c75c87ddb3c79c
	SHA1	2bb0a91c93034f671696da64a2cf6191a60a79c5
	SHA256	87a3aefb5cdf714882eb02051916371fbf04af2eb7a5ddeae4b6b441b2168e36
	Filename	App_Web_Container_1.dll
<u>AllaKore RAT</u>	Domain	manzisuape[.]com, siperasul[.]com, cupertujo[.]com, idaculipa[.]com, mepunico[.]com, barrosoon[.]com, tllemeuas[.]com
<u>SystemBC</u>	Domain	pachisuave[.]com
<u>EAGLET</u>	IPv4	185[.]225[.]17[.]104, 188[.]127[.]254[.]44




Attack Name	TYPE	VALUE
TINYHELL	MD5	2c89a18944d3a895bd6432415546635e, aac5d83d296df81c9259c9a533a8423a, 8023d01ffb7a38b582f0d598afb974ee, 5724d76f832ce8061f74b0e9f1dcad90, e7622d983d22e749b3658600df00296d, b9e4784fa0e6283ce6e2094426a02fce, bf80c96089d37b8571b5de7cab14dd9f, 3243e04afe18cc5e1230d49011e19899
	SHA1	50520639cf77df0c15cc95076fac901e3d04b708, 1a6d07da7e77a5706dd8af899ebe4daa74bbbe91, 06a1f879da398c00522649171526dc968f769093, f8697b400059d4d5082eee2d269735aa8ea2df9a, cf7af504ef0796d91207e41815187a793d430d85, 01735bb47a933ae9ec470e6be737d8f646a8ec66, cec327e51b79cf11b3eeffebf1be8ac0d66e9529, 2e9215a203e908483d04dfc0328651d79d35b54f
	SHA256	98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14 d244d8373888, 5bef7608d66112315eefff354dae42f49178b7498f994a728ae6 203a8a59f5a2, c0ec15e08b4fb3730c5695fb7b4a6b85f7fe341282ad469e4e14 1c40ead310c3, 5995aaff5a047565c0d7fe3c80fa354c40e7e8c3e7d4df292316c 8472d4ac67a, 905b18d5df58dd6c16930e318d9574a2ad793ec993ad2f68bca 813574e3d854b, e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd411 82deea978400ed, 3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd 1065723f11f7e, 7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc 3ae56cfd13b4
	IPv4:Port	129[.]126[.]109[.]50[:]22, 116[.]88[.]34[.]184[:]22, 223[.]25[.]78[.]136[:]22, 45[.]77[.]39[.]28[:]22, 101[.]100[.]182[.]122[:]22, 118[.]189[.]188[.]122[:]22, 158[.]140[.]135[.]244[:]22, 8[.]222[.]225[.]8[:]22




Attack Name	TYPE	VALUE
<u>Remcos</u>	SHA256	5cf4a8c83f8591950c24c8b5d79c5464e4cb1b608fc61775f605d6a3503c73c3, 1728133a5a75adc097d2b5dee5693c5b1b72d25832435213bad a40be433b2f75
<u>AsyncRAT</u>	SHA256	394908cbe5ba04a3b772ef11ea6a2c6a0c8d3d9689c89ccd1410 aaa583bb07d7, 48ee878fetc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865a b292be9f0, 2e432426a7a0a10a0068c035368f749c298e1ef1add61e31a8b2 5da74676fcaa, 2a84f9440f120edd032eddb4b61339ee184743d47805e2ed505 72ca4905c1fdd, 66663cf3596b0e6fd2721d81f91cda058ca61feb46f9943ef1a91f ec7a68590d, 666f0c305b0a6cc558192918bc144c3119d898c3365610139514 0d93e9e10e69, fa32ea24d1a6041be009ad0c59ce61f3d00e0588700c709c0222 ecd8c8c3753, 81ffcabc8db8db4f42ee4d53f35d47e5cca9aba8fadf972a97596b 79492cb03
<u>NailaoLocker</u>	SHA256	46f3029fcc7e2a12253c0cc65e5c58b5f1296df1e364878b1780 27ab26562d68
<u>Auto-color</u>	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796 cfc3072d4c43











Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6463</u>		WordPress Forminator Forms plugin versions prior to 1.44.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wpmudev:forminator_forms:*:*:*:*:wordpress:*:*	-
WordPress Forminator Plugin Unauthenticated Arbitrary File Deletion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1485: Data Destruction; T1070: Indicator Removal	https://wordpress.org/plugins/forminator/advanced/ , https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/forminator/forminator-forms-contact-form-payment-form-custom-form-builder-1442-unauthenticated-arbitrary-file-deletion-triggered-via-administrator-form-submission-deletion




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49719</u>		Microsoft SQL Server: 2016 - 2022	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:sql_server:*:*:*:*:*:*	-
Microsoft SQL Server Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1213: Data from Information Repositories, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-49719




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6554</u>		Google Chrome prior to 138.0.7204.96	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*.*	-
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-6554 , https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-3721</u>		TBK DVR-4104 and DVR-4216 up to 20240412	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tbk_vision:tbk_dvr_4104:*:*:*:*:*:*:*	RondoDox botnet
TBK DVR OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1071: Application Layer Protocol	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-12856</u>		Four-Faith F3x24 and F3x36	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:four-faith:f3x24:*:*:*:*:*:*:*	RondoDox botnet
Four-Faith OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1499: Endpoint Denial of Service, T1078.001: Default Accounts	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-47812</u>		Wing FTP Server before 7.4.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wftpserv:wing_ftp_server:*:*:*:*:*:*	-
Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-158	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1136: Create Account	https://www.wftpserv.com/download.htm




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-25257</u>		Fortinet FortiWeb versions: 7.6.0 - 7.6.3 7.4.0 - 7.4.7 7.2.0 - 7.2.10 7.0.0 - 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*	-
Fortinet FortiWeb SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-151




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6558</u>		Google Chrome prior to 138.0.7204.157	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chrome Insufficient Validation of Untrusted Input in ANGLE and GPU Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1497: Virtualization/Sandbox Evasion, T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-0688</u>		Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY		
Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	GhostContainer
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1203: Exploitation for Client Execution, T1059: Command and Scripting	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54309		CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*	-
CrushFTP Unprotected Alternate Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-420	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1211: Exploitation for Defense Evasion	https://www.crushftp.com/download.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53770		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	-
Microsoft SharePoint Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-53771</u>		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*	-
Microsoft SharePoint Server Spoofing Vulnerability		cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707 CWE-22 CWE-20	T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53771




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49706</u>		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*	-
Microsoft SharePoint Server Spoofing Vulnerability		cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49704</u>		Microsoft SharePoint Enterprise Server: 2016 - 2019	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*	-
Microsoft SharePoint Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20281</u>		Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20282</u>		Cisco ISE and ISE-PIC Release 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*.~.*.*.*.* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*.~.*.*.*.*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20337</u>		Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*.~.*.*.*.* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*.~.*.*.*.*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21590</u>		Juniper Junos OS	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*:*	TINYSHELL
Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter	https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31324		SAP NetWeaver	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*	Auto-color
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/may-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5394		WordPress Alone Theme Version 7.8.3 and below	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:alone_theme:alone_theme:*:*:*:*:*:*	-
WordPress Alone Theme Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1059 Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://themeforest.net/item/alone-charity-multipurpose-nonprofit-wordpress-theme/15019939?srltid=AfmBOooSAqUyZH2ZA9U0DOLSX4pH_drgM0BOTtNABJqo1l-WYwYlnBjV

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos, is often employed by attackers to gain complete control over systems. It operates stealthily, elevates privileges, and persists through reboots. Common methods of delivery include phishing emails, exploit kits, and watering hole attacks.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Information Theft, Remote Control	-
Blind Eagle			
	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a publicly available remote access trojan (RAT) on GitHub. A modified version ensures persistence by creating a scheduled task that triggers at startup. Upon activation, a complex sequence initiates AsyncRAT within Windows Sandbox, which must be manually enabled and requires a reboot.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Remote Control, Information Theft	-
Blind Eagle			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
NimDoor	<p>NimDoor is a sophisticated macOS backdoor malware, primarily attributed to North Korean threat actors, that specifically targets Web3 and cryptocurrency businesses. It distinguishes itself by utilizing the relatively uncommon Nim programming language for its binaries, making it harder to detect and analyze. The infection typically begins with social engineering tactics, that initiates a multi-stage infection process, including process injection and the deployment of persistent components. Once established, NimDoor is capable of exfiltrating sensitive data like browser information, Keychain credentials, and Telegram chat histories, all communicated securely to its command-and-control servers using encrypted channels.</p>	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			macOS
ASSOCIATED ACTOR			PATCH LINK
-		System Compromise, Data Theft	-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DEVMAN	<p>DEVMAN ransomware is a new and evolving variant belonging to the DragonForce malware family, which has emerged as a significant threat in 2025. This ransomware encrypts victim data and appends a ".DEVMAN" extension to the locked files, dropping a ransom note. DEVMAN first exfiltrates sensitive data and then encrypts the systems. While seemingly still under development due to some peculiar behaviors, DEVMAN has already shown capabilities for rapid lateral movement, and is actively engaging in collaborations with established Ransomware-as-a-Service (RaaS) groups, expanding its reach across various industries globally.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Windows
ASSOCIATED ACTOR			PATCH LINK
-		Data Theft, Encrypt Data	-

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>Hpingbot</u>	<p>Hpingbot is a newly discovered, rapidly spreading botnet family that emerged in June 2025. Written in the Go programming language, it's a cross-platform threat, infecting both Windows and Linux/IoT devices across various processor architectures. Hpingbot is notable for its innovative use of Pastebin for payload delivery and leveraging the legitimate network testing tool hping3 to launch powerful DDoS attacks. While its primary purpose appears to be DDoS, it also exhibits sophisticated persistence mechanisms, including modifying system services and scheduled tasks, and the ability to download and execute arbitrary payloads, indicating potential for broader malicious activities beyond just DDoS.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		System Persistence, Launch DDoS attacks	Windows, Linux, IoT
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>Dire Wolf</u> TYPE Ransomware ASSOCIATED ACTOR -	Dire Wolf is a ransomware written in Golang, compressed with UPX, and engineered to disable recovery options while employing robust encryption. Each attack is tailored, featuring distinctive ransom notes and dedicated negotiation portals, highlighting a targeted operation.	-	-
		IMPACT	AFFECTED PLATFORM
		Data Exfiltration, Data Integrity Risks, Financial Loss	Windows (cross-platform capability via Golang)
			PATCH LINK -

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RondoDox</u> TYPE Botnet ASSOCIATED ACTOR -	RondoDox is designed for Linux-based systems. Its shell script downloader scans for writable directories with execution permissions to deploy its payload. Once established, it sets up multiple redundant mechanisms to retain control, such as modifying system startup scripts, creating hidden services, and renaming critical security utilities to evade detection and removal.	Exploiting Critical Vulnerabilities in TBK DVRs and Four-Faith devices	CVE-2024-3721 CVE-2024-12856
		IMPACT	AFFECTED PLATFORM
		Resource Drain, Disruption of Services	TBK DVR-4104 and DVR-4216 devices, Four-Faith F3x24 and F3x36
			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>Batavia</u>	Batavia is a Windows-based spyware that steals the victim's documents and collects sensitive system information, including installed programs, drivers, and operating system components.	Multi-Stage Phishing Campaign	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Exfiltration of Sensitive Information	Windows
Spyware			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Lumma</u>	Lumma Stealer is a potent info-stealing malware that evades detection by injecting itself into memory, employing multiple layers of encryption and obfuscation. The payload, cleverly disguised as a Base64-encoded DLL concealed within a block of French text, is specifically crafted to bypass most antivirus defenses.	Social Engineering via Github	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Exfiltration, Evasion of Detection	Windows
Stealer			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
NordDragonScan	<p>NordDragonScan, a newly identified information-stealing malware, is actively targeting systems through malicious HTA scripts delivered via deceptive shortened links.</p> <p>This .NET based threat is engineered to quietly harvest sensitive data.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
INTERLOCK	<p>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.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Financial Loss, Data Encryption, and Operational Disruption	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>INTERLOCK PHP</u>	The Interlock PHP RAT is a lightweight, fileless remote access trojan used by the Interlock ransomware group for initial access and system reconnaissance. It is delivered via social engineering (FileFix phishing) and establishes covert communication through Cloudflare Tunnel and fallback IPs. The RAT enables attackers to execute commands, deploy payloads, and maintain persistent access before ransomware deployment.	FileFix phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
RAT		Stealthy Persistence, Pre-Ransomware Intrusion	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Octalyn Stealer</u>	The Octalyn Forensic Toolkit, though disguised as an educational tool, is actually a stealthy credential stealer that preys on unsuspecting users. Shared openly on GitHub, it lures in low-skilled actors with a simple builder that creates custom data-stealing payloads using just a Telegram bot token and chat ID. Once deployed, the malware silently steals sensitive information like browser cookies, saved passwords, Discord tokens, crypto wallets, VPN configs, and more organizing everything neatly into folders before zipping it up and sending it back to the attacker via Telegram.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Stealer		Data theft and System Compromise.	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>GLOBAL Ransomware</u>	GLOBAL GROUP, a Ransomware-as-a-Service (RaaS) operation active since June 2025, is gaining traction on Russian-speaking cybercrime forums by offering high affiliate payouts and flexible tooling. The group relies on Initial Access Brokers for network entry. It offers affiliates AI-powered negotiation systems, mobile-accessible dashboards, and customizable ransomware builders, making the platform more attractive to a wider range of cybercriminal partners.	Via Initial Access Brokers	-
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data Theft and Data Encryption	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>GhostContainer</u>	GhostContainer, is a stealthy and highly sophisticated malware and has been discovered targeting Microsoft Exchange servers in government and high-tech environments across Asia. This backdoor blends seamlessly into normal operations, making it incredibly hard to detect, while allowing attackers to maintain long-term access, all without ever reaching out to an external command-and-control server.	Exploiting vulnerabilities	CVE-2020-0688
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Unauthorized access and Data theft	Microsoft Exchange Server
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688

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>Voldemort</u>	Voldemort malware is a stealthy, modular backdoor used in targeted cyberattacks for persistent access and surveillance. It supports command execution, credential theft, and lateral movement across compromised networks. The malware often employs encrypted communication channels to evade detection and maintain long-term access.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Persistent Access, Credential Theft, Lateral Movement	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>HealthKick</u>	HealthKick is a custom backdoor used by China-aligned threat actors, specifically observed targeting the Taiwanese semiconductor industry. It is typically delivered via spear-phishing campaigns, often through DLL sideloading vulnerabilities. Once active, HealthKick can execute commands, capture results, and exfiltrate data to a command-and-control server using a "FakeTLS" protocol.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Credential Theft, Data Exfiltration	-
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>PureRAT</u>	PureRAT is a modern and highly capable Remote Access Trojan (RAT) that was first identified in January 2023. Engineered for stealth and flexibility, this malware gives attackers complete control over compromised systems. Once deployed, PureRAT can quietly monitor user activity, log keystrokes, steal sensitive data, and upload additional malicious payloads. It also has the ability to hijack webcams and microphones for surveillance, disable security tools, and install itself in a way that ensures persistence even after system reboots. Unlike older RATs, PureRAT is modular and lightweight, making it easier to customize and harder to detect.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	-
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Ghost Crypt</u>	Ghost Crypt emerged on April 15, 2025, when it was first advertised on Hackforums by a newly created account under the name “ghostcrypt.” Marketed as a crypting and sideloading service, Ghost Crypt offers advanced obfuscation techniques designed to help threat actors bypass security defenses. It supports packing both executable (EXE) and dynamic link library (DLL) files, making it versatile for delivering a wide range of malicious payloads while evading detection.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Encryption	-
Tool			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>AllaKore RAT</u>	AllaKore RAT is a lightweight, open-source remote access tool written in Delphi, first observed in the wild in 2015. Despite its simplicity, it serves as a powerful spying and data exfiltration utility. Once deployed on a victim's system, AllaKore can silently record keystrokes, capture screenshots, transfer files to and from the infected device, and even grant attacker's full remote control.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
TYPE			PATCH LINK
RAT			
ASSOCIATED ACTOR			-
Greedy Sponge			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SystemBC</u>	SystemBC is a multi-platform malware proxy tool and Remote Access Trojan (RAT) written in C, with indications of Russian origins. It has become increasingly popular among cybercriminals due to its ability to maintain a persistent connection to compromised systems. This persistent access enables attackers to remotely deliver and execute a variety of malicious payloads, including additional executables, PowerShell scripts, Windows commands, and .bat or VBS scripts. Designed to act as a proxy and facilitate covert communications, SystemBC plays a key role in enabling follow-up attacks, data theft, or lateral movement within networks, making it an asset in the toolkits of many threat actors.	Phishing	-
		IMPACT	AFFECTED PRODUCT
		Deliver additional executables, Execute commands	-
TYPE			PATCH LINK
Tool			
ASSOCIATED ACTOR			-
Greedy Sponge			

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>EAGLET</u>	EAGLET is a custom backdoor designed to facilitate data exfiltration and remote command execution on compromised Windows systems. Once deployed, it collects detailed system information and connects to a hard-coded command-and-control (C2) server. Upon establishing this connection, EAGLET processes HTTP responses from the server to retrieve and execute attacker-issued commands. Its streamlined design enables covert communication with the C2 infrastructure, making it an effective tool for persistent access and data theft in targeted intrusions.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			
UNG0901			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TINYSHELL</u>	TINYSHELL is a lightweight, fileless backdoor often used by Chinese state-sponsored threat actors in cyberespionage campaigns. Typically delivered via spear-phishing or exploited servers, it operates entirely in memory to evade detection and provides attackers with remote shell access, command execution, file transfer, and proxy capabilities for lateral movement. TINYSHELL leverages obfuscated PowerShell and HTTP/S-based C2 communication, making it stealthy and effective in long-term intrusions.	Exploiting Vulnerability	CVE-2025-21590
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	Juniper Junos OS
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US
UNC3886			

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>NailaoLocker</u>	NailaoLocker is a ransomware distributed by the Green Nailao threat cluster, primarily targeting European healthcare organizations via ShadowPad and PlugX backdoors. It uses AES-256-CTR encryption, appending a ".locked" extension to encrypted files, and demands ransom via a Proton email address.	Exploiting Vulnerability	CVE-2024-24919
		IMPACT	AFFECTED PRODUCT
TYPE		Encrypt Data	Check Point Security Gateway
Ransomware			PATCH LINK
ASSOCIATED ACTOR			
-			https://support.checkpoint.com/results/sk/sk182336

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Auto-color</u>	A Linux malware strain, Auto-color, is named after the filename it adopts upon installation. Auto-color provides attackers with complete remote control over compromised systems. The malware integrates seamlessly into the system, resisting deletion. If the user lacks root privileges, it halts installation to avoid detection. However, when executed with elevated privileges, it installs a malicious library that mimics a legitimate system library to remain undetected.	Exploiting Vulnerability	CVE-2025-31324
		IMPACT	AFFECTED PRODUCT
TYPE		Remote Control, Persistent Presence	SAP NetWeaver
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
-			https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-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>Bert Ransomware</u>	BERT ransomware (aka Water Pombero), active since March 2025, has rapidly evolved into a multi-platform threat targeting systems across critical sectors. Leveraging REvil’s code and demanding Bitcoin via the Session messenger, the campaign’s growing operational footprint and double-extortion tactics signal a persistent and escalating threat landscape for global enterprises.	Phishing	
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data theft and Data exfiltration	Windows, Linux
ASSOCIATED ACTOR			PATCH LINK
-			-


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Ghost RAT</u>	Gh0st RAT is a notorious remote access trojan designed for Windows systems, widely used in cyber espionage campaigns targeting high-value networks. It provides attackers with complete control over infected machines, allowing them to monitor screens in real time, log keystrokes both online and offline, and stream live audio and video from the victim’s webcam and microphone. The malware can download and execute remote binaries, forcibly shut down or reboot the system, disable user input by locking the keyboard and mouse, and grant shell access for full command execution. Gh0st RAT also allows attackers to monitor running processes and manipulate the System Service Descriptor Table (SSDT) to evade detection.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCT
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-


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


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PhantomNet	PhantomNet, also known as SManager, is a stealthy backdoor malware linked to China-nexus APT groups. Typically deployed in multi-stage attacks, PhantomNet is known for its role in maintaining long-term access to compromised systems. It is often delivered through supply-chain compromises or trojanized applications. Once active, it facilitates command execution, data exfiltration, and ongoing surveillance, making it a key tool in the APT arsenal.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	-
Backdoor			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.

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)</u>	Colombia	Financial institutions	Latin America
	MOTIVE		
	Information theft and espionage, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	Remcos, AsyncRAT	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1656: Impersonation; T1027: Obfuscated Files or Information; T1011: Exfiltration Over Other Network Medium; T1140: Deobfuscate/Decode Files or Information; T1053: Scheduled Task/Job; T1078: Valid Accounts; T1588: Obtain Capabilities; T1588.004: Digital Certificates; T1552: Unsecured Credentials; T1132: Data Encoding; T1132.001: Standard Encoding			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
<div></div> <div><u>APT36 (aka Mythic Leopard, Transparent Tribe, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, C-Major)</u></div>	Pakistan	Defense, Government	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	BOSS (Bharat Operating System Solutions) Linux
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1543.003: Windows Service; T1036: Masquerading; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1571: Non-Standard Port; T1204: User Execution; T1592: Gather Victim Host Information; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1113: Screen Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Gold Melody (aka Prophet Spider, UNC961)</u>	-	Financial Services, Manufacturing, Retail, Technology, Transportation, Logistics	Europe and the U.S.
	MOTIVE		
	Financial Gain, Information theft, and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1036.005: Match Legitimate Resource Name or Location; T1036.010: Masquerade Account Name; T1046: Network Service Discovery; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1136: Create Account; T1136.001: Local Account; T1190: Exploit Public-Facing Application; T1217: Browser Information Discovery; T1505: Server Software Component; T1505.003: Web Shell; T1572: Protocol Tunneling; T1587: Develop Capabilities; T1587.001: Malware; T1036: Masquerading			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u>Linen Typhoon (aka Emissary Panda, APT 27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Budworm, Group 35, ATK 15, Iron Tiger, Earth Smilodon, Red Phoenix, ZipToken, Iron Taurus, Circle Typhoon)</u></p>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
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; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Violet Typhoon (aka APT 31, Judgment Panda, Zirconium, RedBravo, Bronze Vinewood, TA412, Red Keres)</u>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
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; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Storm-2603</u>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server

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; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact


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	Government IT Services	Africa
	MOTIVE		
	Financial crime, Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Windows
TTPs			
TA0008: Lateral Movement; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0001: Initial Access; TA0010: Exfiltration; TA0040: Impact; TA0007: Discovery; T1574.001: DLL; T1078: Valid Accounts; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1078.002: Domain Accounts; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1190: Exploit Public-Facing Application; T1567: Exfiltration Over Web Service; T1543.003: Windows Service; T1614.001: System Language Discovery; T1505.003: Web Shell; T1505: Server Software Component; T1505.004: IIS Components; T1543.003: Windows Service; T1543: Create or Modify System Process; T1055: Process Injection; T1140: Deobfuscate/Decode Files or Information; T1070.004: File Deletion; T1070: Indicator Removal; T1036: Masquerading; T1555: Credentials from Password Stores; T1003.002: Security Account Manager; T1003: OS Credential Dumping; T1552: Unsecured Credentials; T1555.003: Credentials from Web Browsers; T1046: Network Service Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1570: Lateral Tool Transfer; T1021.002: SMB/Windows Admin Shares; T1021: Remote Services; T1560.001: Archive via Utility; T1560: Archive Collected Data; T1119: Automated Collection; T1005: Data from Local System; T1071.001: Web Protocols; T1071.004: DNS; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1090.001: Internal Proxy; T1090: Proxy; T1572: Protocol Tunneling; T1048: Exfiltration Over Alternative Protocol			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Greedy Sponge</u>	-	All	Mexico
	MOTIVE		
	Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	AllaKore RAT, SystemBC	-

TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1591: Gather Victim Org Information; T1591.001: Determine Physical Locations; T1027: Obfuscated Files or Information; T1027.015: Compression; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1204: User Execution; T1204.002: Malicious File; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1070: Indicator Removal; T1070.004: File Deletion; T1132: Data Encoding; T1132.001: Standard Encoding; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1140: Deobfuscate/Decode Files or Information; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1041: Exfiltration Over C2 Channel; T1555: Credentials from Password Stores; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1218: System Binary Proxy Execution; T1218.003: CMSTP; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div>UNG0901</div>	-	Aerospace and Defense	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	EAGLET	Windows
TTPs			
TA0007: Discovery; TA0002: Execution; TA0003: Persistence; TA0040: Impact; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0001: Initial Access; TA0010: Exfiltration; T1041: Exfiltration Over C2 Channel; T1537: Transfer Data to Cloud Account; T1059: Command and Scripting Interpreter; T1566.001: Spearphishing Attachment; T1059.001: PowerShell; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1566: Phishing; T1574.002: DLL; T1036: Masquerading; T1082: System Information Discovery; T1482: Domain Trust Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1005: Data from Local System			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UNC3886</u>	China	Government, Telecommunications, Technology, Aerospace, Defense, Energy, Utility, Critical Infrastructure	North America, Oceania, Europe, Africa, and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-21590	TINYSHELL	Juniper Junos OS
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0042: Resource Development; TA0005: Defense Evasion; TA0006: Credential Access; TA0003: Persistence; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1600: Weaken Encryption; T1041: Exfiltration Over C2 Channel; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1059: Command and Scripting Interpreter; T1014: Rootkit; T1021.004: SSH; T1021: Remote Services; T1078: Valid Accounts; T1078.001: Default Accounts; T1068: Exploitation for Privilege Escalation; T1562: Impair Defenses; T1090: Proxy; T1202: Indirect Command Execution; T1140: Deobfuscate/Decode Files or Information; T1095: Non-Application Layer Protocol; T1588.004: Digital Certificates; T1584: Compromise Infrastructure; T1071.001: Web Protocols; T1071: Application Layer Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Scattered Spider (aka UNC3944, Starfraud, Oktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest, Oktapus, DEV-0971, Storm-0971)</u>	-	Retail, Airline, Insurance	United States
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	VMware vSphere, Windows
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1566.004: Spearphishing Voice; T1598: Phishing for Information; T1566: Phishing; T1059.001: PowerShell; T1490: Inhibit System Recovery; T1547: Boot or Logon Autostart Execution; T1078.002: Domain Accounts; T1078: Valid Accounts; T1548.001: Setuid and Setgid; T1204: User Execution; T1136: Create Account; T1548: Abuse Elevation Control Mechanism; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1003.003: NTDS; T1003: OS Credential Dumping; T1555: Credentials from Password Stores; T1018: Remote System Discovery; T1087.002: Domain Account; T1087: Account Discovery; T1555.003: Credentials from Web Browsers; T1021: Remote Services; T1005: Data from Local System; T1486: Data Encrypted for Impact			

MITRE ATT&CK TTPS

Tactic	Technique	Sub_Technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	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	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task

Tactic	Technique	Sub_Technique
TA0003: Persistence	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1484.001: Group Policy Modification
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location

Tactic	Technique	Sub_Technique
TA0005: Defense Evasion	T1055: Process Injection	
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.003: CMSTP
		T1218.005: Mshta
		T1218.007: Msiexec
		T1218.011: Rundll32
	T1497: Virtualization/Sandbox Evasion	
	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
		T1548.002: Bypass User Account Control
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1620: Reflective Code Loading	
	T1656: Impersonation	T1484.001: Group Policy Modification
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
		T1003.003: NTDS

Tactic	Technique	Sub_Technique
TA0006: Credential Access	T1056: Input Capture	T1056.001: Keylogging
		T1056.001: Keylogging
	T1110: Brute Force	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	T1518.001: Security Software Discovery
		T1614.001: System Language Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	

Tactic	Technique	Sub_Technique
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1011: Exfiltration Over Other Network Medium	
	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1537: Transfer Data to Cloud Account	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1568.003: DNS Calculation
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	

Tactic	Technique	Sub_Technique
TA0040: Impact	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.002: External Defacement
	T1498: Network Denial of Service	
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.005: Botnet
		T1583.006: Web Services
	T1584: Compromise Infrastructure	
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.004: Digital Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
TA0043: Reconnaissance	T1591: Gather Victim Org Information	T1591.001: Determine Physical Locations
	T1592: Gather Victim Host Information	
	T1598: Phishing for Information	T1598.001: Spearphishing Service
		T1598.002: Spearphishing Attachment
		T1598.004: Spearphishing Voice
		T1590.002: DNS
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1568.003: DNS Calculation

Top 5 Takeaways

#1

In July, there were seven zero-day vulnerabilities, with the standout “celebrity” vulnerability, **CitrixBleed2**, taking center stage. Meanwhile, CVE-2025-53770 is being actively exploited to target on-premises Microsoft SharePoint Servers, allowing attackers to bypass patches and gain unauthorized access. With three China-backed groups involved, organizations with internet-facing SharePoint instances should assume compromise and act quickly.

#2

Ransomware is on the rise, with relentless variants like **DEVMAN**, **Dire Wolf**, **Interlock**, **GLOBAL**, and **Bert**, claiming new victims. As attacks grow more sophisticated, organizations must act fast strengthening defenses, securing backups, and refining disaster recovery plans to stay ahead of the threat.

#3

Cyberattacks hit **209** countries in July, with **United States**, **Turkey**, **Germany**, **Russia** and **India**, facing the brunt of the threats. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region was immune as adversaries expanded their reach globally.

#4

The **Technology**, **Government**, **Manufacturing**, **Retail** and **Financial** sectors were prime targets, with ransomware, data theft, and espionage campaigns wreaking havoc. As attackers refine their tactics, organizations in these industries must stay ahead with proactive security measures.

#5

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **Remcos**, **RondoDox**, **ChostContainer**, **LummaStealer**, **TINYSHELL**, and **NailaoLocker**.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **21 significant vulnerabilities** and block the indicators related to the **11 active threat actors**, **28 active malware**, and **179 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 **21 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>Dire Wolf</u>	SHA256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3,8fdee53152ec985ffeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
	SHA1	ed7c9fbd42605c790660df86b7ec325490f6d827,4a5852e9f9e20b243d8430b229e41b92949e4d69
	MD5	a71dbf2e20c04da134f8be86ca93a619,aa62b3905be9b49551a07bc16eaad2ff
	TOX ID	B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2
	TOR Address	hxxp[:]//direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd[.]onion
	File Name	data345.exe
<u>RondoDox</u>	SHA256	0a9ebbcecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9,9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd,6c81fd73b4bef6fef379cbefdcce7f374ea7e6bf1bf0917cf4ca7b72d4cee788,a55a3859a203ca2bae7399295f92aeae61d845ffa173c1938f938f5c148eef99,57573779f9a62e ECB80737d41d42165af8bb9884579c50736766abb63d2835ba,3daa53204978b7797bd53f5c964eed7a73d971517a764785ce3ab65a9423c2e7,8bf8928bc255e73e0b5b0ce13747c64d82d5f2647da129f189138773733ac21f,20a24b179bdbbdcc0053838c0484ea25eff6976f2b8cb5630ab4efb28b0f06b5,42aa715573c7d2fca01914504cb7336db715d73d1e20d23e4bd37f2e4f4fe389
<u>Lumma</u>	SHA256	acbaa6041286f9e3c815cd1712771a490530f52c90ce64da20f28cfa0955a5ca

Attack Name	TYPE	VALUE
<u>NordDragonScan</u>	SHA256	f8403e30dd495561dc0674a3b1aedaea5d6839808428069d98e30e19bd6dc045,fbffe681c61f9bba4c7abcb6e8fe09ef4d28166a10bfeb73281f874d84f69b3d,39c68962a6b0963b56085a0f1a2af25c7974a167b650cf99eb1acd433ecb772b,9d1f587b1bd2cce1a14a1423a77eb746d126e1982a0a794f6b870a2d7178bd2c,7b2b757e09fa36f817568787f9eae8ca732dd372853bf13ea50649dbb62f0c5b,f4f6beea11f21a053d27d719dab711a482ba0e2e42d160cefdbdad7a958b93d0
<u>Interlock ransomware</u>	SHA256	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e,a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3,2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb,8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54,28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f
<u>Interlock PHP RAT</u>	SHA256	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3,8afd6c0636c5d70ac0622396268786190a428635e9cf28ab23add939377727b0
	IPv4	64[.]95[.]12[.]71,184[.]95[.]51[.]165
	Domain	existed-bunch-balance-councils[.]trycloudflare[.]com,ferrari-rolling-facilities-lounge[.]trycloudflare[.]com,galleries-physicians-psp-wv[.]trycloudflare[.]com,evidence-deleted-procedure-bringing[.]trycloudflare[.]com,nowhere-locked-manor-hs[.]trycloudflare[.]com,ranked-accordingly-ab-hired[.]trycloudflare[.]com
<u>Octalyn Stealer</u>	SHA256	8bd9925f7b7663ca2fcb305870248bd5de0c684342c364c24ef24bffbcdcd8b
<u>GLOBAL Ransomware</u>	SHA256	a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73
	TOR Address	vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id[.]onion,gdbkvfe6g3whrzkdlibytksygk45zwgmznzh5i2xmqyo3mrpipysjaggyd[.]onion

Attack Name	TYPE	VALUE
<u>GhostContainer</u>	MD5	01d98380dfb9211251c75c87ddb3c79c
	SHA1	2bb0a91c93034f671696da64a2cf6191a60a79c5
	SHA256	87a3aefb5cdf714882eb02051916371fbf04af2eb7a5ddeae4b6b441b2168e36
	Filename	App_Web_Container_1.dll
<u>Voldemort</u>	SHA256	1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb, ec5fef700d1ed06285af1f2d01fa3db5ea924de3c2da2f0e6b7a534f69d8409c, cd009ea4c682b61963210cee16ed663eee20c91dd56483d456e03726e09c89a7
<u>Ghost Crypt</u>	SHA256	69a40bd2f667845ab95ad8438dae390f2e8b9680f4d30cb20e920c45cda565f9
<u>AllaKore RAT</u>	SHA256	20fe630a63dd1741ec4ade9fe05b2e7e57208f776d5e20bbf0a012fea96ad0c0, f76b456cf2af1382325c704bf70b5168d28d30da0f3d0a5207901277e01db395, 4bf4bcf1cc45d9e50efbd184aad827e2c81f900a53961cf4fbeat90fa31ca7549, fed1c094280d1361e8a9aafdb4c1b3e63e0f2e5bb549d5d737d0a33f2b63b4b8, 5d16547900119112c12a755e099bed1fafe1890869df4db297a6a21ec40185b0, e9cd7c4db074c8e7c6b488a724be1cd05c8536dae28674ce3aa48ebb258e3c31, 32ef3a0da762bc88afb876537809350a885bbbc3ec59b1838e9e9ccc0a04b081, d8343068669d8fbb52b0af87bd3d4f3579d76192d021b37b6fd236b0973e4a5d, 53b85d1b7127c365a4ebae5f22ed479cd5d7e9efc716fb9df68ebdd18551834a, 84b046a4dbfcd9d4b2d62b4bc8faaf4c6395696f1e688f464bc9e0b760885263, 50e5cd438024b34ba638e170f6e4595b0361dedb0ea925d06d06f68988468ddf
<u>AllaKore RAT</u>	Domain	manzisuape[.]com, siperasul[.]com, cupertujo[.]com, idaculipa[.]com, mepunico[.]com, barrosuon[.]com, tllelmeuas[.]com

Attack Name	TYPE	VALUE
<u>SystemBC</u>	Domain	pachisuave[.]com
<u>EAGLET</u>	IPv4	185[.]225[.]17[.]104, 188[.]127[.]254[.]44
<u>TINYSHELL</u>	MD5	2c89a18944d3a895bd6432415546635e, aac5d83d296df81c9259c9a533a8423a, 8023d01ffb7a38b582f0d598afb974ee, 5724d76f832ce8061f74b0e9f1dcad90, e7622d983d22e749b3658600df00296d, b9e4784fa0e6283ce6e2094426a02fce, bf80c96089d37b8571b5de7cab14dd9f, 3243e04afe18cc5e1230d49011e19899
	SHA1	50520639cf77df0c15cc95076fac901e3d04b708, 1a6d07da7e77a5706dd8af899ebe4daa74bbbe91, 06a1f879da398c00522649171526dc968f769093, f8697b400059d4d5082eee2d269735aa8ea2df9a, cf7af504ef0796d91207e41815187a793d430d85, 01735bb47a933ae9ec470e6be737d8f646a8ec66, cec327e51b79cf11b3eeffebf1be8ac0d66e9529, 2e9215a203e908483d04dfc0328651d79d35b54f
	SHA256	98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14 d244d8373888, 5bef7608d66112315eefff354dae42f49178b7498f994a728ae6 203a8a59f5a2, c0ec15e08b4fb3730c5695fb7b4a6b85f7fe341282ad469e4e14 1c40ead310c3, 5995aaff5a047565c0d7fe3c80fa354c40e7e8c3e7d4df292316c 8472d4ac67a, 905b18d5df58dd6c16930e318d9574a2ad793ec993ad2f68bca 813574e3d854b, e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd411 82deea978400ed, 3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd 1065723f11f7e, 7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc 3ae56cfd13b4
	IPv4:Port	129[.]126[.]109[.]50[:]:22, 116[.]88[.]34[.]184[:]:22, 223[.]25[.]78[.]136[:]:22, 45[.]77[.]39[.]28[:]:22, 101[.]100[.]182[.]122[:]:22, 118[.]189[.]188[.]122[:]:22, 158[.]140[.]135[.]244[:]:22, 8[.]222[.]225[.]8[:]:22

Attack Name	TYPE	VALUE
<u>Remcos</u>	SHA256	5cf4a8c83f8591950c24c8b5d79c5464e4cb1b608fc61775f605d6a3503c73c3, 1728133a5a75adc097d2b5dee5693c5b1b72d25832435213bada40be433b2f75
<u>AsyncRAT</u>	SHA256	394908cbe5ba04a3b772ef11ea6a2c6a0c8d3d9689c89ccd1410aaa583bb07d7, 48ee878fetc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0, 2e432426a7a0a10a0068c035368f749c298e1ef1add61e31a8b25da74676fcaa, 2a84f9440f120edd032eddb4b61339ee184743d47805e2ed50572ca4905c1fdd, 66663cf3596b0e6fd2721d81f91cda058ca61feb46f9943ef1a91fec7a68590d, 666f0c305b0a6cc558192918bc144c3119d898c33656101395140d93e9e10e69, fa32ea24d1a6041be009ad0c59ce61f3d00e0588700c709c0222ecd8c8c3753, 81ffcabc8db8db4f42ee4d53f35d47e5cca9aba8fadf972a97596b79492cb03
<u>NimDoor</u>	SHA256	469fd8a280e89a6edd0d704d0be4c7e0e0d8d753e314e9ce205d7006b573865f
<u>DEVMAN</u>	SHA256	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403
	SHA1	4a34bbad85312ef34b60818a47f7b5bb8e9a7e26
	MD5	e84270afa3030b48dc9e0c53a35c65aa
	Filename	e47qfsnz2trbkhnt.devman
	Mutex	hsfjuukjzloqu28oajh727190
	Tox ID	9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
	TOR Address	qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd[.]onion
<u>Hpingbot</u>	SHA256	3359037b5a331ecf79ab9aa114f673e96a227a038fdb377badfbe16b5eaa4e7f
<u>NailaoLocker</u>	SHA256	46f3029fcc7e2a12253c0cc65e5c58b5f1296df1e364878b178027ab26562d68
<u>Bert Ransomware (aka Water Pombero)</u>	SHA256	c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db
<u>Auto-color</u>	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43

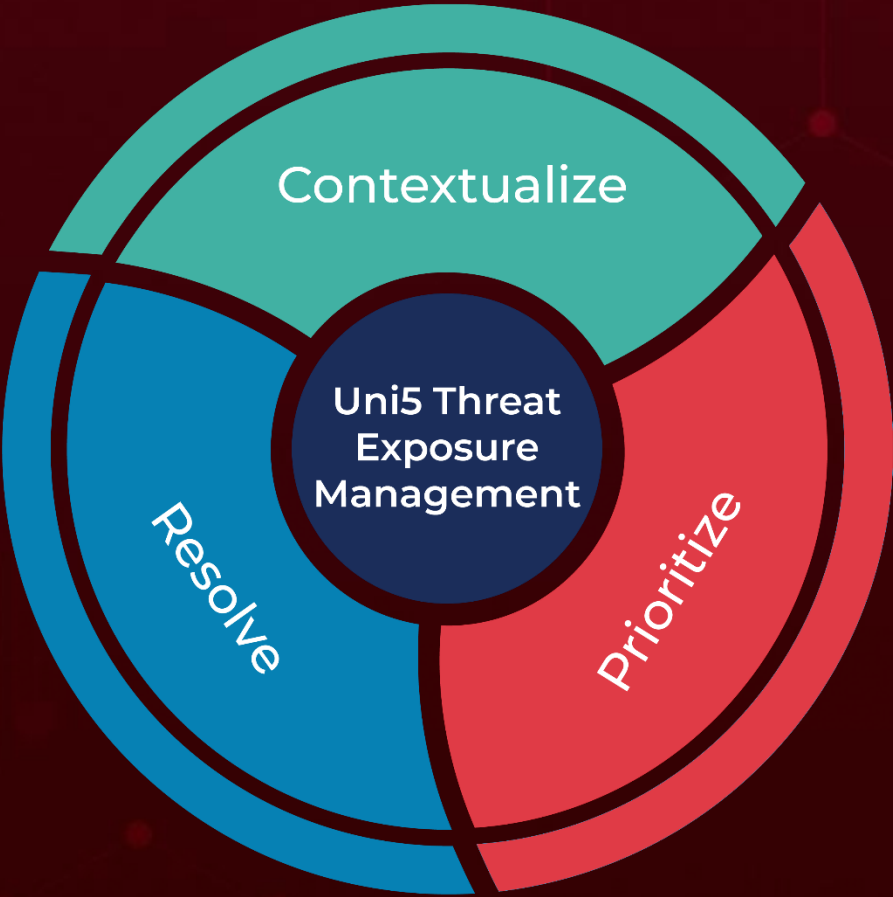
Attack Name	TYPE	VALUE
<u>Ghost RAT</u>	MD5	1244b7d19c37baab18348fc2bdb30383
	SHA1	365888661b41cbe827c630fd5eea05c5ddc2480d
	SHA256	1e5c37df2ace720e79e396bbb4816d7f7e226d8bd3ffc3cf8846c4cf49ab1740
	IPv4:Port	104[.]234[.]15[.]90[:]19999
<u>PhantomNet (SManager)</u>	IPv4:Port	45[.]154[.]12[.]93[:]2233
	MD5	a74c5c49b6f1c27231160387371889d3
	SHA1	fb32d8461ddb6ca2f03200d85c09f82fb6c5bde3
	SHA256	c9dac9ced16e43648e19a239a0be9a9836b80ca592b9b36b70d0b2bdd85b5157

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

What Next?

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

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON
August 5, 2025 • 1:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com