Date of Publication
July 1, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JUNE 2025

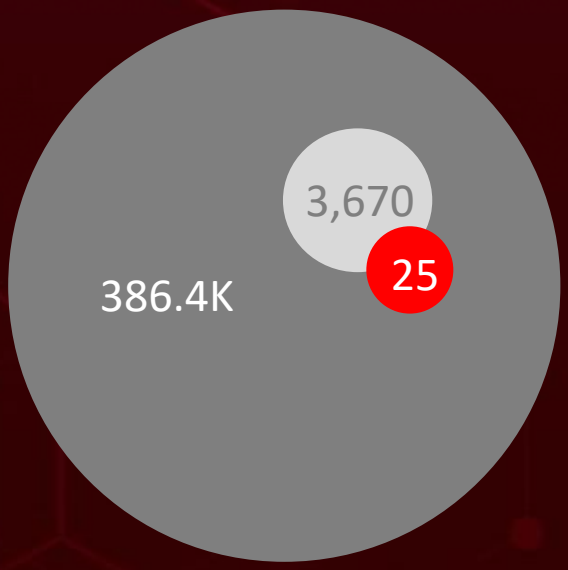
Table Of Contents

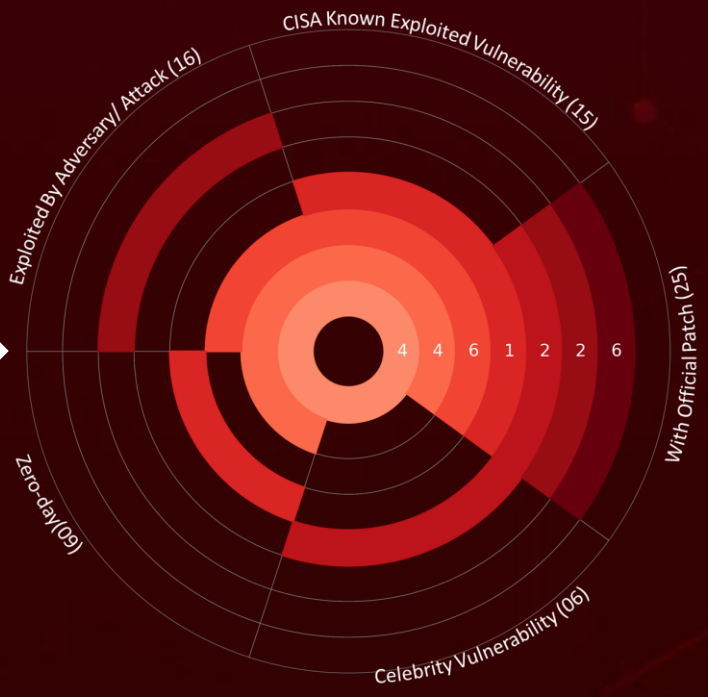
Summary

June unleashed chaos across the cybersecurity landscape, with active exploitation of **five** celebrity vulnerabilities and **nine** zero-days. One of the most urgent threats was a critical zero-day in Google Chrome's V8 engine, **CVE-2025-5419**, already being exploited in the wild. This flaw allows malicious websites to corrupt memory and potentially seize control of a device simply by visiting a compromised page.

In parallel, **Stealth Falcon**, a long-operating cyber-espionage group, weaponized a Windows zero-day CVE-2025-33053 in a targeted attack against a **Turkish defense firm**. A critical **CVE-2025-24016** Wazuh vulnerability fueled a surge in **Mirai botnet** attacks globally. Adding to the volatility, a newly uncovered flaw, **CVE-2025-49144**, in the **Notepad++ installer** could let attackers hijack systems by placing a malicious file in the same directory as the installer. This vulnerability is addressed in Notepad++ v8.8.2, and users are strongly advised to update.

Meanwhile, **Water Curse**, a financially motivated threat group, weaponizes GitHub by hosting fake developer tools that deploy multi-stage malware once cloned and executed. **APT28**, a Russian state-sponsored actor, targeted government entities with spear-phishing campaigns via Signal, delivering malicious documents that unleashed **BEARDSHELL** and **COVENANT** malware. As cyber threats intensify, vigilance and adaptability are no longer optional. Organizations must stay ahead of adversaries, fortifying their defenses against an ever-evolving digital battleground.





Total Vulnerabilities Published

Vulnerabilities Published in the Month

Exploited Vulnerabilities

Insights

In June 2025, a geopolitical cybersecurity landscape unfolds, revealing **United States, United Kingdom, Canada, Turkey,** and **Saudi Arabia** as the top-targeted countries

Highlighted in **June 2025** is a cyber battleground encompassing the **Government, Financial, Technology, Cryptocurrency,** and **Healthcare** sectors, designating them as the top industries

New Phishing Campaign Masquerades as Rothschild Career Offers to Hijack Devices

SERPENTINE#CLOUD Campaign Turns Cloudflare Tunnels into Malware Pipelines

Famous Chollima North Korean Hackers Target Crypto Pros with New **PylangGhost RAT**

Brazil First, The World Next: The Phantom Enigma Phishing Operation

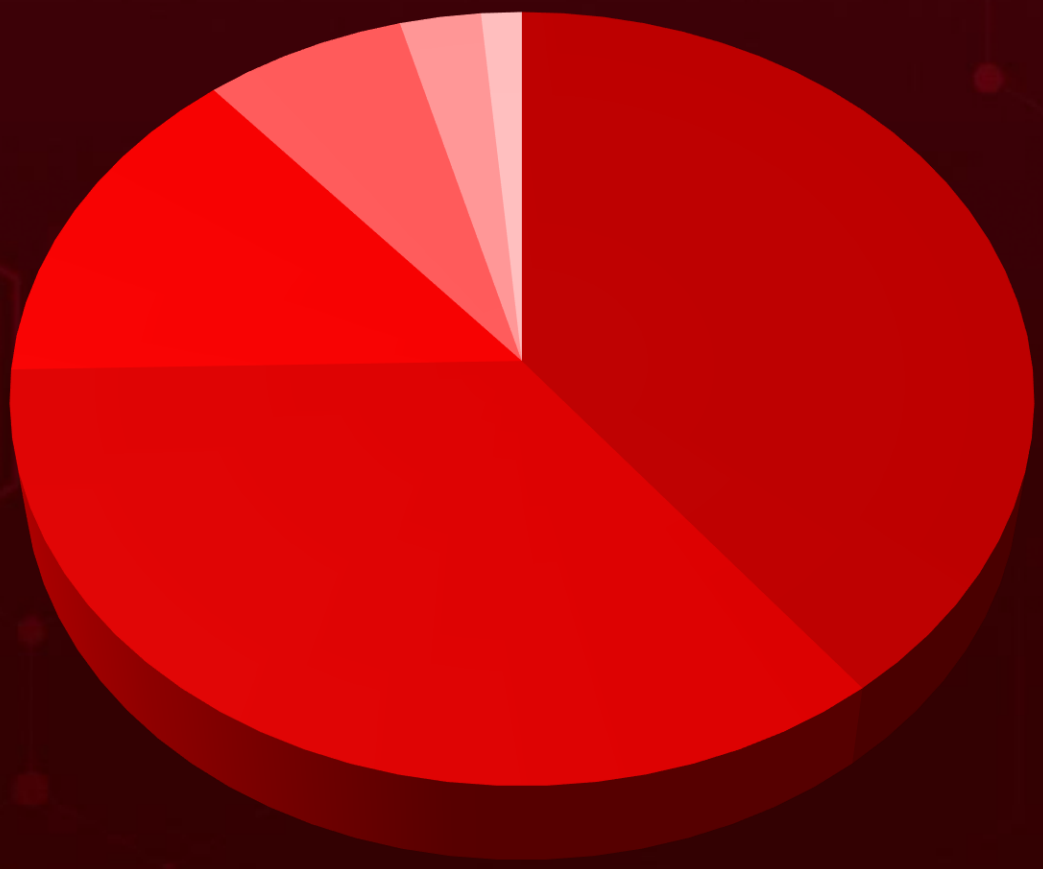
CitrixBleed 2 Poised for Active Attacks Patch Before Hackers Strike

Tax Season Turns Treacherous as **HoldingHands RAT** Infiltrates **Taiwanese** Networks

Operation ToyBox Story: North Korea's Fileless Espionage Campaign Uncovered

Crypto Wallets, Passwords, and Cookies: Katz Stealer Takes It All

Threat Landscape



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

Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32711	✗	Microsoft 365 Copilot	-
	CISA KEV		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:365_copilot:*:*:*:*:*:*:*:*	-
EchoLeak (M365 Copilot Information Disclosure Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-77	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1005: Data from Local System	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27065	✓	Microsoft Exchange Server	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	Prometei botnet
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1059 : Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26858	✓	Microsoft Exchange Server	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*	Prometei botnet
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059 : Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0144	✓	Microsoft SMBv1	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:server_message_block:1.0:*:*:*:*:*:*:*	Prometei botnet
EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059 : Command and Scripting Interpreter, T1210 : Exploitation of Remote Services	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0708	✓	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Prometei botnet
BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-416	T1021.001: Remote Desktop Protocol, T1068 : Exploitation for Privilege Escalation, T1059: Command and Scripting	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5777	✕	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	-
	CISA KEV		
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	✕	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:*:*:*	-
CitrixBleed 2 (Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability)	**CWE ID**	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-125	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-2025-42999	SAP NetWeaver Deserialization Vulnerability	SAP NetWeaver Java systems	✓	✓	✓
CVE-2024-57727	SimpleHelp Path Traversal Vulnerability	SimpleHelp remote support software	✗	✓	✓
CVE-2024-57728	SimpleHelp Arbitrary File Upload Vulnerability	SimpleHelp remote support software	✗	✗	✓
CVE-2024-57726	SimpleHelp Privilege Escalation Vulnerability	SimpleHelp remote support software	✗	✗	✓
CVE-2025-5419	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Google Chrome	✓	✓	✓
CVE-2025-48827	vBulletin Remote Code Execution Vulnerability	vBulletin	✗	✗	✓
CVE-2025-48828	vBulletin Remote Code Execution Vulnerability	vBulletin	✗	✗	✓
CVE-2025-49113	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube Webmail	✗	✗	✓
CVE-2025-20286	Cisco Identity Services Engine Static Credential Vulnerability	Cisco ISE	✗	✗	✓
CVE-2025-33053	Microsoft Windows External Control of File Name or Path Vulnerability	Windows	✓	✓	✓
CVE-2025-32711	EchoLeak (M365 Copilot Information Disclosure Vulnerability)	Microsoft 365 Copilot	✗	✗	✓
CVE-2022-41128	Microsoft Windows Scripting Languages Remote Code Execution Vulnerability	Windows	✓	✓	✓
CVE-2025-24016	Wazuh Server Deserialization of Untrusted Data Vulnerability	Wazuh Server	✗	✓	✓
CVE-2025-3248	Langflow Missing Authentication Vulnerability	Langflow	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2015-2291	Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	IQVW32.sys and IQVW64.sys in the Intel Ethernet diagnostics driver for Windows	✗	✓	✓
CVE-2021-35464	ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability	ForgeRock AM server	✗	✓	✓
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi, VMware vCenter Server, VMware Cloud Foundation	✗	✓	✓
CVE-2021-27065	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26858	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2017-0144	EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	Microsoft SMBv1	✓	✓	✓
CVE-2019-0708	BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	Windows	✓	✓	✓
CVE-2025-2783	Google Chromium Mojo Sandbox Escape Vulnerability	Google Chrome (Windows)	✓	✓	✓
CVE-2025-49144	Notepad++ Privilege Escalation Vulnerability	Notepad++ Versions 8.8.1 and prior	✗	✗	✓
CVE-2025-6543	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	NetScaler ADC and NetScaler Gateway	✗	✗	✓
CVE-2025-5777	CitrixBleed 2 (Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability)	NetScaler ADC and NetScaler Gateway	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
DragonForce	Ransomware	CVE-2024-57727 CVE-2024-57728 CVE-2024-57726	SimpleHelp remote support software v5.5.7 and before, Windows	✓	Exploiting Vulnerabilities, Phishing
Lyrix	Ransomware	-	Windows	-	-
NetSupport RAT	RAT	-	Windows	-	Phishing
Chaos RAT	RAT	-	-	-	Phishing
Mesh Agent	Hack Tool	-	-	-	Phishing
Blitz	RAT	-	Windows	-	Fake Standoff 2 game cheats on Telegram
XMRig	Miner	-	Windows	-	Fake Standoff 2 game cheats on Telegram
Atomic Stealer	Stealer	-	Windows and macOS	-	Social Engineering
VELETRIX	Loader	-	-	-	Spear-phishing email
VShell	OST framework	-	-	-	Spear-phishing email
Myth Stealer	InfoStealer	-	-	-	Fraudulent gaming websites
Horus Agent	Framework	CVE-2025-33053	Web Distributed Authoring and Versioning (WebDAV)	✓	Phishing
Horus Loader	Loader	CVE-2025-33053	Web Distributed Authoring and Versioning (WebDAV)	✓	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
RoKRAT	Backdoor	CVE-2022-41128	Microsoft Windows	✓	Spear-phishing
AsyncRAT	RAT	-	Windows	-	Spear-phishing Link
Skuld Stealer	Stealer	-	Windows	-	Spear-phishing Link
Mirai	Botnet	CVE-2025-24016	Wazuh Server	✓	Exploiting Vulnerability
Resbot	Botnet	CVE-2025-24016	Wazuh Server	✓	Exploiting Vulnerability
Fog ransomware	Ransomware	-	Windows	-	-
Anubis	Ransomware	-	Windows, Linux, NAS, and ESXi (VMware) environments	-	Phishing
Sakura RAT	RAT	-	Windows	-	-
DULLRAT	Backdoor	-	Windows	-	-
HoldingHands RAT	RAT	-	Windows	-	Phishing
Flodrix	Botnet	CVE-2025-3248	Langflow	✓	Exploiting vulnerability
Gunra Ransomware	Ransomware	-	Windows	-	Phishing
PylangGhost	RAT	-	Windows	-	Phishing through fake job offers
RevengeRAT	RAT	-	Windows	-	Phishing
Katz Stealer	Stealer	-	Windows	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BERT Ransomware	Ransomware	-	Windows, Linux	-	Phishing
Prometei	Botnet	CVE-2021-27065 CVE-2021-26858 CVE-2017-0144 CVE-2019-0708	Windows, Linux	✓	Exploiting vulnerabilities
PoshC2	Tool	-	-	-	Phishing
Chisel	Tool	-	-	-	-
Classroom Spy	Tool	-	-	-	-
BeardShell	Backdoor	-	Windows	-	Phishing
Covenant	Framework	-	Windows	-	Phishing
SlimAgent	Tool	-	Windows	-	Dropped via Covenant
Trinper	Backdoor	-	Windows	-	Phishing

Adversaries Summary

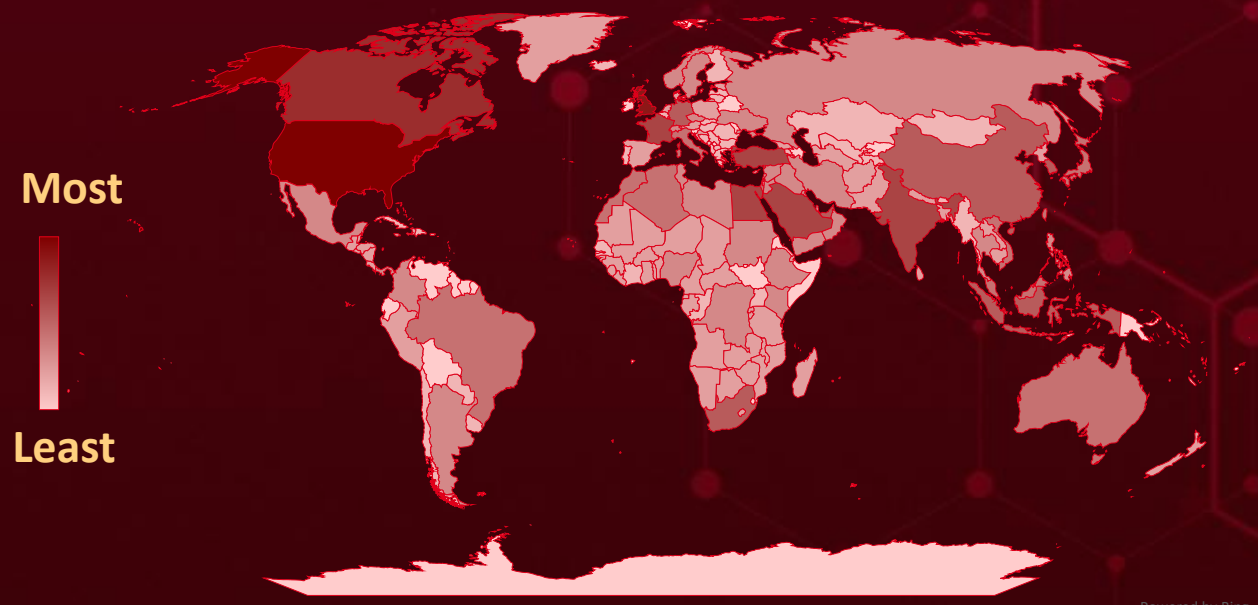
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
sw1zzx	Information Theft, Espionage, Financial Gain	Russian-speaking	-	Blitz, XMRig	Windows
Stealth Falcon	Information Theft and Espionage	UAE	CVE-2025-33053	Horus Agent, Horus Loader	Web Distributed Authoring and Versioning (WebDAV)
APT37	Information Theft and Espionage	North Korea	CVE-2022-41128	RoKRAT	Microsoft Windows
Water Curse	Financial gain	-	-	Sakura RAT, DULLRAT	Windows
Famous Chollima	Financial Gain, Information Theft and Espionage	North Korea	-	PylangGhost	-
Scattered Spider	Financial gain	Suspected UK and US	CVE-2015-2291 CVE-2021-35464 CVE-2024-37085	DragonForce Ransomware	-
APT28	Information Theft and Espionage	Russia	-	BeardShell, Covenant, and SlimAgent	Windows
TaxOff	Information Theft and Espionage	-	-	Trinper	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
SAP	Application Server Java	SAP NetWeaver Java systems Version 7.1x and above
simplehelp	Remote Desktop / Remote Support Tool	SimpleHelp remote support software v5.5.7 and before
	Web Browser	Google Chrome prior to 137.0.7151.68 Microsoft Edge, Google Chrome (Windows) Version Before 134.0.6998.178
vBulletin	Open-Source Forum Software	vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3
	Web Application - Webmail Client	Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11
CISCO	Network Access Control (NAC) System / Security Appliance	Cisco ISE versions: 3.1 to 3.4
Microsoft	Operating Systems	Windows: 10 - 11 24H2, Windows Server: 2008 - 2025, Windows: 7 - 11 22H2 10.0.22621.521, Windows Server: 2008 - 2022 20H2, Windows Server: 2019 - 2022 23H2
	AI-powered assistant	Microsoft 365 Copilot
	Email Server	Microsoft Exchange Server
	File Sharing Protocol	Microsoft SMBv1
wazuh.	SIEM/XDR Security Platform	Wazuh Server version 4.4.0 to 4.9.0
	Web-based LLM orchestration tool	Langflow versions prior to 1.3.0

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
intel	Windows kernel-mode driver	IQVW32.sys before 1.3.1.0 and IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows
ForgeRock	Identity and Access Management (IAM) solution	ForgeRock AM server before 7.0
vmware	Hypervisor, Virtualization management server, Cloud infrastructure platform	VMware ESXi, VMware vCenter Server, VMware Cloud Foundation
Notepad++	Text Editor	Notepad++ Versions 8.8.1 and prior
citrix	Application Delivery Controller (ADC), Secure Access Gateway, FIPS-Compliant and NDcPP-Compliant Security Devices	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46, 13.1 BEFORE 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP, NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS

Targeted Countries



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

Color	Countries
	United States
	United Kingdom
	Canada
	Turkey
	Saudi Arabia
	Egypt
	France
	India
	South Africa
	China
	South Korea
	United Arab Emirates
	Germany
	Singapore
	Indonesia
	Brazil
	Japan
	Taiwan
	Algeria
	Morocco
	Australia
	Italy

Color	Countries
	Vietnam
	Israel
	Malaysia
	Sudan
	Ukraine
	Bahrain
	Yemen
	Kuwait
	Mexico
	Switzerland
	Colombia
	Tunisia
	Nigeria
	Jordan
	Norway
	Iraq
	Oman
	Sweden
	Panama
	Syria
	Philippines
	Thailand

Color	Countries
	Qatar
	Ethiopia
	Russia
	Argentina
	Czech Republic
	Kenya
	Democratic Republic of Congo
	Libya
	Iran
	Lebanon
	Angola
	Brunei
	Zambia
	Denmark
	Cambodia
	Djibouti
	Togo
	Dominica
	Nicaragua
	Aruba
	Burkina Faso
	El Salvador
	Saint Vincent and the Grenadines
	Equatorial Guinea

Color	Countries
	Central African Republic
	Estonia
	Costa Rica
	Austria
	Netherlands
	Gabon
	North Korea
	Georgia
	Palestine
	Ghana
	Puerto Rico
	Greenland
	Saint Kitts and Nevis
	Guadeloupe
	Seychelles
	Guatemala
	Sri Lanka
	Guinea
	Tanzania
	Guinea-Bissau
	Turkmenistan

Color	Countries
	Haiti
	Curacao
	Honduras
	Nepal
	Bahamas
	New Zealand
	Bangladesh
	Niger
	Barbados
	British Virgin Islands
	Jamaica
	Pakistan
	Belize
	Peru
	Benin
	Poland
	Bermuda
	Burundi
	Laos
	Rwanda
	Afghanistan
	Saint Lucia

Targeted Industries

Most

Government
Financial
Technology
Cryptocurrency
Healthcare

Gaming
Manufacturing

Insurance
Tele-communications
Media
Construction
Retail
Professional Services
Food products
Transportation

Energy
Defence
Consumers
Banking
Real Estate
Electrical
Legal

Pharmaceutical
Engineering
Entertainment
Oil & Gas
Chemical
Political Entities
Think-Tanks
Education
Marine

Aerospace
Logistics
Utilities
Hospitality

Agriculture
Critical Infrastructure
NGOs
Aviation
Religious
E-commerce

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1036** Masquerading
T1071 Application Layer Protocol	**T1082** System Information Discovery	**T1588** Obtain Capabilities	**T1059.001** PowerShell	**T1041** Exfiltration Over C2 Channel
T1588.006 Vulnerabilities	**T1204.002** Malicious File	**T1190** Exploit Public-Facing Application	**T1071.001** Web Protocols	**T1113** Screen Capture
T1083 File and Directory Discovery	**T1140** Deobfuscate/ Decode Files or Information	**T1497** Virtualization /Sandbox Evasion	**T1070** Indicator Removal	**T1562** Impair Defenses
T1057 Process Discovery	**T1070.004** File Deletion	**T1105** Ingress Tool Transfer	**T1547** Boot or Logon Autostart Execution	**T1056** Input Capture

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
DragonForce	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9, d626eb0565fac677fdc13fb0555967dc31e600c74fbbd110b744f8e3a59dd3f9, ba1be94550898eedb10eb73cb5383a2d1050e96ec4df8e0bf680d3e76a9e2429
Mesh Agent	SHA256	07f7ce55e75afda05241c70710d5c6769909d94193e41b370a29b5dca3ef1f3d, 12155ad4d117ea2b13131df52de4045e635e100d45bac057d6f5674e894dec99
Blitz	SHA256	0e80fe5636336b70b1775e94aaa219e6aa27fcf700f90f8a5dd73a22c898d646, cacc1f36b3817e8b48fabbb4b4bd9d2f1949585c2f5170e3d2d04211861ef2ac, aa5cd0219e8a0bd2e7d6c073f611102d718387750198bff564c20ca7ebada309, f3b7bbe1079974fd505abaadbcf4dc0517620592eacbbe5f314a76775dd760c2, cdf192e92d14b9d7e1201c23621c4e0b8ee0673c192bdd734afd97519afef271, 6441e7000713f96c7ae114ce62378556d01fa29d435a5be0f11a5e80be9a26ed, b1b1ce259fcf5127c3477e278c3696dc7d15db63b673fdcf75e1deb89a0f6fd1, 5ef29d6d4f72e62e0d5a1d0b85eed70b729cd530c8cb2745c66a25f5b5c7299e, 5fc132b054099a1a65f377a3a22b003a6507107f3095371b44dbf5e098b02295, b18e21e50f1c346c83c4cba933b6466ada22febaafa25c03ac01122a12164375, a34a4a7c71de2d4ec4baf56fd143d27eeedebb785a2ba3e0740b92e62efd81ea, bedeafd3680cad581a619fb58aa4f57ed991c4a8dd94df46ef9cbd08a8dd6052, ae2f4c49f73f6d88b193a46cd22551bb31183ae6ee79d84be010d6acf9f2ee57, 88e2d0d59a9751e4ce5223951f5a75b1731b1ee82d18705aba83ba4bd7e8e5c1
XMRig	SHA256	47ce55095e1f1f97307782dc4903934f66beec3476a45d85e33e48d63e1f2e15

Attack Name	TYPE	VALUE
Horus Loader	SHA256	da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa
RoKRAT	SHA256	92ab3a9040f5e620bc4b76295239c5240130d968c6cbeaa7dc555d2cf19bfae1, d182834a984c9f5b44ea0aca5786223a78138ff23d33362ab699c76bf6987261, 9b8218774c3abc0a449cfc490f12e81155af00ec90c2e1d630a61c29f70a98cb
Mirai	SHA256	dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9, 7b659210c509058bd5649881f18b21b645acb42f56384cbd6dcb8d16e5aa0549, 64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4eb692b08f52b0f, 4c1e54067911aeb5aa8d1b747f35fdcdfdf4837cad60331e58a7bbb849ca9eed, 811cd6ebeb9e2b7438ad9d7c382db13c1c04b7d520495261093af51797f5d4cc, 90df78db1fb5aea6e21c3daca79cc690900ef8a779de61d5b3c0db030f4b4353, 8a58fa790fc3054c5a13f1e4e1fcb0e1167dbfb5e889b7c543d3cdd9495e9ad6, c9df0a2f377ffab37ede8f2b12a776a7ae40fa8a6b4724d5c1898e8e865cfea1, 6614545eec64c207a6cc981fccae8077eac33a79f286fc9a92582f78e2ae243a
Resbot	SHA256	9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b
AsyncRAT	SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a
	Domain	microads[.]top
	URL	hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/AClient[.]exe,

Attack Name	TYPE	VALUE
AsyncRAT	URLs	hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/AClient[.]exe, hxxps[:]//pastebin[.]com/raw/ftknPNF7, hxxps[:]//pastebin[.]com/raw/NYpQCL7y, hxxps[:]//pastebin[.]com/raw/QdseGsQL
	IPv4	101[.]99[.]76[.]120, 87[.]120[.]127[.]37, 185[.]234[.]247[.]8
Gunra Ransomware	Filename	gunraransome.exe R3ADM3.txt
	MD5	9a7c0adedc4c68760e49274700218507
	SHA1	77b294117cb818df701f03dc8be39ed9a361a038
	SHA256	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
	Tox ID	2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22
	TOR Address	gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd[.]onion
Horus Agent	SHA256	ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b
PylangGhost	SHA256	267009d555f59e9bf5d82be8a046427f04a16d15c63d9c7ecca749b11d8c8fc3
Katz Stealer	Domain	katz-stealer[.]com, katzstealer[.]com
	SHA256	6dc8e99da68b703e86fa90a8794add87614f254f804a8d5d65927e0676107a9d, e73f6e1f6c28469e14a88a633aef1bc502d2dbb1d4d2dfcaaef7409b8ce6dc99, 2798bf4fd8e2bc591f656fa107bd871451574d543882ddec3020417964d2faa9, e345d793477abbecc2c455c8c76a925c0dfe99ec4c65b7c353e8a8c8b14da2b6, c601721933d11254ae329b05882337db1069f81e4d04cd4550c4b4b4fe35f9cd, fdc86a5b3d7df37a72c3272836f743747c47bfbc538f05af9ecf78547fa2e789, 25b1ec4d62c67bd51b43de181e0f7d1bda389345b8c290e35f93ccb444a2cf7a, 964ec70fc2fdf23f928f78c8af63ce50aff058b05787e43c034e04ea6cbe30ef, d92bb6e47cb0a0bdbb51403528ccfe643a9329476af53b5a729f04a4d2139647,

Attack Name	TYPE	VALUE
Katz Stealer	SHA256	b249814a74dff9316dc29b670e1d8ed80eb941b507e206ca0dfdc4ff033b1c1f, 925e6375deaa38d978e00a73f9353a9d0df81f023ab85cf9a1dc046e403830a8, 96ada593d54949707437fa39628960b1c5d142a5b1cb371339acc8f86dbc7678, b912f06cf65233b9767953ccf4e60a1a7c262ae54506b311c65f411db6f70128, 2852770f459c0c6a0ecfc450b29201bd348a55fb3a7a5ecdcc9986127fdb786b, 5dd629b610aee4ed7777e81fc5135d20f59e43b5d9cc55cdad291fcf4b9d20be
BERT Ransomware	SHA256	6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02, ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be, f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799, 78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c, 8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311
BeardShell	SHA256	d1deeaf0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a, 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1
Covenant	SHA256	84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460
SlimAgent	SHA256	9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c
	MD5	889b83d375a0fb00670af5276816080e
Trinper	SHA256	f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666, d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2, 99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96
	SHA1	20943541522cd3937b275c42016ad3e1e64e3f38, d9fa06025ecd08fc417c9948148e7827280365f2, 39ecc624bd2d52db083424fbb3a47b0c60f5ae4e
	MD5	16f6227f760487a70a3168cf9a497ac3, dba17d2faa311f28e68477ea5cc1a300, 1b7b4608f2c9e0a4863a00edd60c3b78

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-42999	✗	SAP NetWeaver Java systems Version 7.1x and above	UNC5221, UNC5174, CL-STA-0048
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:netweaver:7.5:*:*:*:*:*:*:*	KrustyLoader, Qilin ransomware, BianLian, RansomExx, PipeMagic
SAP NetWeaver Deserialization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57727	✗	SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1566: Phishing, T1190: Exploit Public-Facing Application	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57728	✗	SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Arbitrary File Upload Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE- 59 CWE-22	T1566: Phishing, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57726	✗	SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5419	✗	Google Chrome prior to 137.0.7151.68 Microsoft Edge	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1190: Exploit Public-Facing Application, T1566: Phishing, T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48827	✕	vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*:*:*	-
vBulletin Remote Code Execution Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48828	✕	vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vbulletin:vbulletin:*:*:*:*:*:*:*:*	-
vBulletin Remote Code Execution Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49113	✗	Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20286	✗	Cisco ISE versions: 3.1 to 3.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:3.0:*:*:*:*:*:*:*	-
Cisco Identity Services Engine Static Credential Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-259	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials, T1078: Valid Accounts	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-33053	✗	Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	Stealth Falcon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Horus Agent, Horus Loader
Microsoft Windows External Control of File Name or Path Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1071.002: File Transfer Protocols	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41128	✗	Windows: 7 - 11 22H2 10.0.22621.521, Windows Server: 2008 - 2022 20H2	APT37
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	RoKRAT
Microsoft Windows Scripting Languages Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24016	✗	Wazuh Server version 4.4.0 to 4.9.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wazuh:wazuh:*:*:*:*:*:*:*:*	Mirai, Resbot
Wazuh Server Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059.006: Python, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://github.com/wazuh/wazuh/releases/tag/v4.9.1

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-2291	✗	IQVW32.sys before 1.3.1.0 and IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows	Scattered Spider
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw32.sys:1.03.0.7:*:*:*:*:*:*:* cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw64.sys:1.03.0.7:*:*:*:*:*:*:*	-
Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1068: Exploitation for Privilege Escalation; T1499: Endpoint Denial of Service	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-35464	✗	ForgeRock AM server before 7.0	Scattered Spider
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:forgerock:access_management:*:*:*:*:*:*:*:* cpe:2.3:a:forgerock:openam:*:*:*:*:*:*:*:*	-
ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application; T1505.003: Server Software Component: Web Shell	https://backstage.forgerock.com/knowledge/advisories/article/a47894244

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37085	✗	VMware ESXi VMware vCenter Server VMware Cloud Foundation	Scattered Spider
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:internet_explorer:*:*:*:*:*:*:*	-
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2783	✗	Google Chrome (Windows) Version Prior to 134.0.6998.178	TaxOff
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*	Trinper
Google Chromium Mojo Sandbox Escape Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting; T1497 : Virtualization/Sandbox Evasion	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49144	✗	Notepad++ Versions 8.8.1 and prior	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:notepad-plus-plus:notepad:*:*:*:*:*:*:*	-
Notepad++ Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-276 CWE-272 CWE-427	T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	https://notepad-plus-plus.org/downloads/v8.8.2/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6543	✕	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46, 13.1 BEFORE 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP	-
	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	✕		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DragonForce	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. 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.	Exploiting Vulnerabilities, Phishing	CVE-2024-57727 CVE-2024-57728 CVE-2024-57726
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, Data Theft	SimpleHelp remote support software v5.5.7 and before
ASSOCIATED ACTOR			**PATCH LINK**
Scattered Spider			https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

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
Lyrix	Lyrix Ransomware is a Python-based malware strain that has been converted into a Windows executable using PyInstaller, enabling it to run seamlessly on Windows systems. Designed to specifically target Windows environments, Lyrix employs strong encryption algorithms to lock victims' files and appends a distinct file extension to each encrypted file, making identification straightforward yet recovery difficult without the decryption key. The ransomware also integrates sophisticated evasion techniques and persistence mechanisms, allowing it to avoid detection and maintain a foothold on compromised systems.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NetSupport RAT	NetSupport RAT (Remote Access Trojan) is a legitimate remote administration tool often exploited for malicious purposes. Cybercriminals use it to gain control over compromised systems, enabling them to execute commands, transfer files, and monitor activity.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote control 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 CVEs
Chaos RAT	Chaos RAT is a cross-platform, open-source remote access tool written in Go. First discovered in 2022 and continuously evolving through 2024 and into 2025, Chaos RAT was originally created for legitimate remote administration. However, threat actors have increasingly weaponized it to target both Windows and Linux systems. Typically delivered via phishing emails, Chaos RAT grants attackers' full control of infected machines, enabling them to steal sensitive data, run arbitrary commands, and establish persistent access. Notably, earlier versions of its web-based control panel contained serious vulnerabilities (now patched), which ironically posed risks not only to victims but also to the attackers using it.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise, Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mesh Agent	Mesh Agent RAT is a remote access tool designed to run on a wide range of devices, enabling remote management through a MeshCentral server. The agent is available for multiple operating systems, including Windows, various Linux distributions, macOS, and FreeBSD, and is compiled for several processor architectures such as x86-32, x86-64, ARM, and MIPS. Its cross-platform flexibility makes it a powerful tool for legitimate administration but also a potential asset for threat actors in malicious campaigns.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Hack tool		Remote Management	-
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
Blitz	Blitz is a Windows-based malware first detected in 2024, distributed via fake Standoff 2 game cheats on Telegram. It employs a two-stage infection process with a downloader and a versatile bot capable of keylogging, DoS attacks, and cryptomining.	Fake Standoff 2 game cheats on Telegram	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Denial-of-Service (DoS) attacks, Financial Losses	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
sw1zzx			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
XMRig	XMRig is an open-source cryptocurrency miner often exploited by cybercriminals in cryptojacking attacks, covertly harnessing victims' computing resources to mine Monero (XMR).	Fake Standoff 2 game cheats on Telegram	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Operational Disruption, Financial Losses	Windows
Miner			
ASSOCIATED ACTOR			**PATCH LINK**
sw1zzx			-

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
Atomic Stealer	Atomic Stealer, or AMOS, is a prevalent macOS-targeting malware designed to harvest and exfiltrate sensitive data, including account credentials, browser information, and cryptocurrency wallet details.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Financial Losses	Windows and macOS
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VELETRIX	VELETRIX is a custom implant that functions as a loader, establishing initial access on compromised systems. It uses basic anti-analysis techniques, notably leveraging the Sleep and Beep Windows APIs to evade detection and disrupt automated analysis.	Spear-phishing email	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload Delivery, Persistence Risk	-
Loader			
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
VShell	VShell is a well-known cross-platform OST framework developed in Golang. Originally released as open-source and later removed by its creator, it has been widely weaponized by China-aligned threat groups. The VShell implant establishes a persistent command-and-control (C2) channel, providing attackers with continuous remote access to compromised systems.	Spear-phishing email	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Persistent Remote Access, Information Theft	-
OST framework			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Myth Stealer	Myth Stealer is a Rust-based malware that continually evolves, adding features like clipboard hijacking to steal cryptocurrency. It exfiltrates passwords, browser cookies, saved credit cards, and screenshots to its operators. The malware is actively sold via subscription plans on Telegram.	Fraudulent gaming websites	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	-
InfoStealer			
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
Horus Agent	Horus Agent is a custom C++ based espionage tool. It employs advanced protections, including custom string encryption, control flow flattening, and API hashing to evade analysis. The implant can fingerprint systems, inject shellcode into legitimate processes, and remain dormant until receiving further instructions.	Phishing	CVE-2025-33053
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Persistent Remote Control	Web Distributed Authoring and Versioning (WebDAV)
Framework			
ASSOCIATED ACTOR			**PATCH LINK**
Stealth Falcon			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Horus Loader	Horus Loader is a custom, multi-stage C++ loader that leverages Code Virtualizer to transform code into custom virtual machine (VM) instructions, complicating reverse engineering. It serves as a lightweight alternative to the Themida protector. The loader is digitally signed, though with an outdated, timestamp-free signature, likely to evade certain security detections.	Phishing	CVE-2025-33053
		IMPACT	**AFFECTED PRODUCT**
TYPE		Initial Payload Delivery	Web Distributed Authoring and Versioning (WebDAV)
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
Stealth Falcon			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053

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
RoKRAT	RokRAT is a sophisticated remote access trojan that collects sensitive system data, captures live screenshots, monitors processes, and maintains encrypted command-and-control communications via cloud APIs on services like Dropbox, pCloud, and Yandex.	Spear-phishing	CVE-2022-41128
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft	Microsoft Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
APT37			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is a publicly available remote access trojan (RAT) hosted on GitHub. A modified variant achieves persistence by creating a scheduled task set to run at startup. On execution, it triggers a multi-step process to launch AsyncRAT within Windows Sandbox, which requires manual activation and a system reboot.	Spear-phishing Link	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote Control, Information Theft	Windows
RAT			
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
Skuld Stealer	Skuld Stealer specializes in data exfiltration, targeting browser credentials, gaming sessions, Discord tokens, and cryptocurrency wallet seed phrases. It also compromises Electron-based wallets like Exodus and Atomic by injecting malicious .asar files.	Spear-phishing Link	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Wallet Compromise, Facilitates Further Intrusions	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mirai	Mirai is a notorious malware targeting Internet of Things (IoT) devices by exploiting weak or default credentials. Compromised devices are enlisted into a botnet used for large-scale Distributed Denial of Service (DDoS) attacks. Its open-source release has spawned numerous variants.	Exploiting Vulnerability	CVE-2025-24016
		IMPACT	**AFFECTED PRODUCT**
TYPE		Device Hijacking, Network Overload	Wazuh Server
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/wazuh/wazuh/releases/tag/v4.9.1

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Resbot	ResBot, also known as Resentual, is a Mirai-based botnet variant. It leveraged multiple domains featuring Italian nomenclature to distribute and expand its network of infected devices.	Exploiting Vulnerability	CVE-2025-24016
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Device Hijacking, Network Overload	Wazuh Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/wazuh/wazuh/releases/tag/v4.9.1

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Fog ransomware	Fog ransomware, first identified in April 2024, is a double-extortion threat that infiltrates networks. It spreads laterally using legitimate tools like RDP and PowerShell, exfiltrates sensitive data, and encrypts files with AES and RSA algorithms, appending extensions such as .fog, .FLOCKED, or .ffog. The malware disables security tools, deletes backups, and targets both Windows and Linux systems.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Information Theft, Data encryption, Financial loss	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 CVEs
Anubis	Anubis is a destructive ransomware threat that emerged in December 2024, offering both file encryption and an optional wiper mode that renders data unrecoverable. Distributed via phishing, stolen credentials, and access brokers, it operates under a ransomware-as-a-service (RaaS) model.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data theft and Data exfiltration	Windows, Linux, NAS, and ESXi (VMware) environments
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sakura RAT	Sakura RAT is a lightweight remote access trojan used by the Water Curse group to maintain control over compromised systems. It supports basic functions like system reconnaissance, command execution, and credential theft. Often deployed in later stages, it acts as a modular payload for long-term access and data harvesting.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote control, Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Water Curse			-

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
DULLRAT	DULLRAT is a lightweight, JavaScript-based backdoor used in the Water Curse campaign, often embedded within malicious Electron applications. It enables remote access, command execution, and data theft, acting as part of a modular multi-stage infection chain.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System control, Data theft and Unauthorized access	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Water Curse			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HoldingHands RAT	HoldingHands RAT, also known as Gh0stBins, is a variant of the notorious Gh0st RAT, commonly used by Chinese state-sponsored threat actors. It's delivered via sophisticated phishing campaigns, often mimicking official communications like tax or invoice lures. Once active, it establishes command-and-control, allowing attackers to collect user data, manage files, and conduct remote desktop operations on compromised systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
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
Gunra Ransomware	Gunra ransomware, a malware strain written in C/C++, is quickly making headlines for its aggressive double-extortion tactics. Built on the leaked Conti ransomware source code, it has compromised approximately 13 high-profile organizations worldwide since its emergence in April 2025.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Flodrix	Flodrix is a botnet actively exploiting a critical vulnerability in Langflow, a framework for building AI applications. Once a system is compromised, Flodrix turns it into part of a botnet capable of launching high-volume Distributed Denial of Service (DDoS) attacks. It can also achieve full system compromise and potentially exfiltrate sensitive data, employing stealth techniques like self-deletion to evade detection.	Exploiting vulnerability	CVE-2025-3248
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Botnet		Network Overload, Compromise systems	Langflow
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/langflow-ai/langflow/releases/tag/1.3.0

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
RevengeRAT	RevengeRAT is a versatile Remote Access Trojan, often distributed via spear-phishing emails containing malicious attachments or links. It's known for its .NET origins and has been leveraged by various threat groups, including state-sponsored actors, in campaigns targeting diverse sectors.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Data theft, Full system control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Katz Stealer	Katz Stealer is a newly discovered, sophisticated information-stealing malware-as-a-service (MaaS) that emerged in 2025. It targets a vast array of sensitive data including browser credentials, crypto wallets, and system information, employing stealthy evasion techniques like UAC bypass and in-memory execution.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Stealer		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
PylangGhost	PylangGhost is a Python-based Remote Access Trojan (RAT) identified in May 2025, primarily targeting cryptocurrency and blockchain professionals in India. Linked to the North Korean threat group Famous Chollima, it's delivered via fake job offers on spoofed job sites, tricking victims into executing malicious commands to install fake video drivers.	Phishing through fake job offers	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote control, Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Famous Chollima			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Trinper	Trinper is a credential-stealing malware designed to extract sensitive information such as login credentials and system details from infected machines. It typically targets Windows systems and uses obfuscation techniques to evade detection.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		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 CVEs
BERT Ransomware	BERT ransomware, 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 CVEs
Prometei	By early 2023, the Prometei v3 botnet, an upgraded version of the Prometei botnet malware, had compromised over 10,000 systems mining the Monero cryptocurrency. In its latest iteration, identified in March 2025, Prometei stepped up with new Linux-specific variants.	Exploiting vulnerabilities	CVE-2021-27065 CVE-2021-26858 CVE-2017-0144 CVE-2019-0708
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Network compromise, Data mining	Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144

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
BeardShell	BEARDSHELL is a custom backdoor developed by APT28, written in C++, and designed for stealthy remote access. It executes decrypted PowerShell scripts directly in memory and communicates with command-and-control servers via the Icedrive cloud API. The malware uses ChaCha20-Poly1305 encryption and system-specific directories to evade detection and blend in with normal traffic.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System control, Data theft and Unauthorized access	Windows
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Covenant	Covenant is an open-source .NET-based command-and-control (C2) framework often used by both red teams and threat actors like APT28. In this campaign, it was loaded in memory to enable fileless execution and stealthy communication. It connected to attacker-controlled Koofr cloud storage for payload delivery and command execution.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Framework		Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SlimAgent	SLIMAGENT is a C++-based malicious tool used by APT28 to capture screenshots from infected systems. It leverages Windows GDI functions to take screenshots, encrypts them using AES and RSA, and stores them locally with timestamps.	Dropped via Covenant	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Tool		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-

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
PoshC2	PoshC2 is an open-source post-exploitation and command-and-control (C2) framework used by attackers to control compromised systems. Written in PowerShell and Python, it enables remote execution, credential harvesting, and lateral movement. Though originally developed for legitimate penetration testing, it is often abused by threat actors.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Tool		Remote control, data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Chisel	Chisel is a fast TCP/UDP tunnel, used to bypass firewalls and enable covert communication between systems. It acts as a reverse proxy, commonly used in red team operations and by threat actors. Though designed for legitimate network debugging, it's often misused for data exfiltration and C2 communication.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Tool		Firewall evasion, data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Classroom Spy	Classroom Spy is a remote monitoring software designed for educators to oversee student computer activity in classrooms. It allows viewing screens, controlling systems, and managing student behavior during lessons. However, it is misused as spyware by malicious actors for unauthorized surveillance.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Tool		Unauthorized monitoring, privacy invasion	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
sw1zzx	Russian-speaking	Gaming	Europe, Asia, North Africa and North America
	MOTIVE		
	Information Theft, Espionage, Financial Gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Blitz, XMRig	Windows
TTPs			
TA0003: Persistence; TA0040: Impact; TA0005: Defense Evasion; TA0002: Execution; TA0007: Discovery; TA0011: Command and Control; TA0009: Collection; T1496: Resource Hijacking; T1204: User Execution; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1497.001: System Checks; T1574.001: DLL; T1574: Hijack Execution Flow; T1036: Masquerading; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1082: System Information Discovery; T1056.001: Keylogging; T1056: Input Capture; T1113: Screen Capture; T1499: Endpoint Denial of Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Stealth Falcon (aka FruityArmor, Project Raven, G0038)	UAE	Defense and Government Organizations	Middle East, Africa
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2025-33053	Horus Agent, Horus Loader	Web Distributed Authoring and Versioning (WebDAV)
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1003: OS Credential Dumping; T1105: Ingress Tool Transfer; T1056: Input Capture; T1056.001: Keylogging; T1095: Non-Application Layer Protocol; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1016: System Network Configuration Discovery; T1106: Native API			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
APT37 (aka RICOCHET CHOLLIMA, Reaper, TEMP.Reaper, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt)	North Korea **MOTIVE** Information Theft and Espionage	Governments, Think Tanks, Activists (Civil Society)	South Korea
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2022-41128	RoKRAT	Microsoft Windows

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; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1082: System Information Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1113: Screen Capture; T1115: Clipboard Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1070.004: File Deletion; T1132: Data Encoding; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Water Curse	-	Cryptocurrency, Gaming, Information Technology	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	Sakura RAT, DULLRAT	Windows

TTPs
TA0006: Credential Access; TA0010: Exfiltration; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; T1053.005: Scheduled Task; T1119: Automated Collection; T1560: Archive Collected Data; T1102.002: Bidirectional Communication; T1102: Web Service; T1557: Adversary-in-the-Middle; T1497: Virtualization/Sandbox Evasion; T1113: Screen Capture; T1555: Credentials from Password Stores; T1082: System Information Discovery; T1497.001: System Checks; T1213: Data from Information Repositories; T1555.003 Credentials from Web Browsers; T1005: Data from Local System; T1543: Create or Modify System Process; T1036 Masquerading; T1218: System Binary Proxy Execution; T1048: Exfiltration Over Alternative Protocol; T1548 Abuse Elevation Control Mechanism; T1112: Modify Registry; T1027: Obfuscated Files or Information; T1057: Process Discovery:; T1548.002: Bypass User Account Control; T1562.001: Disable or Modify Tools; T1562.004 Disable or Modify System Firewall; T1562: Impair Defenses; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1129: Shared Modules; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Famous Chollima (aka Wagemole, Contagious Interview, Nickel Tapestry, Storm-1877, UNC5267, Void Dokkaebi, PurpleBravo, TenaciousPungsan, WaterPlum, BadClone)	North Korea	Cryptocurrency	India
	MOTIVE		
	Financial gain, Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PylangGhost	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.003: Spearphishing via Service; T1189: Drive-by Compromise; T1059: Command and Scripting Interpreter; T1059.006: Python; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1083: File and Directory Discovery; T1012: Query Registry; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027: Obfuscated Files or Information; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1560.001: Archive via Utility; T1560: Archive Collected Data; T1543: Create or Modify System Process; T1656: Impersonation; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)	Suspected UK and US	Commercial facilities, Telecommunications, Technology, Business-Process Outsourcing (BPO), Financial services, Hospitality, Media and entertainment, Healthcare, Retail, Insurance, Managed Service Providers (MSPs), Manufacturing, Cryptocurrency, and Food services	United States, Canada, United Kingdom, Singapore, India, France, Sweden, and Australia
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2015-2291 CVE-2021-35464 CVE-2024-37085	DragonForce Ransomware	-

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; T1585.001: Social Media Accounts; T1585: Establish Accounts; T1566: Phishing; T1660: Phishing; T1566.004: Spearphishing Voice; T1199: Trusted Relationship; T1078.002: Domain Accounts; T1078: Valid Accounts; T1648: Serverless Execution; T1204: User Execution; T1136: Create Account; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1484.002: Domain Trust Modification; T1484: Domain Policy Modification; T1578.002: Create Cloud Instance; T1578: Modify Cloud Compute Infrastructure; T1656: Impersonation; T1606: Forge Web Credentials; T1621: Multi-Factor Authentication Request Generation; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552: Unsecured Credentials; T1217: Browser Bookmark Discovery; T1538: Cloud Service Dashboard; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1539: Steal Web Session Cookie; T1021: Remote Services; T1021.007: Cloud Services; T1213.003: Code Repositories; T1213.002: Sharepoint; T1213: Data from Information Repositories; T1074: Data Staged; T1114:Email Collection; T1530: Data from Cloud Storage; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1567.002: Exfiltration to Cloud Storage; T1526: Cloud Service Discovery; T1218: System Binary Proxy Execution; T1562: Impair Defenses ; T1568: Dynamic Resolution; T1003: OS Credential Dumping; T1036: Masquerading; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
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)	Russia	Government	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	BeardShell, Covenant, and SlimAgent	Windows
TTPs			
TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; T1567.002; TA0001: Initial Access; TA0010: Exfiltration; T1546: Event Triggered Execution; TA0002: Execution; TA0011; TA0004: Privilege Escalation; TA0040: Command and Control; T1564: Hide Artifacts; T1567: Exfiltration to Cloud Storage: Exfiltration Over Web Service; T1041: Exfiltration Over C2 Channel: Impact; T1059.005: Visual Basic; T1546.015: Component Object Model HijackingT1566.003; T1566: Spearphishing via Service Phishing; T1059: Command and Scripting Interpreter; T1053.005: Scheduled Task; T1071.001: Web Protocols; T1021: Remote Services; T1082; T1574.001: DLL; T1218: System Binary Proxy Execution; T1071: Application Layer Protocol; T1204: User Execution; T1204.002: Malicious File; T1562; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1053: Impair Defenses; T1573: Encrypted Channel; T1003: OS Credential Dumping; T1113: System Information Discovery: Screen Capture; T1036: Masquerading: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1102: Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TaxOff	-	Media Outlets, Educational Institutions and Government Organizations	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Trinper	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1106: Native API; T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1041: Exfiltration Over C2 Channel; T1572: Protocol Tunneling: T1070: Indicator Removal; T1070.004: File Deletion; T1070.009: Clear Persistence; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1056: Input Capture; T1056.001: Keylogging; T1057: Process Discovery; T1083: File and Directory Discovery; T1115: Clipboard Data; T1071: Application Layer Protocol: T1090: Proxy; T1090.004: Domain Fronting; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	
	T1595: Active Scanning	
		T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	
		T1598.001: Spearphishing Service
		T1598.002: Spearphishing Attachment
TA0042: Resource Development	T1583: Acquire Infrastructure	
		T1583.001: Domains
		T1583.004: Server
	T1584: Compromise Infrastructure	
		T1584.005: Botnet
		T1584.006: Web Services
	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
		T1585.001: Social Media Accounts
		T1586.002: Email Accounts
		T1608.001: Upload Malware
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	
	T1195: Supply Chain Compromise	
		T1195.001: Compromise Software Dependencies and Development Tools
	T1199: Trusted Relationship	
	T1566: Phishing	
		T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	
		T1053.003: Cron
		T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
TA0002: Execution	T1059: Command and Scripting Interpreter	
		T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	
		T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	
		T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	
		T1037.001: Logon Script (Windows)
	T1053: Scheduled Task/Job	
		T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	
		T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1133: External Remote Services	
	T1136: Create Account	
	T1176: Browser Extensions	
	T1505: Server Software Component	
		T1505.003: Web Shell
	T1542: Pre-OS Boot	
		T1542.003: Bootkit
	T1543: Create or Modify System Process	
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
		T1546.015: Component Object Model Hijacking
		T1546.016: Installer Packages
	T1547: Boot or Logon Autostart Execution	
		T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification

Tactic	Technique	Sub-technique
TA0003: Persistence	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	
		T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	
		T1037.001: Logon Script (Windows)
	T1053: Scheduled Task/Job	
		T1053.003: Cron
		T1053.005: Scheduled Task
	T1055: Process Injection	
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
		T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1134: Access Token Manipulation	
		T1134.002: Create Process with Token
	T1484: Domain or Tenant Policy Modification	
		T1484.002: Domain Trust Modification
	T1543: Create or Modify System Process	
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
		T1546.015: Component Object Model Hijacking
		T1546.016: Installer Packages
	T1547: Boot or Logon Autostart Execution	
		T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	
		T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	
		T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	
		T1027.002: Software Packing
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.012: LNK Icon Smuggling
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	
		T1036.001: Invalid Code Signature
		T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	
		T1055.012: Process Hollowing
	T1070: Indicator Removal	
		T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.006: Timestomp
		T1070.009: Clear Persistence
	T1078: Valid Accounts	
		T1078.001: Default Accounts
		T1078.002: Domain Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	
		T1134.002: Create Process with Token
	T1140: Deobfuscate/Decode Files or Information	
	T1202: Indirect Command Execution	
	T1218: System Binary Proxy Execution	
		T1218.007: Msiexec
	T1222: File and Directory Permissions Modification	
	T1480: Execution Guardrails	
		T1480.001: Environmental Keying
	T1484: Domain or Tenant Policy Modification	
		T1484.002: Domain Trust Modification
	T1497: Virtualization/Sandbox Evasion	
		T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1542: Pre-OS Boot	
		T1542.003: Bootkit
	T1548: Abuse Elevation Control Mechanism	
		T1548.002: Bypass User Account Control
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	
		T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1564: Hide Artifacts	
		T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.006: Run Virtual Instance
	T1574: Hijack Execution Flow	
		T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1578: Modify Cloud Compute Infrastructure	
		T1578.002: Create Cloud Instance
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	
		T1003.001: LSASS Memory
		T1003.008: /etc/passwd and /etc/shadow
	T1056: Input Capture	
		T1056.001: Keylogging
		T1056.003: Web Portal Capture
		T1056.004: Credential API Hooking
	T1110: Brute Force	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	
		T1552.001: Credentials In Files
		T1552.004: Private Keys
	T1555: Credentials from Password Stores	
		T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.004: Windows Credential Manager
	T1556: Modify Authentication Process	
	T1557: Adversary-in-the-Middle	
	T1606: Forge Web Credentials	
	T1621: Multi-Factor Authentication Request Generation	
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
		T1087.001: Local Account
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
		T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1518: Software Discovery	
		T1518.001: Security Software Discovery
	T1526: Cloud Service Discovery	
	T1538: Cloud Service Dashboard	
	T1580: Cloud Infrastructure Discovery	
	T1614: System Location Discovery	
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	
		T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
		T1021.007: Cloud Services
	T1072: Software Deployment Tools	
	T1210: Exploitation of Remote Services	
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	
		T1056.001: Keylogging
		T1056.003: Web Portal Capture
		T1056.004: Credential API Hooking
	T1074: Data Staged	
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1213: Data from Information Repositories	
		T1213.002: Sharepoint
		T1213.003: Code Repositories
	T1530: Data from Cloud Storage Object	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	
		T1560.001: Archive via Utility

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1001: Data Obfuscation	
	T1071: Application Layer Protocol	
		T1071.001: Web Protocols
	T1090: Proxy	
		T1090.003: Multi-hop Proxy
		T1090.004: Domain Fronting
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	
		T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	
		T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	
		T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	
		T1567.002: Exfiltration to Cloud Storage
		T1567.004 : Exfiltration Over Webhook
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1529: System Shutdown/Reboot	
	T1531: Account Access Removal	
	T1657: Financial Theft	

Top 5 Takeaways

#1

In **June 2025, nine zero-day** vulnerabilities were discovered, with the '**Five Celebrity Vulnerabilities**' taking center stage. These included flaws such as **EchoLeak, ProxyLogon, EternalBlue, BlueKeep, CitrixBleed 2**.

#2

Several new malicious tools were detected in **June 2025,** including **Lyrix Ransomware, Gunra Ransomware, PylangGhost,** and **Bert Ransomware.** These fresh entries expand the ransomware and malware landscape, bringing diverse techniques and operational approaches that warrant close attention.

#3

Notably, **Atomic Stealer, Mirai botnet, Prometei botnet, DragonForce ransomware,** and **Fog Ransomware** staged significant rebounds this month, surfacing with upgraded variants. Enhanced capabilities in persistence, encryption, and evasion highlight the ongoing evolution of established threats in response to defensive improvements.

#4

In June 2025, cyber threat activity predominantly focused on the **United States, the United Kingdom, Canada, Turkey,** and **Saudi Arabia**. These nations experienced heightened malicious campaigns spanning ransomware, botnets, and custom malware deployments.

#5

Key sectors under fire included **Government, Financial Services, Technology, Cryptocurrency,** and **Healthcare**. Attackers concentrated their efforts on disrupting essential services, accessing sensitive financial and medical data, and targeting crypto-related assets.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **25 significant vulnerabilities** and block the indicators related to the **8 active threat actors, 37 active malware,** and **219 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 **25 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
DragonForce	SHA256	6782ad0c3efc0d0520dc2088e952c504f6a069c36a0308b88c7daadd600250a9, d626eb0565fac677fdc13fb0555967dc31e600c74fbbd110b744f8e3a59dd3f9, ba1be94550898eedb10eb73cb5383a2d1050e96ec4df8e0bf680d3e76a9e2429
Lyrix	SHA256	fcfa43ecb55ba6a46d8351257a491025022f85e9ae9d5e93d945073f612c877b, 77706303f801496d82f83189beff412d83a362f017cadecc7a3e349a699ce458
NetSupport RAT	SHA256	431b0b19239fc5e0eeaee70cd6e807868142e8cd0b2b6b1bd4a7a2cc8eb57d15, ab8fdde9fb9b88c400c737d460dcbf559648dc2768981bdd68f55e1f98292c2a, b2daa2b5afb389828e088ec8b27c0636bdad94b2ef71dcf8034ee601cb60d8d6, 58874c0dc26a78cdc058f84af9967f31b3c43173edc7515fa400e6ef8386205f, b258de3b7ef42b4f4bfb0fb5ffe7c55df6aef01cc591abe34a70d1ff82130cd5, e9fe19455642673b14c77d18a1e7ed925f23906bf11237dfafd7fb2cba1f666d, 1a128f6748d71d02c72ba51268be181143405830a4e48dfa53bf3d6ed3391211, 89043d2817d1bb4cb57ed939823dca0af9ae412655a6c75c694cb13d088efe5a, 8ffacc942d1c3f45e797369a1f4cbd5dcd84372abf979b06220236d5a5cea649, b3e879b5952988fb0c656240365db8f01198f9d83cd2a3ec0e2a8ee172e20a11, c6907acabf2edf0be959c64a434e101963f7c18dcf79f116e0ce6b5ced5dd08c, 07576e1db7e7bd0f7d2c54b6749fdd73c72dba8c2ba8ab110b305cfc10c93c80, 80b274871e5024dfa9e513219fe3df82cc8fe4255010bd5d04d23d5833962c10, d7fadf7ef45c475bd9a759a771d99ccf95edfa8a0c101ce2439a07b66c2e5c72, f9a241a768397efb4b43924fbd32186fcb1c88716fff3085d3ddcdd322d3404f

Attack Name	TYPE	VALUE
Chaos RAT	SHA256	1e074d9dca6ef0edd24afb2d13ca4429def5fc5486cd4170c989ef60efd0bbb0, d0a63e059ed2c921c37c83246cdf4de0c8bc462b7c1d4b4ecd23a24196be7dd7, 773c935a13ab49cc4613b30e8d2a75f1bde3b85b0bba6303eab756d70f459693, c8dc86afd1cd46534f4f9869efaa3b6b9b9a1efaf3c259bb87000702807f5844, 90c8b7f89c8a23b7a056df8fd190263ca91fe4e27bda174a9c268adbfc5c0f04, 8c0606db237cfa33fa3fb99a56072063177b61fa2c8873ed6af712bba2dc56d9, 2732fc2bb7b6413c899b6ac1608818e4ee9f0e5f1d14e32c9c29982eecd50f87, 839b3a46abee1b234c4f69acd554e494c861dcc533bb79bd0d15b9855ae1bed7, 77962a384d251f0aa8e3008a88f206d6cb1f7401c759c4614e3bfe865e3e985c, 57f825a556330e94d12475f21c2245fa1ee15aedd61bffb55587b54e970f1aad, 44c54d9d0b8d4862ad7424c677a6645edb711a6d0f36d6e87d7bae7a2cb14d68, c9694483c9fc15b2649359dfbd8322f0f6dd7a0a7da75499e03dbc4de2b23cad, 080f56cea7acfd9c20fc931e53ea1225eb6b00cf2f05a76943e6cf0770504c64, a583bdf46f901364ed8e60f6aadd2b31be12a27ffcccecc962872bc73a9ffd46c, a364ec51aa9314f831bc498ddaf82738766ca83b51401f77dbd857ba4e32a53b, a6307aad70195369e7ca5575f1ab81c2fd82de2fe561179e38933f9da28c4850, c39184aeb42616d7bf6daaddb9792549eb354076b4559e5d85392ade2e41763e, 67534c144a7373cacbd8f9bd9585a2b74ddbb03c2c0721241d65c62726984a0a, 719082b1e5c0d18cc0283e537215b53a864857ac936a0c7d3ddbaf7c7944cf79
Mesh Agent	SHA256	07f7ce55e75afda05241c70710d5c6769909d94193e41b370a29b5dca3ef1f3d, 12155ad4d117ea2b13131df52de4045e635e100d45bac057d6f5674e894dec99
Blitz	SHA256	0e80fe5636336b70b1775e94aaa219e6aa27fcf700f90f8a5dd73a22c898d646,

Attack Name	TYPE	VALUE
Blitz	SHA256	cacc1f36b3817e8b48fabbb4b4bd9d2f1949585c2f5170e3d2d04211861ef2ac, aa5cd0219e8a0bd2e7d6c073f611102d718387750198bff564c20ca7ebada309, f3b7bbe1079974fd505abaadbcf4dc0517620592eacbbe5f314a76775dd760c2, cdf192e92d14b9d7e1201c23621c4e0b8ee0673c192bdd734afd97519afef271, 6441e7000713f96c7ae114ce62378556d01fa29d435a5be0f11a5e80be9a26ed, b1b1ce259fcf5127c3477e278c3696dc7d15db63b673fdcf75e1deb89a0f6fd1, 5ef29d6d4f72e62e0d5a1d0b85eed70b729cd530c8cb2745c66a25f5b5c7299e, 5fc132b054099a1a65f377a3a22b003a6507107f3095371b44dbf5e098b02295, b18e21e50f1c346c83c4cba933b6466ada22febaafa25c03ac01122a12164375, a34a4a7c71de2d4ec4baf56fd143d27eeedebb785a2ba3e0740b92e62efd81ea, bedeafd3680cad581a619fb58aa4f57ed991c4a8dd94df46ef9cbd08a8dd6052, ae2f4c49f73f6d88b193a46cd22551bb31183ae6ee79d84be010d6acf9f2ee57, 88e2d0d59a9751e4ce5223951f5a75b1731b1ee82d18705aba83ba4bd7e8e5c1
XMRig	SHA256	47ce55095e1f1f97307782dc4903934f66beec3476a45d85e33e48d63e1f2e15
Atomic Stealer	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 3fb1bafe9e659a68b9177ef7b5d2e5240e6be86fb82f33f89c281bb058857c7a, a6a2ffe881e4e771f9c09283c483bcb41b5b84448b2df64afb84709d3fa09a9e
	MD5	eaedee8fc9fe336bcde021bf243e332a, 6fd092d86235d7ae35c557523f493674
Vshell	SHA256	ba4f9b324809876f906f3cb9b90f8af2f97487167beead549a8cddfd9a7c2fdc, bb6ab67ddbb74e7afb82bb063744a91f3fecf5fd0f453a179c0776727f6870c7, 2206cc6bd9d15cf898f175ab845b3deb4b8627102b74e1accefe7a3ff0017112, a0f4ee6ea58a8896d2914176d2bfbdb9e16b700f52d2df1f77fe6ce663c1426a
Myth Stealer	SHA256	65a84024daf30c12fd2e76db661bf6e85f3da30bb3aaa7e774152855d718b0c4,

Attack Name	TYPE	VALUE
Myth Stealer	SHA256	e5d09da6648add4776de8091b0182b935405791bf41476465b0e7dcb066fc0dc, acd66cb5f1447b803245c495400ad0886352920e35defcca6c45519fb7d33693, 6c54e6648a6a33583d7707a9f7c5e83dd08ed481df6354c52e8f81e729d74a82
Horus Agent	SHA256	ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b
RoKRAT	SHA256	92ab3a9040f5e620bc4b76295239c5240130d968c6cbeaa7dc555d2cf19bfae1, d182834a984c9f5b44ea0aca5786223a78138ff23d33362ab699c76bf6987261, 9b8218774c3abc0a449cfc490f12e81155af00ec90c2e1d630a61c29f70a98cb
AsyncRAT	SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a
	Domain	microads[.]top
	URLs	hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/AClient[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/AClient[.]exe, hxxps[:]//pastebin[.]com/raw/ftknPNF7, hxxps[:]//pastebin[.]com/raw/NYpQCL7y, hxxps[:]//pastebin[.]com/raw/QdseGsQL
	IPv4	101[.]99[.]76[.]120, 87[.]120[.]127[.]37, 185[.]234[.]247[.]8
Skuld Stealer	SHA256	8135f126764592be3df17200f49140bfb546ec1b2c34a153aa509465406cb46c
	URLs	hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/skul[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/skul[.]exe

Attack Name	TYPE	VALUE
Mirai	SHA256	dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9, 7b659210c509058bd5649881f18b21b645acb42f56384cbd6dcb8d16e5aa0549, 64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4eb692b08f52b0f, 4c1e54067911aeb5aa8d1b747f35fdcdfdf4837cad60331e58a7bbb849ca9eed, 811cd6ebeb9e2b7438ad9d7c382db13c1c04b7d520495261093af51797f5d4cc, 90df78db1fb5aea6e21c3daca79cc690900ef8a779de61d5b3c0db030f4b4353, 8a58fa790fc3054c5a13f1e4e1fcb0e1167dbfb5e889b7c543d3cdd9495e9ad6, c9df0a2f377ffab37ede8f2b12a776a7ae40fa8a6b4724d5c1898e8e865cfea1, 6614545eec64c207a6cc981fccae8077eac33a79f286fc9a92582f78e2ae243a
Resbot	SHA256	9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b
Fog ransomware	SHA256	181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa
Anubis	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
Sakura RAT	SHA1	5cd53d94caf0e811b82bad958b34322eb082567f
DULLRAT	SHA1	60bdf425bd22c34bad7d5663db31d2107153f729, 68911ad6696cfdb15c967a82c2d8aab1be634659, d94f476b2aceaf4e83197475280f89ecbe3b8d35
	SHA256	af6e99f86899fe12907850ba365d75b57238300869795d5f998b7b2f57f11837
HoldingHands RAT	SHA256	50fbd7e4cfa193f009d80913efd1cd2b04a9007db2fb97d5b26c9786216db124, a19fdfc131e8fbe063289c83a3cdefb9fb9fb6f1f92c83b892d3519a381623db
Flodrix	SHA256	EC0F2960164CDCF265ED78E66476459337C03ACB469B6B302E1E8AE01C35D7EC, 52A034E732BCE0CB10FBFAE6F3C208FFB885D490FBCD70BAD62FB2E32A7C33F8, E4AEA6EE7005EE4B500E0B8673B69EA91D1A7532FACAD653E575BA29824845D9, 7BDBF2766AD55F9A67BFBB97A32D308530E4B5959BB68A9ACB22326DFEE8F282,

Attack Name	TYPE	VALUE
Flodrix	SHA256	E08E03091DEFB5006792934389AA350E8C48C37E59E282EF8FE3C3F126212E20, 57CEDC81378F98E568539CC653349FF70EF851A6D51886FD2560F30DF5E31BBD, C97128A452FF24D9BA70A3A7674C1D7AD21BABC9C75E7C34330BADDAEEA3D4BD, 80C956C5F279A436E7CF81B3E47333144DA5EF39BD76BD8C4A65E4571125EA7A, DC9A484F4910EE08EB22AFAB8D328EEF5328C9A5A8ABC6A50062E2065262A81F, 4AA59DDE4C8DA2CFF1A3AFE02DB3AE6C00D99E698DB11838B791E1D6C582FFB6, 912573354E6ED5D744F490847B66CB63654D037EF595C147FC5A4369FEF3BFEE, 09EFD15FF0317424B9B964626DA5E42D68B3CE91F509B16DAD9892D156D3EABE, 1E5E9723C6B492C477471CCCB4D7B26AAE653B0C5491C29739F784C664699D36, AB0F9774CA88994091DB0AE328D98F45034F653BD34E4F5E85679A972D3A039C, C2BCDD6E3CC82C4C4DB6AAF8018B8484407A3E3FCE8F60828D2087B2568ECCA4, A6CF8124E9B4558AACC7DDFA24B440454B904B937929BE203ED088B1040D1B36, EC52F75268B2F04B84A85E08D56581316BD5CCFEB977E002EB43270FE713F307, CCB02DCE1BCA9C3869E1E1D1774764E82206026378D1250AED324F1B7F9B1F11, 9991C664C052EC407E53439AC6BB4DF3CBBE3E54AF243D007A39D8A3DAB935B9, F73B554E6AA7095CFC79CDB687204D99533AEDA73309106BA6CC9428FF57BD1E, EE84591092A971C965B4E88CC5D6E8C2F07773B3BEE1486F3A52483EE72A2B3B, 002F3B2C632E0BE6CBC3FDF8AFCD0432FFE36604BA1BA84923CADAA147418187, 99B59E53010D58F47D332B683EB8A40DF0E0EACEF86390BCA249A708E47D9BAD, 78B430BFF7D797B020D06702659E26D8CA01C8FC968239390697AEFF472623A7, D8D5A32BBD747C92FA1BB55DCE4ABB20E8D09711AEBCBFE8E7EEC83173F9E627, 08CF20E54C634F21D8708573EEF7FDE4DBD5D3CD270D2CB8790E3FE1F42ECCEC, 6DD0464DD0ECDE4BB5A769C802D11AB4B36BBE0DD4F0F44144121762737A6BE0,

Attack Name	TYPE	VALUE
Flodrix	SHA256	C462A09DB1A74DC3D8ED199EDCA97DE87B6ED25C2273C4A3AFE811ED0C1C8B1D, C2DCEB14EB91802CD4F78E78634E7837F4B2F4D1329D3F5293C53798B4D0C30E, 9850EB26D8CBEF3358DA4DF154E054759A062116C2AA82DE9A69A8589F0DCE49, A42F8428AA75C180C2F89FBB8B1E44307C2390ED0EBF5AF10015131B5494F9E1, E1C830643DE2EC7BC7C032F7EC96C302CE54E703EAF576D3796D1BBD05D8A63F, 51085CD2DE0ED6A9A6738AC85A8CAF297FBD22DB4B049822A9802BB8140DCD3D, 64927195D388BF6A1042C4D689BCB2C218320E2FA93A2DCC065571ADE3BB3BD3, ABB0C4AD31F013DF5037593574BE3207A4C1E066A96E58CE243AAF2EF0FC0E4D, 47497B24AF6FF42DAE582998AEEEDBC7B9CA6B3E0D82E8E49E8AC4A0F453A659, DF9E9006A566A4FE30EAA48459EC236D90FD628F7587DA9E4A6A76D14F0E9C98 99B59E53010D58F47D332B683EB8A40DF0E0EACEF86390BCA249A708E47D9BAD, 78B430BFF7D797B020D06702659E26D8CA01C8FC968239390697AEFF472623A7, D8D5A32BBD747C92FA1BB55DCE4ABB20E8D09711AEBCBFE8E7EEC83173F9E627, 08CF20E54C634F21D8708573EEF7FDE4DBD5D3CD270D2CB8790E3FE1F42ECCEC, 6DD0464DD0ECDE4BB5A769C802D11AB4B36BBE0DD4F0F44144121762737A6BE0, C462A09DB1A74DC3D8ED199EDCA97DE87B6ED25C2273C4A3AFE811ED0C1C8B1D, C2DCEB14EB91802CD4F78E78634E7837F4B2F4D1329D3F5293C53798B4D0C30E, 9850EB26D8CBEF3358DA4DF154E054759A062116C2AA82DE9A69A8589F0DCE49, A42F8428AA75C180C2F89FBB8B1E44307C2390ED0EBF5AF10015131B5494F9E1, E1C830643DE2EC7BC7C032F7EC96C302CE54E703EAF576D3796D1BBD05D8A63F, 51085CD2DE0ED6A9A6738AC85A8CAF297FBD22DB4B049822A9802BB8140DCD3D, 64927195D388BF6A1042C4D689BCB2C218320E2FA93A2DCC065571ADE3BB3BD3, ABB0C4AD31F013DF5037593574BE3207A4C1E066A96E58CE243AAF2EF0FC0E4D,

Attack Name	TYPE	VALUE
Flodrix	SHA256	47497B24AF6FF42DAE582998AEEEDBC7B9CA6B3E0D82E8E49E8AC4A0F453A659, DF9E9006A566A4FE30EAA48459EC236D90FD628F7587DA9E4A6A76D14F0E9C98
	MD5	Eaf854b9d232566e82a805e9be8b2bf2, 176f293dd15b9cf87ff1b8ba70d98bcf, 82d8bc51a89118e599189b759572459f
	SHA1	E367cee9e02690509b4acdf7060f1a4387d85ec7, 7823b91efceedaf0e81856c735f13ae45b494909, d703ec4c4d11c7a7fc2fcf4a4b8776862a3000b5
Katz Stealer	Domain	katz-stealer[.]com, katzstealer[.]com
	SHA256	6dc8e99da68b703e86fa90a8794add87614f254f804a8d5d65927e0676107a9d, e73f6e1f6c28469e14a88a633aef1bc502d2dbb1d4d2dfcaaef7409b8ce6dc99, 2798bf4fd8e2bc591f656fa107bd871451574d543882ddec3020417964d2faa9, e345d793477abbecc2c455c8c76a925c0dfe99ec4c65b7c353e8a8c8b14da2b6, c601721933d11254ae329b05882337db1069f81e4d04cd4550c4b4b4fe35f9cd, fdc86a5b3d7df37a72c3272836f743747c47bfbc538f05af9ecf78547fa2e789, 25b1ec4d62c67bd51b43de181e0f7d1bda389345b8c290e35f93ccb444a2cf7a, 964ec70fc2fdf23f928f78c8af63ce50aff058b05787e43c034e04ea6cbe30ef, d92bb6e47cb0a0bdbb51403528ccfe643a9329476af53b5a729f04a4d2139647, b249814a74dff9316dc29b670e1d8ed80eb941b507e206ca0dfdc4ff033b1c1f, 925e6375deaa38d978e00a73f9353a9d0df81f023ab85cf9a1dc046e403830a8, 96ada593d54949707437fa39628960b1c5d142a5b1cb371339acc8f86dbc7678, b912f06cf65233b9767953ccf4e60a1a7c262ae54506b311c65f411db6f70128, 2852770f459c0c6a0ecfc450b29201bd348a55fb3a7a5ecdcc9986127fdb786b, 5dd629b610aee4ed7777e81fc5135d20f59e43b5d9cc55cdad291fcf4b9d20eb
RevengeRAT	IPv4	104[.]26[.]3[.]158

Attack Name	TYPE	VALUE
RevengeRAT	SHA256	7a8c864ed8b7ca908d3f317d7e63a30a85fb3e8c94070f23f2cf0bfa01c5e0b5, 837f60772b83b9aed7304d8e56f4aa8a49f7b79122e6d394447e9225105d6b6d, a30fa780cca1e7ab27f5802c749737ead187b8139e39cb736237087da1660024, 382593c547f7b0f4f9bebe0039ff7194ad8bf5969aae5f7d8267d48ece91bc96
Gunra Ransomware	Filename	gunraransome.exe R3ADM3.txt
	MD5	9a7c0adedc4c68760e49274700218507
	SHA1	77b294117cb818df701f03dc8be39ed9a361a038
	SHA256	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
	Tox ID	2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22
	TOR Address	gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd[.]onion
Horus Loader	SHA256	da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa
PylangGhost	SHA256	267009d555f59e9bf5d82be8a046427f04a16d15c63d9c7ecca749b11d8c8fc3
BERT Ransomware	SHA256	6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02, ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be, f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799, 78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c, 8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311
Prometei	SHA256	46cf75d7440c30cbfd101dd396bb18dc3ea0b9fe475eb80c4545868aab5c578c, cc7ab872ed9c25d4346b4c58c5ef8ea48c2d7b256f20fe2f0912572208df5c1a, 205c2a562bb393a13265c8300f5f7e46d3a1aabe057cb0b53d8df92958500867, 656fa59c4acf841dcc3db2e91c1088daa72f99b468d035ff79d31a8f47d320ef,

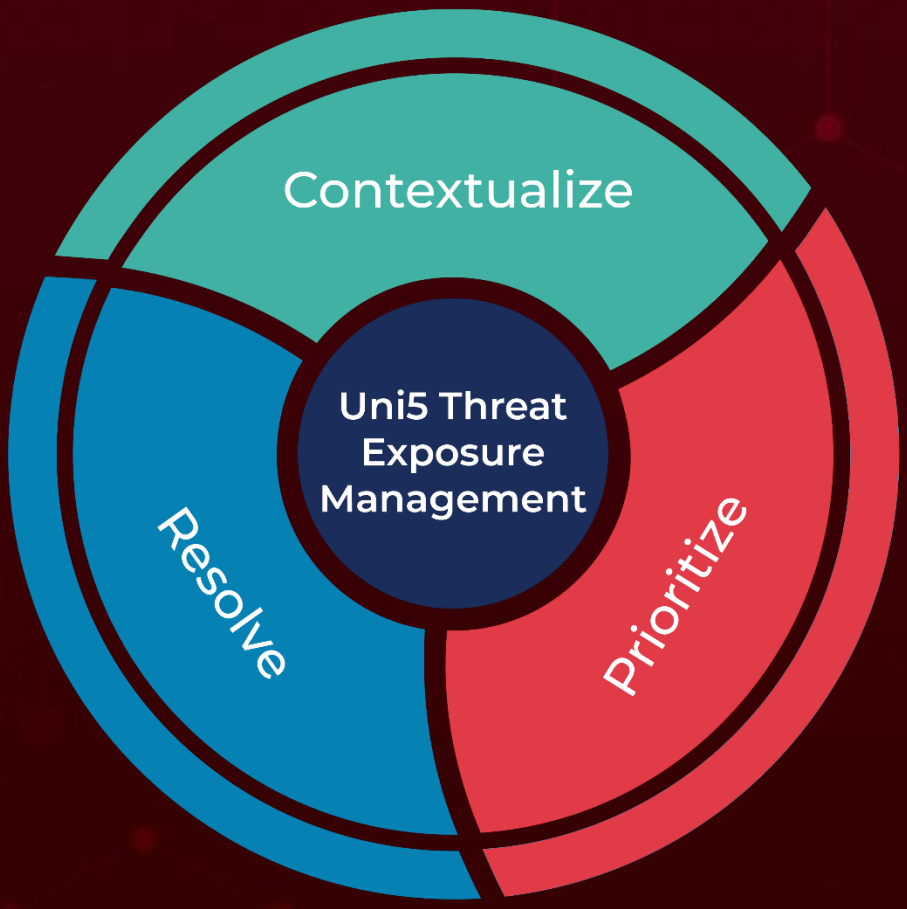
Attack Name	TYPE	VALUE
Prometei	SHA256	67279be56080b958b04a0f220c6244ea4725f34aa58cf46e5161cfa0af0a3fb0, 7a027fae1d7460fc5fccaf8bed95e9b28167023efcbb410f638c5416c6af53ff, 87f5e41cbc5a7b3f2862fed3f9458cd083979dfce45877643ef68f4c2c48777e, b1d893c8a65094349f9033773a845137e9a1b4fa9b1f57bdb57755a2a2dcb708, d21c878dcc169961bebda6e7712b46adf5ec3818cc9469debf1534ffa8d74fb7, d4566c778c2c35e6162a8e65bb297c3522dd481946b81baffc15bb7d7a4fe531, 00ad8a3aba502de1235773e96d3674e15b6f72187545c09ccfd8e6b3c91300bc
BeardShell	SHA256	d1deeaf0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a, 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1
Covenant	SHA256	84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460
SlimAgent	SHA256	9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c
	MD5	889b83d375a0fb00670af5276816080e
PoshC2	SHA256	e14b07b67f1a54b02fc6b65fdba3c9e41130f283bfea459afa6bee763d3756f8
Chisel	SHA256	e788f829b1a0141a488afb5f82b94f13035623609ca3b83f0c6985919cd9e83b
Classroom Spy	SHA256	831d98404ce5e3e5499b558bb653510c0e9407e4cb2f54157503a0842317a363
Trinper	SHA256	f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666, d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2, 99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96
	SHA1	20943541522cd3937b275c42016ad3e1e64e3f38, d9fa06025ecd08fc417c9948148e7827280365f2, 39ecc624bd2d52db083424fbb3a47b0c60f5ae4e
	MD5	16f6227f760487a70a3168cf9a497ac3, dba17d2faa311f28e68477ea5cc1a300, 1b7b4608f2c9e0a4863a00edd60c3b78

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

July 1, 2025 • 10:00 PM

More at www.hivepro.com