Date of Publication
April 2, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

MARCH 2025

Table Of Contents

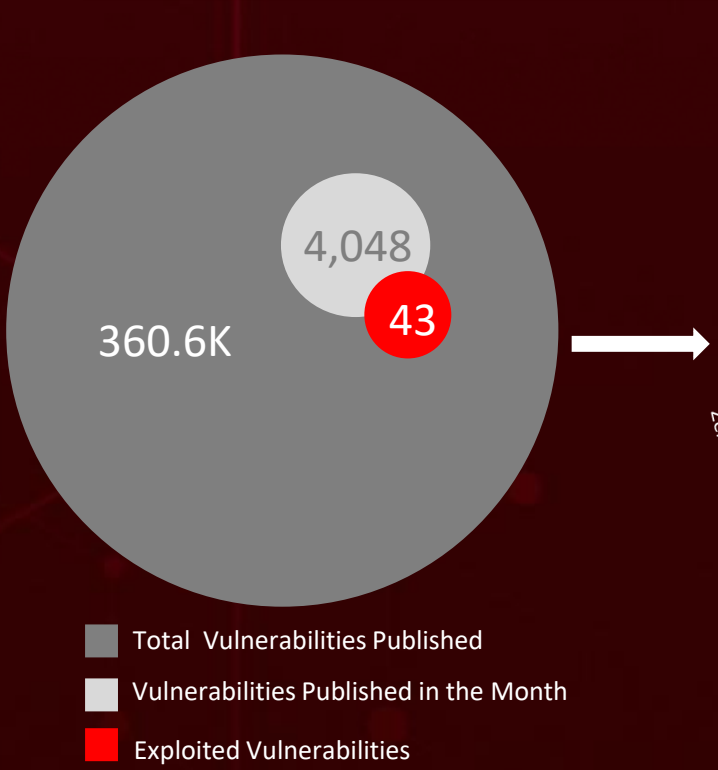
Summary

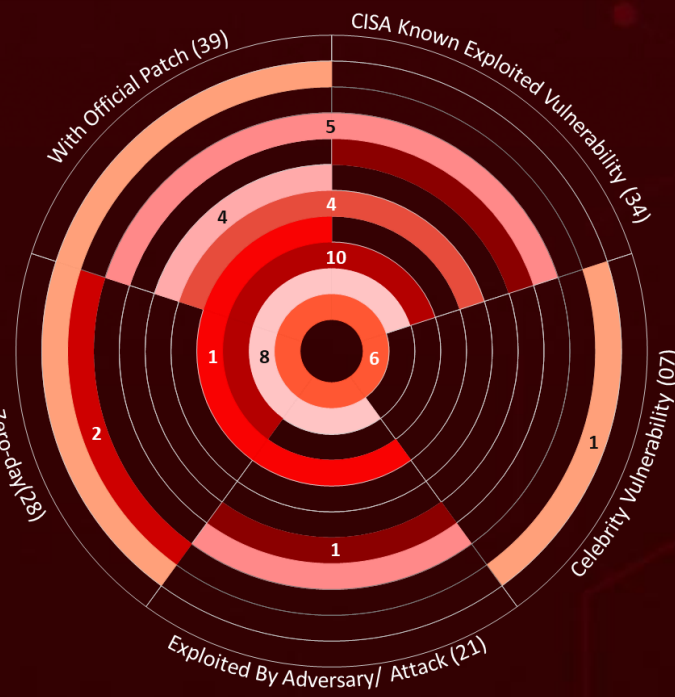
March sent shockwaves through the cybersecurity landscape by actively exploiting **four** celebrity vulnerabilities and **28** zero-days. Among the most alarming was a sophisticated **supply chain attack** that compromised the GitHub Action, exposing secrets in CI/CD workflows. This breach, cataloged as **CVE-2025-30154**, triggered a secondary attack on **CVE-2025-30066**, endangering over **23,000 repositories**.

Meanwhile, two critical flaws **CVE-2025-0364 and CVE-2024-54761** were discovered in the **BigAnt Server**, with **no official patch available**. The existence of **public exploits** makes immediate defensive measures, such as disabling SaaS registration and restricting access is crucial. Google also rushed to patch **CVE-2025-2783**, a zero-day Chrome vulnerability actively exploited in the wild. This flaw has been weaponized in phishing campaigns, redirecting unsuspecting victims to malicious domains under the **cyber-espionage operation ForumTroll**.

Adding to the chaos, **OBSCURE#BAT** a stealthy malware campaign, leveraged social engineering and deceptive downloads to infiltrate systems, mainly preying on English-speaking users. Meanwhile, China's **MirrorFace APT** group, traditionally focused on Japan-linked targets, launched its first known attack against a European entity. Dubbed **Operation AkaiRyū** (Red Dragon), the campaign unveiled an upgraded arsenal of espionage tactics. Elsewhere, the elusive **FishMonger** group (aka Earth Lusca) executed **Operation FishMedley**, targeting governments, NGOs, and think tanks across Asia, Europe, and the United States.

State-sponsored cyber espionage also took a new turn with **Silk Typhoon** an advanced threat actor now exploiting mainstream IT solutions, remote management tools, cloud apps, and unpatched vulnerabilities to breach networks. As cyber threats intensify, vigilance and adaptability are no longer optional they are essential. Organizations must stay ahead of adversaries, fortifying their defenses against an ever-evolving digital battleground.





Insights

In March 2025, a geopolitical cybersecurity landscape unfolds, revealing **Turkey, Japan, Russia, the United Arab Emirates,** and the **United States** as the top-targeted countries

Highlighted in **March 2025** is a cyber battleground encompassing the **Government, Technology, Healthcare, Education,** and **Telecommunication** sectors, designating them as the top industries

Breaking the Virtual Barrier: VMware Patches **Three** Critical Zero-Days

AI Under Attack: ChatGPT Exploit Fuels Over **10,000** Cyber Strikes in a Week

Hackers Hijack Chrome in Operation ForumTroll: Are You at Risk?

Invisible Invasion: PolarEdge Turns Cisco, ASUS & QNAP Devices Into Cyber Weapons

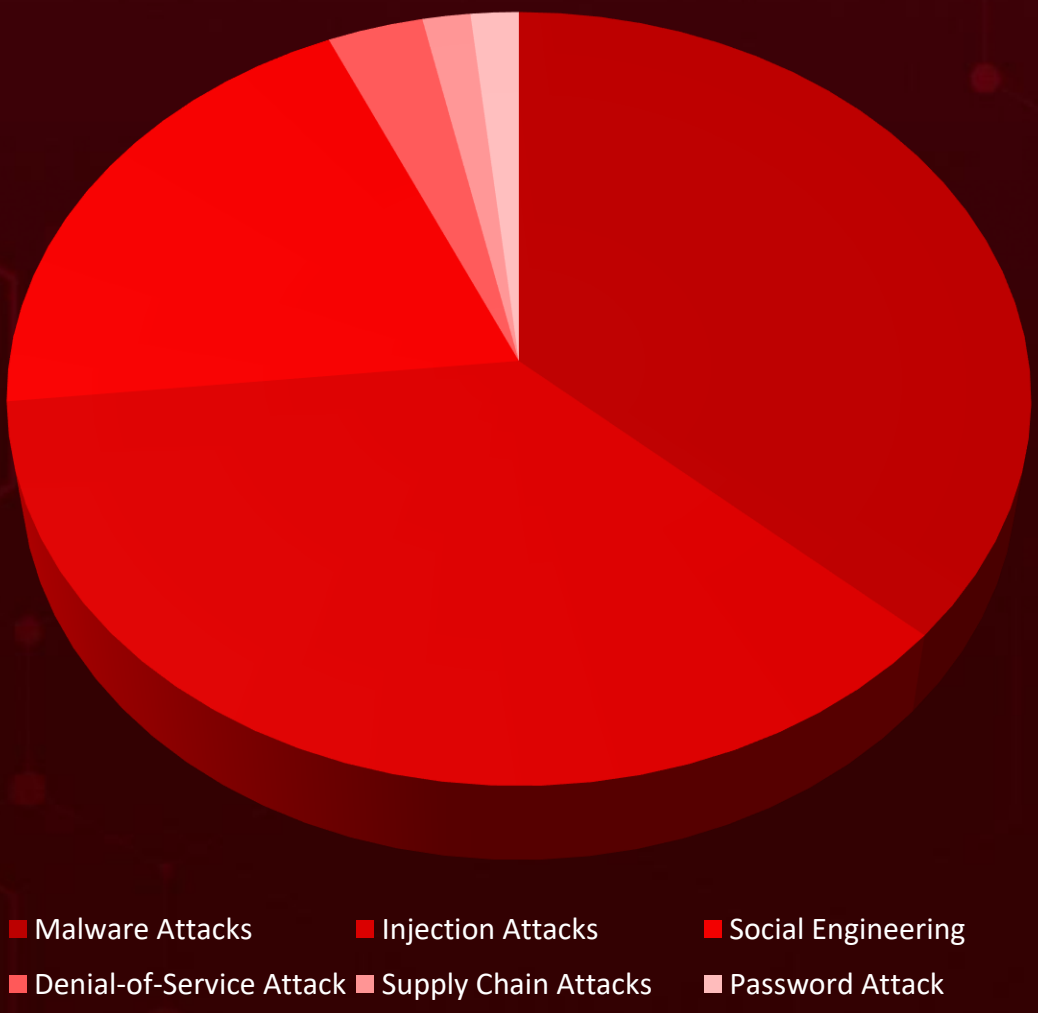
SuperBlack Ransomware: The LockBit 3.0 Offshoot Exploiting Fortinet Flaws

Water Gamayun Strikes! **MSC** EvilTwin Vulnerability Allows Silent Code Execution

Medusa Ransomware: The Relentless Cyber Predator Terrorizing Organizations

CVE-2025-24201: Apple Scrambles to Patch WebKit Zero-Day Actively Used in Cyber Attacks

Threat Landscape



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	✓	Microsoft Exchange Server	Silk Typhoon
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*	-
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1190: Exploit Public-Facing Application; T1078: Valid Accounts	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26857	✓	Microsoft Exchange Server	Silk Typhoon
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	-
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-502	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26858	✓	Microsoft Exchange Server	Silk Typhoon
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	-
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1505.003: Web Shell	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27065	✓	Microsoft Exchange Server	Silk Typhoon
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	-
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1505.003: Web Shell	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	✓	Apache Log4j2	Silk Typhoon
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	-
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7014	✓	Telegram Android versions 10.14.4 and older	-
	CISA KEV		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:telegram:telegram:*:*:*:*:*:android:*:*	-
EvilVideo Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1664: Exploitation for Initial Access; T1658: Exploitation for Client Execution	https://telegram.org/android

<table>
<tr><th>CVE ID</th><th>ZERO-DAY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-26633</td><td>✓</td><td rowspan="2">Windows: 10 - 11 24H2
Windows Server: 2008 - 2025</td><td rowspan="2">Water Gamayun</td></tr>
<tr><td>CISA KEV</td></tr>
<tr><td rowspan="3">✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*</td><td>EncryptHub, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader</td></tr>
<tr><td rowspan="2">MSC EvilTwin (Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability)</td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-707</td><td>T1553: Subvert Trust Controls;
T1204:User Execution;
T1566: Phishing</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633</td></tr>
</table>

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-22224	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability	VMware ESXi, Cloud Foundation, Telco Cloud Infrastructure, Workstation	✓	✓	✓
CVE-2025-22225	VMware ESXi Arbitrary Write Vulnerability	VMware ESXi, Cloud Foundation, Telco Cloud Infrastructure, Workstation	✓	✓	✓
CVE-2025-22226	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability	VMware ESXi, Cloud Foundation, Telco Cloud Infrastructure, Workstation, Fusion	✓	✓	✓
CVE-2025-0364	BigAntSoft BigAnt Server Authentication Bypass Vulnerability	BigAnt Server	✓	✗	✗
CVE-2024-54761	BigAntSoft BigAnt Office Messenger SQL Injection Vulnerability	BigAnt Server	✓	✗	✗
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS)	✓	✓	✓
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS)	✓	✓	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto PAN-OS	✓	✓	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	NetScaler ADC and NetScaler Gateway	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26857	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-2021-27065	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-44228	Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2	✓	✓	✓
CVE-2025-27218	Sitecore XM and XP Deserialization Vulnerability	Sitecore Experience Manager (XM) and Experience Platform	✗	✗	✓
CVE-2024-4577	PHP-CGI OS Command Injection Vulnerability	PHP version: 5 -8.3.7	✗	✓	✓
CVE-2023-20118	Cisco Small Business RV Series Routers Command Injection Vulnerability	Cisco Small Business RV Series Routers	✗	✓	EOL
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓
CVE-2025-24201	Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability	Apple iOS and iPadOS	✓	✓	✓
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	Windows	✓	✓	✓
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Windows	✓	✓	✓
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability	Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-24985	Windows Fast FAT File System Driver Remote Code Execution Vulnerability	Windows	✓	✓	✓
CVE-2025-24991	Windows NTFS Information Disclosure Vulnerability	Windows	✓	✓	✓
CVE-2025-24993	Windows NTFS Remote Code Execution Vulnerability	Windows	✓	✓	✓
CVE-2025-26633	MSC EvilTwin (Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability)	Microsoft Management Console	✓	✓	✓
CVE-2025-26630	Microsoft Access Remote Code Execution Vulnerability	Microsoft Office, Microsoft 365 Apps for Enterprise	✗	✗	✓
CVE-2025-27363	FreeType Out of Bounds Write Vulnerability	FreeType	✗	✗	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClientEMS	✗	✓	✓
CVE-2025-24472	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS and FortiProxy Office	✗	✓	✓
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓
CVE-2025-24813	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat	✗	✓	✓
CVE-2025-30066	tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability	GitHub Action	✗	✓	✓
CVE-2025-30154	reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability	reviewdog/action-setup	✗	✓	✓
CVE-2022-24521	Microsoft Windows CLFS Driver Privilege Escalation Vulnerability	Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication	✗	✓	✓
CVE-2024-50570	Fortinet Cleartext Storage of Sensitive Information Vulnerability	FortiClientWindows, FortiClientLinux	✓	✗	✓
CVE-2024-7014	EvilVideo Vulnerability	Telegram Android	✓	✗	✓
CVE-2024-27564	ChatGPT Pictureproxy.php Server-Side Request Forgery Vulnerability	pictureproxy.php component	✗	✗	✗
CVE-2025-2783	Google Chromium Mojo Sandbox Escape Vulnerability	Google Chrome (Windows)	✓	✓	✓
CVE-2025-29927	Next.js Middleware Bypass Vulnerability	Next.js React framework	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Havoc Demon	Hack tool	-	Windows	-	Phishing
KaynLdr	Loader	-	Windows	-	Phishing
Sosano	Backdoor	-	-	-	Phishing
Poco RAT	RAT	-	-	-	Phishing
PolarEdge Botnet	Botnet	CVE-2023-20118	Cisco Small Business RV Series Routers	EOL	Exploiting Vulnerability
SilentCryptoMiner	CryptoMiner	-	-	-	Social Engineering
StealerBot	Toolkit	CVE-2017-11882	Microsoft Office	✓	Exploiting Vulnerability
PureCrypter RAT	RAT	CVE-2024-43451	Microsoft Windows	✓	Exploiting Vulnerability
Remcos RAT	RAT	CVE-2024-43451	Microsoft Windows	✓	Exploiting Vulnerability
Medusa	Ransomware	CVE-2024-1709 CVE-2023-48788	ConnectWise ScreenConnect, Fortinet FortiClientEMS	✓	Exploiting Vulnerabilities
SuperBlack	Ransomware	CVE-2025-24472 CVE-2024-55591	FortiOS, FortiProxy	✓	Exploiting Vulnerabilities
SocGholish	Loader	-	Windows	-	Exploits compromised websites, Keitaro Traffic Distribution System (TDS) instances

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
RansomHub	Ransomware	CVE-2022-24521 CVE-2023-27532	Microsoft Windows, Veeam Backup & Replication	✓	Exploits compromised websites, Keitaro Traffic Distribution System (TDS) instances
r77	Rootkit	-	-	-	Social Engineering
StilachiRAT	RAT	-	Windows	-	-
ANEL	Backdoor	-	Windows	-	Spear-phishing
AsyncRAT	RAT	-	Windows	-	Spear-phishing, exploiting social media
ClearFake	Framework	-	Windows and Mac	-	Social Engineering
Emmenhtal	Loader	-	Windows and Mac	-	Social Engineering, Deployed by ClearFake
Lumma	Stealer	-	Windows and Mac	-	Social Engineering, Deployed by ClearFake
Vidar	Stealer	-	Windows and Mac	-	Social Engineering, Deployed by ClearFake
ShadowPad	Backdoor	-	-	-	-
SodaMaster	Backdoor	-	-	-	-
Spyder	Loader	-	-	-	-
VenomRAT	RAT	-	-	-	Phishing emails

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Betruger	Backdoor	CVE-2022-24521 CVE-2023-27532	Microsoft Windows, Veeam Backup & Replication	✓	Deployed by RansomHub
China Chopper	Web Shell	-	Windows	-	Compromised Zyxel CPE routers
INMemory	Web Shell	-	Windows	-	Compromised Zyxel CPE routers
VanHelsing	Ransomware	-	Windows, Linux, BSD, ARM, and VMware ESXi	-	-
EncryptHub	MaaS	CVE-2025-26633	Microsoft Management Console	✓	Phishing
DarkWisp	Backdoor	CVE-2025-26633	Microsoft Management Console	✓	Phishing
SilentPrism	Backdoor	CVE-2025-26633	Microsoft Management Console	✓	Phishing
Rhadamanthys	Information stealer	CVE-2025-26633	Microsoft Management Console	✓	Phishing
Stealc	Information stealer	CVE-2025-26633	Microsoft Management Console	✓	Phishing
MSC EvilTwin	Loader	CVE-2025-26633	Microsoft Management Console	✓	Phishing

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNK_CraftyCamel	Information theft and espionage	-	-	Sosano	-
Silk Typhoon	Information theft and espionage	China	CVE-2025-0282 CVE-2024-12356 CVE-2024-12686 CVE-2024-3400 CVE-2023-3519 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2021-44228	-	Windows
Dark Caracal	Information theft and espionage	Lebanon	-	Poco RAT	-
SideWinder	Information theft and espionage	India	CVE-2017-11882	StealerBot	Microsoft Office
Blind Eagle	Information theft and espionage, Financial crime	Colombia	CVE-2024-43451	PureCrypter RAT, Remcos RAT	Microsoft Windows
Mora_001	Information theft and espionage	-	CVE-2025-24472 CVE-2024-55591	SuperBlack	FortiOS, FortiProxy
MirrorFace	Information theft and espionage	China	-	ANEL (aka UPPERCUT), AsyncRAT	Windows
Desert Dexter	Information Theft, Espionage, Financial Gain	Libya	-	AsyncRAT	-
FishMonger	Information theft and espionage	China	-	ShadowPad, SodaMaster, Spyder	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UAT-5918	Information theft and espionage	-	-	-	-
Weaver Ant	Information theft and espionage	China	-	China Chopper, INMemory	Windows
Water Gamayun	Information theft and espionage	Russia	CVE-2025-26633	EncryptHub, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader	Microsoft Management Console

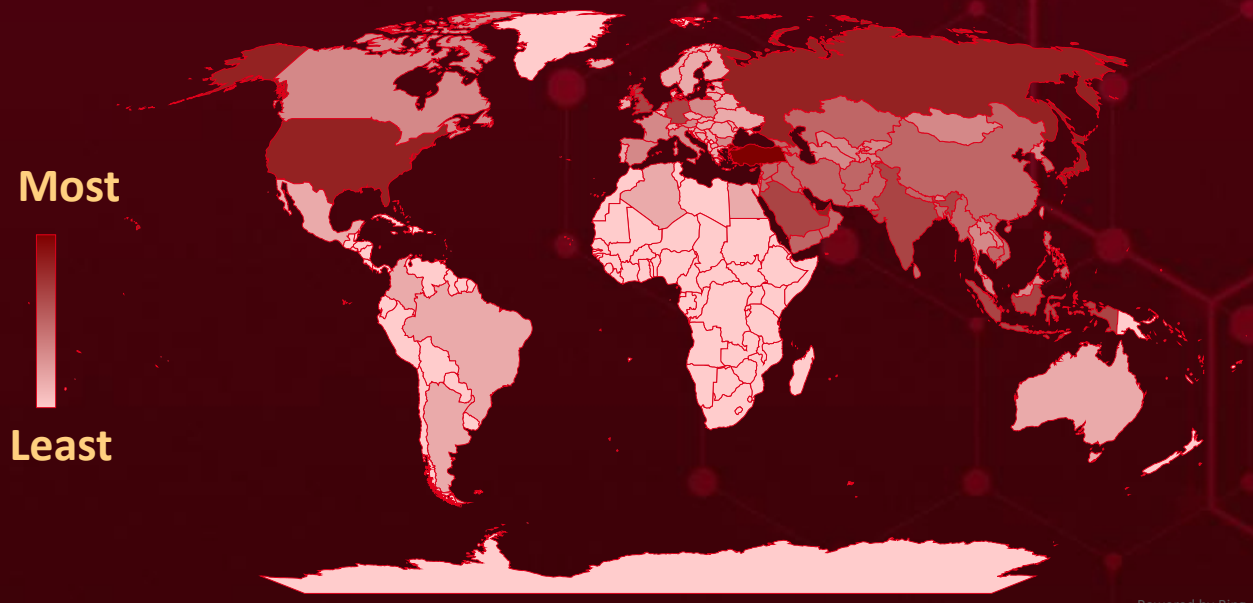
Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Messaging Application	Telegram Android versions 10.14.4 and older
FORTINET	VPN Client / Security Software	Fortinet FortiClientWindows, FortiClientLinux
	Endpoint Security Management	Fortinet FortiClientEMS
	Network Security Operating System	Fortinet FortiOS
	Secure Web Gateway (SWG)	FortiProxy Office
	Instant Messaging Server / Communication Software	BigAntSoft BigAnt Server 5.6.06 and below
vmware	Hypervisor / Virtualization Software	VMware ESXi Versions 7.0 and 8.0
	Cloud Infrastructure Platform	VMware Cloud Foundation Version 4.5.x and 5.x
	Telecommunications Cloud Platform	VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x
	Telecommunications Infrastructure Software	VMware Telco Cloud Infrastructure Version 3.x and 2.x
	Desktop Virtualization Software	VMware Workstation Version 17.x, VMware Fusion Version 13.x
ivanti	VPN / Secure Access Solutions	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
BeyondTrust	Enterprise Remote Workforce Solutions: Remote Access / Privileged Access Management	BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)
paloalto NETWORKS	Security Operating System	Palo Alto Networks PAN-OS

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
citrix	Secure Access Gateway	Citrix NetScaler ADC and NetScaler Gateway
Microsoft	Messaging and Collaboration Platform for Email	Microsoft Exchange Server
	Productivity Software	Microsoft Office, Microsoft Office 2019, Microsoft Office LTSC 2021 & 2024, Microsoft 365 Apps for Enterprise
	Operating System (OS)	Microsoft Windows, Windows 10 - 11 24H2
	Database Management System (DBMS)	Microsoft Access 2016
	Server Operating System (OS)	Windows Server 2008 - 2016, 2012 - 2025, 2008 - 2025
	System Administration and Management Tool.	Microsoft Management Console
THE APACHE SOFTWARE FOUNDATION	Java-based logging utility	Apache Log4j: 2.0 - 2.14.1
	Web Server and Servlet Container	Apache Tomcat Versions 11.0.0-M1 to 11.0.2, Apache Tomcat Versions 10.1.0-M1 to 10.1.34, Apache Tomcat Versions 9.0.0.M1 to 9.0.98
SITECORE	Content Management System (CMS), Digital Experience Platform (DXP)	Sitecore Experience Manager (XM) and Experience Platform (XP) prior to 10.4 versions
php	Web Development Framework	PHP version: 5 - 8.3.7
CISCO	Enterprise Networking Router	Cisco Small Business RV Series Routers
FT	Font Rendering Software Library	FreeType (FreeType) Version from 0.0.0 through 2.13.0
ScreenConnect	Remote Support Software	ConnectWise ScreenConnect

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Mobile Operating System	Apple iOS and iPadOS Versions before 18.3.2
	Desktop Operating System	Apple macOS Sequoia Versions before 15.3.2
	Operating System for Augmented Reality (AR) / Virtual Reality (VR)	Apple visionOS Version before 2.3.2
	Web Browser	Apple Safari Version before 18.3.1
	CI/CD (Continuous Integration/Continuous Deployment) Automation Tool and DevOps Tool.	GitHub Action
VEEAM	Data Backup and Disaster Recovery Solution	Veeam Backup & Replication
	Image Proxy Server	ChatGPT Pictureproxy.php
	Web Browser	Google Chrome (Windows) Version Prior to 134.0.6998.178
NEXT.JS	Web Development Framework	Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0

Targeted Countries



Color	Countries
	Turkey
	Japan
	Russia
	United Arab Emirates
	United States
	Germany
	India
	Cyprus
	Saudi Arabia
	Indonesia
	United Kingdom
	Palestine
	Armenia
	Georgia
	Bahrain
	Oman
	Iran
	Qatar
	Iraq
	Sri Lanka
	Israel
	Nepal

Color	Countries
	Bangladesh
	Pakistan
	Cambodia
	Philippines
	China
	Afghanistan
	Kuwait
	South Korea
	Yemen
	Syria
	Maldives
	Azerbaijan
	Myanmar
	Jordan
	Vietnam
	Kazakhstan
	Lebanon
	Spain
	Netherlands
	Timor-Leste
	France
	Poland

Color	Countries
	Austria
	Tajikistan
	Italy
	Uzbekistan
	Bhutan
	North Korea
	Kyrgyzstan
	Singapore
	Laos
	Taiwan
	Brunei
	Thailand
	Malaysia
	Turkmenistan
	Bulgaria
	Canada
	Mongolia
	Switzerland
	Serbia
	Liechtenstein
	Luxembourg
	Czech Republic
	Albania
	Latvia
	Algeria
	San Marino
	Malta
	Slovakia
	Mexico

Color	Countries
	Denmark
	Moldova
	Greece
	Monaco
	Ukraine
	Estonia
	Romania
	Montenegro
	Akrotiri and Dhekelia
	Andorra
	Finland
	Belarus
	Slovenia
	Ireland
	Bosnia and Herzegovina
	Belgium
	Sweden
	Norway
	Brazil
	Argentina
	Hungary

Color	Countries
	Colombia
	Iceland
	Australia
	Egypt
	Portugal
	Lithuania
	Croatia
	North Macedonia
	Ecuador
	Kosovo
	Western Sahara
	Honduras
	Dominican Republic
	Isle of Man
	Guernsey
	Cuba
	Chile
	Rwanda
	Transnistria
	Gibraltar
	Uganda
	Morocco

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1588** Obtain Capabilities	**T1566** Phishing	**T1204** User Execution
T1082 System Information Discovery	**T1588.006** Vulnerabilities	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1083** File and Directory Discovery
T1036 Masqueradin g	**T1068** Exploitation for Privilege Escalation	**T1140** Deobfuscate/D ecode Files or Information	**T1070** Indicator Removal	**T1041** Exfiltration Over C2 Channel
T1204.002 Malicious File	**T1190** Exploit Public-Facing Application	**T1055** Process Injection	**T1071** Application Layer Protocol	**T1543** Create or Modify System Process
T1003 OS Credential Dumping	**T1053** Scheduled Task/Job	**T1555** Credentials from Password Stores	**T1574** Hijack Execution Flow	**T1057** Process Discovery

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Poco RAT	MD5	a5073df86767ece0483da0316d66c15c, 2a0f523b9e52890105ec6fbccd207dcd, e0bf0aee954fd97457b28c9233253b0a, ec8746a1412d1bd1013dfe51de4b9fd1, fea98ca977d35828e294b7b9cc55fea9, c41645cba3de5c25276650a2013cd32b, 8778b9430947c46f68043666a71a2214, d8ec2df77a01064244f376322ba5aaf1, bbfbd1ece4f4aa43d0c68a32d92b17e5, 32c6c0d29593810f69d7c52047e49373
	SHA1	d0661df945e8e36aa78472d4b60e181769a3f23b, f3a495225dc34cdeba579fb0152e4ccba2e0ad42, ce611811d9200613c1a1083e683faec5187a9280, f719b736ed6b3351d1846127afec8e0c68e54c1d, 63b4d283eaf367122ce0dec9fc0e586e63ef0c78, d8021edcb42b6472dded45f7a028aff6dfe5aaa6, da3ea31e96fba64fcd840e930a99e705eb60c89b, ce60069d5fdef4acced66e6fc049f351c465ee1e, 2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154, 4bf76e731d655f67c9e78a616cf8b21002a53406
	SHA256	05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a, 08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb, 0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a, 0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3, 0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8, 121d941ba5a6ff8d99558e0919f49b926fbcd00e3007aad14ac85e799d55473c, 12e849ffba407d5db756879fd257c4b736eb4b6adac6320d2f1916d6a923fa46, 13306775fdf506b706693deccb44ec364fe04dbf3c471227c2439c2462e19080, 1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ced3e4a7670846205b3ac70, 18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b37932f473c787e24e57e8397

Attack Name	TYPE	VALUE
PolarEdge Botnet	SHA256	eda7cc5e1781c681afe99bf513fcaf5ae86afbf1d84dfd23aa563b1a043cbba8, 13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13, 464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd, 932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5, 121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef
	Domains	longlog[.]cc,landim[.]cc, hitchil[.]cc,Logchim[.]cc, ssofhoseuegsgrfnu[.]ru, aipricadd[.]top, firebasesafer[.]top, largeroofs[.]top, siotherlentsearsitech[.]shop, asustordownload[.]com, gardensc[.]cc, headached[.]cc, durianlink[.]cc, nternetd[.]cc,suiteiol[.]cc, centrequ[.]cc, icecreand[.]cc
	IPv4	119[.]8[.]186[.]227, 159[.]138[.]119[.]99, 43[.]129[.]205[.]244, 122[.]8[.]183[.]181, 195[.]123[.]212[.]54
RansomHub	IPv4	38[.]180[.]81[.]153, 108[.]181[.]115[.]171, 38[.]180[.]195[.]187, 185[.]174[.]101[.]240, 194[.]36[.]209[.]227, 92[.]118[.]112[.]143, 185[.]174[.]101[.]69, 92[.]118[.]112[.]208, 108[.]181[.]182[.]143, 173[.]44[.]141[.]226, 162[.]252[.]173[.]12, 23[.]227[.]193[.]172, 185[.]33[.]86[.]15, 45[.]66[.]248[.]150, 5[.]8[.]63[.]178, 88[.]119[.]175[.]70,

Attack Name	TYPE	VALUE
RansomHub	IPv4	185[.]219[.]220[.]175, 45[.]82[.]85[.]50, 104[.]238[.]61[.]144, 193[.]203[.]49[.]90, 38[.]146[.]28[.]93, 88[.]119[.]175[.]65, 37[.]1[.]212[.]18
	SHA256	2d4fa520c03b358223d8210f2e9bad572e4914efd6e70cb7db85a377e891e69a, 9e0a89c1b98f448865a73049a2b90bdfcd1b9846c4506441cfa6f0e429c1b329, 0ad9ab7aa9ecbc79bca0bfce5be58e0aa2606bdab3898daac43a6fa1231af164, 290b3fe64fd0875b2dc6bc0ad77dd52a70ad91a81dc24220523d38bf6c538afa, 35e853cc67bf1869127ed341ea7b1a5cbf7032523288d514dc4685924f898db2, 9e0274c4e57381e97ccceadba37b64da35cfc379f80abc53e40f310a5e6b690b, a46c3639ba099953def013430063ea018f616c10e4b1cb4fe9a26d261f9dab0d, bd82216f1341159e950e9e7a68015c54c4995c8fd7c12c28a839c5068b0919ad, df4c29cce2cf1a158ed0cefc860dc54f6fbb9bdafdc3bf5af60b506f78e69e4f, 6d215534002fe7627763f5dd971d529d2f2186431244108d1fd8b5e9e2c9a3b2, 24be73b64509dbad476b2873edf500554fed5885826b21e2f538993900d9a364, 84099559a6d1dd1fec8a5c065da9f0747fab8ebb7368c197224fa33035eabe8d, 3c9f0907304f7af7a7b88f931b6733698e86492d02e98e440e87e3ffe2153dbc, c4d51f5a4dc95b0ac4b4f44a74d282d84898ddf56293a7dfddd5cb5eb90ec989, 262a4dff66ceb25d35d5ca8d8d148c1fee88ea2ee1187877a5a0c8d6a0dd24b5, de4d1f58fa8fa9eb156a37a8d9a3396d58e804f92e5eee25878a36a116f66362, Ab84aeee213b902fde9740c466cd53af4bae6d5ea81a2b84c4d534b08b2fa049
Betruger	SHA256	ae7c31d4547dd293ba3fd3982b715c65d731ee07a9c1cc402234d8705c01dfca, b058c128c801e2ee03874e183239ff369c599f3a2324905ff73f99d16d3b1a16,

Attack Name	TYPE	VALUE
China Chopper	SHA1	23c4049121a9649682b3b901eaac0cc52c308756, 9022f78087e1679035e09160d59d679dc3ac345d, be52275b0c2086735dac478dc4f09fd16031669a, c879a8eb6630b0cd7537b068f4e9af2c9ca08a62, 25a593b9517d6c325598eab46833003c40f9491a, a9bbea73504139ce91a0ec20fef303c68a131cd4, 334a88e288ae18c6e3fd7fb2d1ad9548497d52ce, 4aeeae023766153a91b83d02b1b24da20c0dd135, 3cac6ff7cddcb8f82409c79c85d976300fc60861, 55eeaa904bc6518a2715cc77648e6c5187416a46, ff7b2c3938306261881c42e78d0df51d9bcdd574, 089439168d3c75b4da94ab801f1c46ad6b9e1fdc, a5c36b8022751cfeb4a88a21153847df3870c7c0, ad3dbec2b621807fa9a2f1b2f575d7077e494626, 4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb
INMemory	SHA1	f31920d636224356e8c7a182c2b9b37e42a09181, 9dc3d272652851428f5cc44f2fd9458bff1d6a78, 4dd22a08a5b103e1f2238aed7f7ce66c5a542533, 02065bbdb3209e0522db3225600b8e79f8a10293, 81622512757f897206a84b29ee866fb933fa3d48, 151dc47b213aaec3751ffd1427737c65757ab410, 492cbe143f795888d8e5006ac595f65f4565ed6e
VanHelsing	Bitcoin Wallet	bc1q0cuvj9eglxk43v9mqmyjzzh6m8qsvsanedwrru
	TOX Address	FEE914521FB507AB978107ACE3B69B4CA41DA89859408BAE23E1512E8C2E614A26C5FFD482A3
	TOR Address	vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd[.]onion, vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid[.]onion, vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad[.]onion, vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad[.]onion, vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd[.]onion, vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad[.]onion, vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd[.]onion
	SHA256	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17, 99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98
	SHA1	4211cec2f905b9c94674a326581e4a5ae0599df9, 79106dd259ba5343202c2f669a0a61b10adfadff, e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948

Attack Name	TYPE	VALUE
VanHelsing	MD5	3e063dc0de937df5841cb9c2ff3e4651, 5c254d25751269892b6f02d6c6384aef, cd9563b4cbc415b3920633b93c0d351b

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0364	✗	BigAnt Server 5.6.06 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:bigantsoft:bigant_server:*:*:*:*:*:*:*:*	-
BigAntSoft BigAnt Server Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1068 : Exploitation for Privilege, T1190: Exploit Public-Facing Application	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-54761	✗	BigAnt Server 5.6.06 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:bigantsoft:bigant_server:*:*:*:*:*:*:*:*	-
BigAntSoft BigAnt Office Messenger SQL Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	✗

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-22224</td><td>✗</td><td rowspan="2">VMware ESXi Versions 7.0 and 8.0,
VMware Cloud Foundation Version 4.5.x and 5.x,
VMware Telco Cloud Platform
Version 5.x, 4.x, 3.x, and 2.x,
VMware Telco Cloud Infrastructure Version 3.x and 2.x,
VMware Workstation Version 17.x</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:*
cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">VMware ESXi and Workstation TOCTOU Race Condition Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-367</td><td>T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-22225</td><td>  </td><td rowspan="2">VMware ESXi Versions 7.0 and 8.0,
VMware Cloud Foundation Version 4.5.x and 5.x,
VMware Telco Cloud Platform
Version 5.x, 4.x, 3.x, and 2.x,
VMware Telco Cloud Infrastructure
Version 3.x and 2.x</td><td>-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">VMware ESXi Arbitrary Write Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-123</td><td>T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-22226</td><td>  </td><td rowspan="2">VMware ESXi Versions 7.0 and 8.0,
VMware Cloud Foundation Version 4.5.x and 5.x,
VMware Telco Cloud Platform
Version 5.x, 4.x, 3.x, and 2.x,
VMware Telco Cloud Infrastructure
Version 3.x and 2.x,
VMware Workstation Version 17.x,
VMware Fusion Version 13.x</td><td>-</td></tr>
<tr><td>ZERO-DAY</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td></td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:*
cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:fusion:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-125</td><td>T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0282		Ivanti Connect Secure: 22.7R2 through 22.7R2.4 Ivanti Policy Secure: 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12356	✗	BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	https://www.beyondtrust.com/trust-center/security-advisories/bt24-10

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12686	✗	BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	https://www.beyondtrust.com/trust-center/security-advisories/bt24-11

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400		Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 <11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	Silk Typhoon
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Command Injection Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-77	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-27218		Sitecore Experience Manager (XM) and Experience Platform (XP) prior to 10.4 versions	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:*	-
Sitecore XM and XP Deserialization Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94	T1190 : Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003535

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-3519</td><td>  </td><td rowspan="2">NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13;
NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13;
NetScaler ADC and NetScaler Gateway version 12.1, now end of life;
NetScaler ADC 13.1-FIPS before 13.1-37.159;
NetScaler ADC 12.1-FIPS before 12.1-55.297;
NetScaler ADC 12.1-NDcPP before 12.1-55.297</td><td rowspan="2">Silk Typhoon</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter</td><td>https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4577	✗	PHP version: 5 -8.3.7	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	-
PHP-CGI OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.php.net/downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗	Microsoft Office	SideWinder
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*:*	StealerBot
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20118		Cisco Small Business RV Series Routers	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:rv016_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv016:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv042_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv042:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv042g_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv042g:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv082_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv082:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv320_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv320:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv325_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:cisco:rv325:-:*:*:*:*:*:*:*	PolarEdge Botnet
Cisco Small Business RV Series Routers Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24201	✗	Apple iOS and iPadOS Versions before 18.3.2, Apple macOS Sequoia Versions before 15.3.2, Apple visionOS Version before 2.3.2, Apple Safari Version before 18.3.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos_sequoia:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1497: Virtualization/Sandbox Evasion; T1190: Exploit Public-Facing Application	https://support.apple.com/en-us/118481 , https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/122285

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43451	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	Blind Eagle
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	PureCrypter RAT, Remcos RAT
NTLM Hash Disclosure Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1204: User Execution T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24983	✗	Windows: 10 Windows Server: 2008 - 2016	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24984	✗	Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows NTFS Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-532	T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24985	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Fast FAT File System Driver Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190 CWE-122	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24991	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows NTFS Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24993	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows NTFS Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-26630	✗	Microsoft Office 2019 Microsoft Access 2016 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:access:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:*	-
Microsoft Access Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1204: User Execution; T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26630

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-27363	✗	FreeType (FreeType) Version form 0.0.0 through 2.13.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:*	-
FreeType Out of Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://freetype.org/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709		ConnectWise ScreenConnect 23.9.7 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	Medusa Ransomware
ConnectWise ScreenConnect Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://www.screenconnect.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48788		Fortinet FortiClientEMS version 7.2.0 through 7.2.2, and 7.0.1 through 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*:*:*	Medusa Ransomware
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24472	✗	Fortinet FortiOS 7.0.0 through 7.0.16 and FortiProxy Office 7.2.0 through 7.2.12, 7.0.0 through 7.0.19	Mora_001
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortios:*:*:*:*:*:*:*:*:*	SuperBlack
Fortinet FortiOS Authorization Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55591	✗	Fortinet FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12	Mora_001
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortios:*:*:*:*:*:*:*:*:*	SuperBlack
Fortinet FortiOS Authorization Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30066	✗	GitHub Action v1 through v45.0.7	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:tj-actions:changed-files:*:*:*:*:*:*:*:*	-
tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1195: Supply Chain Compromise; T1055: Process Injection	https://github.com/tj-actions/changed-files/releases/tag/v46.0.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30154	✗	reviewdog/action-setup@v1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:reviewdog:action-setup:*:*:*:*:*:*:*:*	-
reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1055: Process Injection	https://github.com/reviewdog/action-setup/releases/tag/v1.3.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-24521		Windows: 7 - 11 21H2 and Windows Server: 2008 - 2022	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	RansomHub, Betruger
Microsoft Windows CLFS Driver Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27532		Veeam Backup & Replication	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	RansomHub, Betruger
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1212: Exploitation for Credential Access	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50570	✗	FortiClientWindows 7.4.0 - 7.4.1, 7.2.0 - 7.2.6, 7.0.0 - 7.0.13 and FortiClientLinux 7.4.0 - 7.4.2, 7.2.0 - 7.2.7, 7.0.0 - 7.0.13	BrazenBamboo
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:windows:*:* cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:linux:*:*	DEEPDATA, LIGHTSPY
Fortinet Cleartext Storage of Sensitive Information Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-312	T1212: Exploitation for Credential Access; T1133: External Remote Services	https://fortiguard.fortinet.com/psirt/FG-IR-23-278

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27564	✗	pictureproxy.php component (dirk1983/mm1.ltd, a third-party ChatGPT implementations)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:dirk1983:chatgpt:2023-05-23:*:*:*:*:*:*:*	-
ChatGPT Pictureproxy.php Server-Side Request Forgery Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy; T1135: Network Share Discovery; T1133: External Remote Services	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2783	✗	Google Chrome (Windows) Version prior to 134.0.6998.178	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium Mojo Sandbox Escape Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1036: Masquerading	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-29927	✗	Next.js versions prior to 12.3.5 and after 11.1.4, prior to 14.2.25 and after 14.0, prior to 15.2.3 and after 15.0, prior to 13.5.9 and after 13.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vercel:next.js:-:*:*:*:*:*:*:*	-
Next.js Middleware Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-285	T1505: Server Software Component; T1553: Subvert Trust Controls; T1574: Hijack Execution Flow	https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw, https://github.com/vercel/next.js/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24813		Apache Tomcat Versions 11.0.0-M1 to 11.0.2, Apache Tomcat Versions 10.1.0-M1 to 10.1.34, Apache Tomcat Versions 9.0.0.M1 to 9.0.98	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:*	-
Apache Tomcat Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502 CWE-44	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://tomcat.apache.org/security-11.html, https://tomcat.apache.org/security-10.html, https://tomcat.apache.org/security-9.html

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Havoc Demon	The Havoc Demon is part of the Havoc C2 framework, a sophisticated post-exploitation tool used by threat actors to control infected systems. It is delivered via a ZIP archive containing a malicious screen saver and a decoy document. The malware employs advanced evasion techniques like sleep obfuscation and indirect syscalls to bypass security measures. Recent campaigns have used Havoc Demon in phishing attacks, leveraging platforms like SharePoint and Microsoft Graph API for stealthy operations	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Remote Access, System Compromise	Windows
Hack tool			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
KaynLdr	KaynLdr is a shellcode loader that loads malware like Havoc Demon DLL, using a modified DJB2 hashing algorithm to evade detection. It executes the DLL's entry point, initiating malicious activities.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Malware execution	Windows
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sosano	Sosano is a sophisticated Golang-based backdoor malware used in highly targeted phishing campaigns, particularly against UAE's aviation and satellite sectors. It employs advanced obfuscation techniques, including unnecessary libraries to complicate analysis, and establishes communication with a command-and-control server to execute commands.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
UNK_CraftyCamel			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Poco RAT	Poco RAT is a sophisticated Remote Access Trojan (RAT) attributed to the Dark Caracal threat group, designed to provide attackers with full control over infected systems. It is delivered via phishing campaigns targeting Spanish-speaking users, often using PDF attachments or links to cloud-hosted malicious archives.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Dark Caracal			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PolarEdge Botnet	PolarEdge is a stealthy TLS backdoor designed to establish persistent remote access. It operates using predefined commands, allowing attackers to control compromised systems discreetly. Further investigation into associated payloads revealed infections across multiple device manufacturers, exposing a botnet of over 2,000 compromised assets worldwide.	Exploiting Vulnerability	CVE-2023-20118
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		System Compromise	Cisco Small Business RV Series Routers
ASSOCIATED ACTOR			**PATCH LINK**
-			EOL

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SilentCryptoMiner	SilentCryptoMiner is a covert cryptocurrency miner based on XMRig, capable of mining multiple cryptocurrencies like ETH, ETC, XMR, and RTM using various algorithms. It employs process hollowing to inject its miner code into dwm.exe for stealth and halts mining when specific processes defined in its configuration are active to evade detection. The malware is remotely controlled via a web panel and incorporates anti-analysis techniques, scanning for virtualized environments and enforcing an executable size between 680 MB and 800 MB. Its configuration is Base64-encoded and AES-CBC encrypted, adding an extra layer of obfuscation.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
CryptoMiner		Mine cryptocurrencies	-
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
StealerBot	StealerBot is a private post-exploitation toolkit, designed for espionage and stealthy data theft. Developed in .NET, it operates as a modular implant, avoiding traditional file-based execution by loading its components directly into memory via ModuleInstaller, a backdoor loader named by the attackers. StealerBot features multiple modules for deploying additional malware, capturing screenshots, logging keystrokes, stealing browser passwords and files, phishing Windows credentials, and escalating privileges by bypassing UAC, making it a versatile tool for persistent access and data exfiltration.	Exploiting Vulnerability	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Toolkit		System Compromise, Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
SideWinder			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PureCrypter RAT	PureCrypter is a .NET-based malware loader deeply integrated into the cybercriminal ecosystem, providing advanced evasion techniques and persistent access. Obfuscated using SmartAssembly, it employs compression, encryption, and obfuscation to bypass antivirus detection. Its key capabilities persistence, code injection, and defense mechanisms are configurable via Google's Protocol Buffer message format.	Exploiting Vulnerability	CVE-2024-43451
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Blind Eagle			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

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
Remcos RAT	Remcos, is often employed by attackers to gain complete control over systems. It operates stealthily, elevates privileges, and persists through reboots. Common methods of delivery include phishing emails, exploit kits, and watering hole attacks.	Exploiting Vulnerability	CVE-2024-43451
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft, Espionage	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Blind Eagle			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Medusa Ransomware	Medusa ransomware employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non- compliant organizations. Operating as a ransomware- as-a-service approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.	Exploiting Vulnerabilities	CVE-2024-1709 CVE-2023-48788
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, data theft, and financial loss	ConnectWise ScreenConnect, Fortinet FortiClientEMS
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.screenconnect.com/download , https://fortiguard.fortinet.com/psirt/FG-IR-24-007

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
SuperBlack	SuperBlack is a ransomware strain deployed by Mora_001, targeting Fortinet devices. By leveraging authentication bypass flaws in FortiOS and FortiProxy, attackers gain initial access, manipulate firewall configurations, and escalate privileges by creating a super_admin account via jsconsole and HTTPS methods, granting full administrative control. A modified variant of LockBit 3.0, SuperBlack shares traits with BlackMatte, BlackMatter, and BrainCipher, linking it to advanced cybercriminal networks.	Exploiting Vulnerabilities	CVE-2025-24472 CVE-2024-55591
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, Data theft	FortiOS, FortiProxy
ASSOCIATED ACTOR			**PATCH LINK**
Mora_001			https://fortiguard.fortinet.com/psirt/FG-IR-24-535

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SocGholish	SocGholish is defined by its concealed JavaScript loader, employing multiple evasion strategies to avoid conventional detection methods. It primarily spreads through compromised legitimate websites. The loader can download and execute malicious payloads, steal sensitive data, and run arbitrary commands, ensuring persistent access for continued exploitation and payload deployment.	Exploits compromised websites, Keitaro Traffic Distribution System (TDS) instances	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Persistent Access, Malware delivery	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
RansomHub	RansomHub, a ransomware-as-a-service (RaaS) that surfaced in early 2024, utilizes highly systematic and strategic tactics. It leverages an array of tools and methods aimed at amplifying the effectiveness of its attacks while reducing the likelihood of detection.	Exploits compromised websites, Keitaro Traffic Distribution System (TDS) instances	CVE-2022-24521 CVE-2023-27532
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Exfiltration of Data, System Compromise, Financial Loss	Microsoft Windows, Veeam Backup & Replication
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521, https://www.veeam.com/kb4424

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
r77	r77 is a user-mode rootkit designed to manipulate system processes, conceal files, and modify registry entries. It establishes persistence by embedding obfuscated scripts in the Windows Registry and configuring scheduled tasks to run covertly in the background. Additionally, it alters registry keys to register a fake driver, further strengthening its foothold.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Remote Access, Exfiltration of Data, System Integrity Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StilachiRAT	StilachiRAT is a recently discovered remote access trojan (RAT) that bypasses detection using delayed execution, API obfuscation, and sandbox evasion. It facilitates lateral movement, credential theft, and remote command execution.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Credential Theft, System Integrity Risk, Remote Access	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

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
AsyncRAT	AsyncRAT is a publicly available remote access trojan (RAT) on GitHub. A modified version ensures persistence by creating a scheduled task that triggers at startup. Upon activation, a complex sequence initiates AsyncRAT within Windows Sandbox, which must be manually enabled and requires a reboot.	Spear-phishing, exploiting social media	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote Control, System Persistence	Windows
ASSOCIATED ACTOR			**PATCH LINK**
MirrorFace, Desert Dexter			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ClearFake	ClearFake is a malicious JavaScript framework that evolves to deceive users into downloading malware. Initially, it used fake browser update alerts in 2023, then adopted the ClickFix tactic, showing misleading error messages to prompt users into executing malicious PowerShell commands. The latest variant now integrates with the Binance Smart Chain, utilizing smart contract ABIs to load JavaScript, fingerprint victims' systems, and deploy its payload.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Framework		Malware Distribution, System Integrity Risk	Windows and Mac
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
Emmenhtal	Emmenhtal, also known as IDATDropper or PEAKLIGHT, is a malicious loader likely distributed since early 2024. It is an obfuscated, multistage payload that uses the LOLBIN mshta.exe to execute a malicious HTA file containing JavaScript. Once executed, the JavaScript decodes and runs a PowerShell script, which decrypts an obfuscated PowerShell loader. This loader ultimately downloads and executes final-stage stealers and commodity RATs.	Social Engineering, Deployed by ClearFake	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Bypassing Traditional Detection, Malware Distribution	Windows and Mac
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma	Lumma Stealer, also known as LummaC2 Stealer, is an information-stealing malware written in C that has been available as Malware-as-a-Service (MaaS) on Russian-speaking forums since at least August 2022. It primarily targets cryptocurrency wallets and two-factor authentication (2FA) browser extensions, stealing sensitive data from the victim's machine.	Social Engineering, Deployed by ClearFake	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss, Data Theft	Windows and Mac
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
Vidar	Vidar is an infostealer malware, operating as Malware-as-a-Service, first discovered in late 2018. Running on Windows, it collects sensitive data from browsers and digital wallets, posing a significant threat by stealing personal information and cryptocurrency from infected users.	Social Engineering, Deployed by ClearFake	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss, Data Theft	Windows and Mac
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShadowPad	ShadowPad, also known as POISONPLUG.SHADOW and XShellGhost, is a sophisticated, modular backdoor sold privately. Regularly updated and delivered in shellcode format, it offers a wide range of capabilities. Popular among threat actors for its cost-effectiveness, ShadowPad's plugins are tailored to specific functions. It is commonly used by China-backed APTs to maintain long-term access in compromised environments, adapting the malware for espionage campaigns.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Persistence Access, Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
FishMonger			-

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
SodaMaster	SodaMaster is a backdoor used for data exfiltration and remote command execution. It exploits legitimate executables through DLL side-loading and, in some instances, incorporates a password stealer for Firefox.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, Remote Access	-
ASSOCIATED ACTOR			**PATCH LINK**
FishMonger			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Spyder	Spyder Loader malware appears focused on intelligence gathering. It loads AES-encrypted blobs to create the wlbsctrl.dll, which serves as a next-stage loader to execute its payload. Using the CryptoPP C++ library, the variant seen in recent attacks employs the ChaCha20 algorithm for string obfuscation. To hinder analysis, the malware wipes the wlbsctrl.dll content before deleting it.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft, Espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
FishMonger			-

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
VenomRAT	VenomRAT 6.0.3 in this campaign leverages Hidden Virtual Network Computing (HVNC) to enable remote control of compromised systems. Upon execution, it replicates itself, alters registry entries for persistence, and places files in the Startup folder to ensure execution on reboot. To avoid detection, it uses Pastebin.com to store payloads and exfiltrated data.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, Persistence, Remote Access	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Betruger	Betruger is a versatile malware that integrates keylogging, network scanning, credential dumping, and privilege escalation into a single tool, reducing the need for multiple attack components. By disguising itself as harmless files like "mailer.exe," it evades detection, boosting the stealth of ransomware attacks.	Deployed by RansomHub	CVE-2022-24521 CVE-2023-27532
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Control, Exfiltration of Data	Microsoft Windows, Veeam Backup & Replication
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521, https://www.veeam.com/kb4424

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
China Chopper	The China Chopper web shell is a lightweight malicious tool that allows attackers to remotely control compromised web servers. It provides features like file management, command execution, and data exfiltration. Its small size and stealth make it effective for maintaining persistent access, enabling further exploitation, and avoiding detection by conventional security measures. Additionally, China Chopper supports AES encryption for its payload.	Compromised Zyxel CPE routers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Web Shell		Remote Control, Data Exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Weaver Ant			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
INMemory	InMemory Web Shell runs malicious code entirely in memory to avoid detection. It decodes a hardcoded GZipped Base64 string into a file called 'eval.dll' and executes it without saving anything to disk. The process involves decoding the string, decompressing it, and then loading the code directly into memory for execution.	Compromised Zyxel CPE routers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Web Shell		Remote Control, Data Exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Weaver Ant			-

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
VanHelsing	VanHelsing is a new ransomware-as-a-service (RaaS) operation that uses a double extortion strategy. It encrypts files with a ".vanhelsing" extension and exfiltrates sensitive data from the victim. Written in C++, it employs advanced encryption methods.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	Windows, Linux, BSD, ARM, and VMware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EncryptHub	EncryptHub is a sophisticated malware-as-a-service platform that enables multi-stage attacks, including credential theft, keylogging, and remote access. It targets high-value systems using trojanized applications and pay-per-install services.	Phishing	CVE-2025-26633
TYPE		**IMPACT**	**AFFECTED PRODUCT**
MaaS		Data theft	Microsoft Management Console
ASSOCIATED ACTOR			**PATCH LINK**
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

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
DarkWisp	DarkWisp is a PowerShell-based backdoor designed for persistent unauthorized access and reconnaissance. It exfiltrates sensitive data and executes commands via TCP and HTTPS communication channels.	Phishing	CVE-2025-26633
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Persistent control, data exfiltration	Microsoft Management Console
ASSOCIATED ACTOR			**PATCH LINK**
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SilentPrism	SilentPrism is a stealthy backdoor used by Water Gamayun for long-term system control. It's designed to establish persistent access to compromised Windows systems, execute arbitrary shell commands, and maintain remote control.	Phishing	CVE-2025-26633
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Remote control, modular attacks	Microsoft Management Console
ASSOCIATED ACTOR			**PATCH LINK**
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

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
Rhadamanthys	Rhadamanthys is information-stealing malware distributed through large-scale phishing campaigns. It is designed to exfiltrate sensitive data from infected systems, including credentials and financial information. Targeting various sectors globally has been observed, often masquerading as legitimate communications to deceive victims.	Phishing	CVE-2025-26633
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Information stealer		Data theft, espionage	Microsoft Management Console
ASSOCIATED ACTOR			**PATCH LINK**
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Stealc	Stealc is an advanced information stealer capable of extracting credentials, browser data, cryptocurrency wallets, and other sensitive information from infected systems.	Phishing	CVE-2025-26633
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Information stealer		Credential theft, financial loss	Microsoft Management Console
ASSOCIATED ACTOR			**PATCH LINK**
Water Gamayun			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>MSC EvilTwin</td><td rowspan="6">MSC EvilTwin is a PowerShell trojan loader exploiting MMC vulnerabilities to execute malicious payloads. It uses fake directories and manipulated .msc files to maintain persistence and steal data.</td><td>Phishing</td><td>CVE-2025-26633</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>Loader</td><td rowspan="3">Code execution, system compromise</td><td>Microsoft Management Console</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Water Gamayun</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633</td></tr>
</table>

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

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UNK_CraftyCamel</td><td>-</td><td rowspan="2">Aviation and Satellite</td><td rowspan="2">United Arab Emirates</td></tr>
<tr><td>MOTIVE
Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Sosano</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0011: Command and Control, T1566: Phishing, T1566.001: Spearphishing Attachment, T1036: Masquerading, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.006: Python, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1083: File and Directory Discovery, T1070: Indicator Removal, T1586: Compromise Accounts, T1586.002: Email Accounts, T1222: File and Directory Permissions Modification, T1218: System Binary Proxy Execution, T1218.005: Mshta, T1071: Application Layer Protocol</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Silk Typhoon (aka Hafnium, Red Dev 13, timmy, ATK233, G0125, Operation Exchange Marauder)	China	IT Services, Healthcare, Legal services, Higher education, Defense, Government, Non-governmental organizations (NGOs), Energy, Law firms, and Policy think tanks	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2025-0282 CVE-2024-12356 CVE-2024-12686 CVE-2024-3400 CVE-2023-3519 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2021-44228	-	Windows

TTPs
TA0042: Resource Development, TA0006: Credential Access, TA0001: Initial Access, TA0008: Lateral Movement, TA0002: Execution, TA0005: Defense Evasion, TA0003: Persistence, TA0010: Exfiltration, T1078: Valid Accounts, T1027: Obfuscated Files or Information, T1505.003: Web Shell, T1574.010: Services File Permissions Weakness, TA0004: Privilege Escalation, TA0040: Impact, T1190: Exploit Public-Facing Application, T1555: Credentials from Password Stores, T1505, TA0009: Collection, T1110.003: Password Spraying, T1586, TA0007: Discovery, TA0010: Exfiltration, TA0011: Command and Control, T1110: Brute Force, T1068: Compromise Accounts, T1083: File and Directory Discovery, T1106: Server Software Component, T1598: Native API, T1574: Phishing for Information Hijack Execution Flow, T1195.002: Compromise Software Supply Chain, T1195: Supply Chain Compromise, T1567.002: Exfiltration to Cloud Storage: Exploitation for Privilege Escalation, T1041: Exfiltration Over C2 Channel, T1059: Command and Scripting Interpreter, T1584: Compromise Infrastructure, T1584.003: Virtual Private Server

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Dark Caracal (aka ATK 27, TAG-CT3, G0070)</td><td>Lebanon</td><td rowspan="2">Banking, Manufacturing and distribution, Healthcare and Pharmaceutical services, Logistics services, Marketplaces</td><td rowspan="2">Latin America</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Poco RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, T1608: Stage Capabilities, T1608.001: Upload Malware, T1583: Acquire Infrastructure, T1583.003: Virtual Private Server, T1588: Obtain Capabilities, T1588.001: Malware, T1566: Phishing, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell: T1055: Process Injection, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1027.002: Software Packing, T1113: Screen Capture, T1082: System Information Discovery, T1132: Data Encoding, T1132.001: Standard Encoding, T1571: Non-Standard Port, T1665: Hide Infrastructure, T1036: Masquerading</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)	India	Government, Military, Defense, Logistics, Maritime, Nuclear, Energy, Telecommunications, Consulting Firms, IT Service, Real Estate, and Hospitality	Pakistan, Sri Lanka, India, Nepal, Bangladesh, Myanmar, Indonesia, Cambodia, Philippines, Vietnam, Egypt, Saudi Arabia, United Arab Emirates, Turkey, Algeria, Djibouti, Mozambique, Rwanda, Uganda, Austria, Bulgaria, Afghanistan, Maldives, and China
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	CVE-2017-11882	StealerBot	Microsoft Office

TTPs
TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0001: Initial Access; TA0002: Exécution; TA0040: Impact; T1584: Compromise Infrastructure; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1053.005: Scheduled Task; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1218.005: Mshta; T1218: System Binary Proxy Execution; T1574.002: DLL Side-Loading; T1548: Abuse Elevation Control Mechanism; T1003: OS Credential Dumping; T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1548.002: Bypass User Account Control; T1056.001: Keylogging; T1056: Input Capture; T1047: Windows Management Instrumentation; T1555: Credentials from Password Stores; T1012: Query Registry; T1113: Screen Capture; T1059.007: JavaScript; T1059.003: Windows Command Shell

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5"> 

Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)</td><td>Colombia</td><td rowspan="3">Government, Judicial Institutions, Private Organizations, Financial, Critical Infrastructure</td><td rowspan="3">Colombia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2024-43451</td><td>PureCrypter RAT, Remcos RAT</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1587: Develop Capabilities; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.001: Malware; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1546: Event Triggered Execution; T1055: Process Injection; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1140: Deobfuscate/Decode Files or Information; T1573: Encrypted Channel; T1550.002: Pass the Hash</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Mora_001</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2025-24472
CVE-2024-55591</td><td>SuperBlack</td><td>FortiOS, FortiProxy</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0004: Privilege Escalation; TA0042: Resource Development; TA0040: Impac; TA0002: Exécution; TA0008: Lateral Movement; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0011: Command and Control; TA0003: Persistences; TA0007: Discovery; T1047: Windows Management Instrumentation; T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpréter; T1210: Exploitation of Remote Services; T1133: External Remote Services; T1556: Modify Authentication Process; T1136.001: Local Account; T1136: Create Account; T1602:Data from Configuration Repository; T1588: Obtain Capabilities; T1588.005: Exploits; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1068: Exploitation for Privilege Escalation; T1098: Account Manipulation; T1486: Data Encrypted for Impact; T1489: Service Stop; T1020: Automated Exfiltration; T1556.001: Domain Controller Authentication</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRY</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="4"> 
MirrorFace (aka Earth Kasha, Operation LiberalFace)</td><td>China</td><td rowspan="3">Diplomatic Organization</td><td rowspan="3">Europe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>ANEL (aka UPPERCUT), AsyncRAT</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.002: Email Accounts; T1585.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1566: Phishing; T1566.002: Spearphishing Link; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1027: Obfuscated Files or Information; T1027.004: Compile After Delivery; T1027.007: Dynamic API Resolution; T1027.011: Fileless Storage; T1055: Process Injection; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestomp; T1070.001: Clear Windows Event Logs; T1127: Trusted Developer Utilities Proxy Execution; T1127.001: MSBuild; T1140: Deobfuscate/Decode Files or Information; T1622: Debugger Evasion; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1564.003: Hidden Window; T1564.006: Run Virtual Instance; T1112: Modify Registry; T1036: Masquerading; T1036.007: Double File Extension; T1218: System Binary Proxy Execution; T1221: Template Injection; T1012: Query Registry; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1124: System Time Discovery; T1087: Account Discovery; T1087.002: Domain Account; T1115: Clipboard Data; T1113: Screen Capture; T1001: Data Obfuscation; T1001.001: Junk Data; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1573: Encrypted Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1132: Data Encoding; T1132.001: Standard Encoding; T1030: Data Transfer Size Limits; T1041: Exfiltration Over C2 Channel; T1047: Windows Management Instrumentation; T1560: Archive Collected Data; T1090: Proxy; T1059.005: Visual Basic</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Desert Dexter</td><td>Libya</td><td rowspan="3">Oil production, Construction, Information Technology, Agriculture</td><td rowspan="3">Libya, Saudi Arabia, Egypt, Turkey, United Arab Emirates, Qatar, Tunisia, Russia, Akrotiri and Dhekelia, Bahrain, Cyprus, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Syria, Yemen, Algeria, Morocco, Sudan, Western Sahara</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage, Financial Gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>AsyncRAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1588: Obtain Capabilities; T1588.001: Malware; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.006: SEO Poisoning; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1059.007: JavaScript; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1620: Reflective Code Loading; T1056: Input Capture; T1056.001: Keylogging; T1074: Data Staged; T1074.001: Local Data Staging; T1113: Screen Capture; T1568: Dynamic Resolution; T1571: Non-Standard Port; T1020: Automated Exfiltration; T1020.001: Traffic Duplication; T1657: Financial Theft; T1036: Masquerading; T1070.004: File Deletion; T1070: Indicator Removal; T1055: Process Injection; T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
FishMonger (aka Earth Lusca, TAG-22, RedHotel, Bronze University, Red Scylla, Chromium, AQUATIC PANDA, Charcoal Typhoon, ControlX, Red Dev 10)	China	Government, NGOs, Think Tank, Religion	Asia, Europe, and the United States
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	ShadowPad, SodaMaster, Spyder	-

TTPs
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.004: Server; T1583.001: Domains; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1072: Software Deployment Tools; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1556: Modify Authentication Process; T1556.002: Password Filter DLL; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1003.002: Security Account Manager; T1087: Account Discovery; T1087.001: Local Account; T1016: System Network Configuration Discovery; T1007: System Service Discovery; T1057: Process Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1095: Non-Application Layer Protocol

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UAT-5918</td><td>-</td><td rowspan="2">Critical Infrastructure, Information Technology, Telecommunication Providers, Universities, Healthcare</td><td rowspan="2">Taiwan, Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0043: Reconnaissance; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation; T1090: Proxy; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1590: Gather Victim Network Information; T1136: Create Account; T1217: Browser Information Discovery; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1003: OS Credential Dumping; T1082: System Information Discovery; T1592: Gather Victim Host Information; T1505: Server Software Component; T1505.003: Web Shell; T1555: Credentials from Password Stores; T1016: System Network Configuration Discovery</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 

Weaver Ant</td><td>China</td><td rowspan="3">Telecommunication</td><td rowspan="3">Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>China Chopper, INMemory</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1590: Gather Victim Network Information; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1059.007: JavaScript; T1078: Valid Accounts; T1078.002: Domain Accounts; T1078.003: Local Accounts; T1505: Server Software Component; T1505.003: Web Shell; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1055: Process Injection; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1003: OS Credential Dumping; T1003.002: Security Account Manager; T1087: Account Discovery; T1087.002: Domain Account; T1083: File and Directory Discovery; T1135: Network Share Discovery; T1018: Remote System Discovery; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1570: Lateral Tool Transfer; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1074: Data Staged; T1074.001: Local Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1572: Protocol Tunneling; T1090: Proxy; T1090.001: Internal Proxy; T1048: Exfiltration Over Alternative Protocol</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Water Gamayun (aka EncryptHub and Larva-208)	Russia	All	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-26633	EncryptHub, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader	Microsoft Management Console
TTPs			
TA0004: Privilege Escalation; TA0001: Initial Access; TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0005: Defense Evasion; TA0011: Command and Control; T1218.014: MMC; T1218: System Binary Proxy Execution; T1543: Create or Modify System Process; T1566: Phishing; T1204: User Execution; T1189: Drive-by Compromise; T1059.001: PowerShell; T1036: Masquerading; T1068: Exploitation for Privilege Escalation; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1041: Exfiltration Over C2 Channel; T1059.003: Windows Command Shell; T1222: File and Directory Permissions Modification			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1598: Phishing for Information	
	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1592: Gather Victim Host Information	
	T1595: Active Scanning	
	T1590: Gather Victim Network Information	
TA0042: Resource Development	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.001: Malware
		T1588.002: Tool
		T1588.006: Vulnerabilities
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
		T1583.001: Domains
		T1583.004: Server
		T1583.008: Malvertising
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.006: SEO Poisoning
		T1608.004: Drive-by Target
	T1585: Establish Accounts	T1585.002: Email Accounts
		T1585.003: Cloud Accounts
		T1585.001: Social Media Accounts
TA0001: Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1664: Exploitation for Initial Access	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript

Tactic	Technique	Sub-technique
TA0002: Execution	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
	T1072: Software Deployment Tools	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1623: Command and Scripting Interpreter	
	T1658: Exploitation for Client Execution	
TA0003: Persistence	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1176: Browser Extensions	
	T1546: Event Triggered Execution	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	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
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1556: Modify Authentication Process	T1556.001: Domain Controller Authentication
		T1556.002: Password Filter DLL
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.010: Services File Permissions Weakness
TA0004: Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1546: Event Triggered Execution	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.012: Process Hollowing
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1098: Account Manipulation	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.010: Services File Permissions Weakness
TA0005: Defense Evasion	T1127: Trusted Developer Utilities Proxy Execution	T1127.001: MSBuild
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1006: Direct Volume Access	
	T1014: Rootkit	
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.004: Compile After Delivery
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.011: Fileless Storage
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.007: Double File Extension
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.014: MMC
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1202: Indirect Command Execution	
	T1221: Template Injection	
	T1222: File and Directory Permissions Modification	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
		T1070.006: Timestomp
		T1070.009: Clear Persistence
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1556: Modify Authentication Process	T1556.001: Domain Controller Authentication
		T1556.002: Password Filter DLL

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
		T1562.003: Impair Command History Logging
	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
		T1574.010: Services File Permissions Weakness
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1056: Input Capture	T1056.001: Keylogging
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1110: Brute Force	T1110.003: Password Spraying
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	T1556.001: Domain Controller Authentication
		T1556.002: Password Filter DLL
	T1040: Network Sniffing	
	T1212: Exploitation for Credential Access	
	T1558: Steal or Forge Kerberos Tickets	
TA0007: Discovery	T1007: System Service Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1124: System Time Discovery	
	T1482: Domain Trust Discovery	
	T1622: Debugger Evasion	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1082: System Information Discovery	T1069.001: Local Groups
		T1069.002: Domain Groups
	T1087: Account Discovery	T1087.001: Local Account
		T1087.002: Domain Account

Tactic	Technique	Sub-technique
TA0007: Discovery	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
	T1518: Software Discovery	T1518.001: Security Software Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	T1550.002: Pass the Hash
	T1072: Software Deployment Tools	
	T1210: Exploitation of Remote Services	
TA0009: Collection	T1056: Input Capture	T1056.001: Keylogging
	T1074: Data Staged	T1074.001: Local Data Staging
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1005: Data from Local System	
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1213: Data from Information Repositories	
	T1602: Data from Configuration Repository	
TA0011: Command and Control	T1001: Data Obfuscation	T1001.001: Junk Data
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.001: Internal Proxy
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	
	T1665: Hide Infrastructure	
TA0010: Exfiltration	T1048: Exfiltration Over Alternative Protocol	
	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	T1020.001: Traffic Duplication
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage

Tactic	Technique	Sub-technique
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1529: System Shutdown/Reboot	
	T1657: Financial Theft	

Top 5 Takeaways

#1

In **March 28, zero-day** vulnerabilities were discovered, with the '**Four Celebrity Vulnerabilities**' taking center stage. These included flaws such as **ProxyLogon**, **Log4Shell**, **MSC EvilTwin**, and **EvilVideo**. Meanwhile, two critical vulnerabilities, **CVE-2025-0364** and **CVE-2024-54761**, were uncovered in BigAnt Server, with **no official patch** available and public exploits in circulation.

#2

Silk Typhoon, a state-sponsored espionage group, has shifted tactics, leveraging widely used IT solutions to infiltrate systems through unpatched vulnerabilities. Meanwhile, several emerging threat actors surfaced in **March 2025**, including **UNK_CraftyCamel**, **Dark Caracal**, **Mora_001**, **MirrorFace**, **Desert Dexter**, **Weaver Ant**, and **Water Gamayun**, marking a significant uptick in global cyber threats.

#3

Cyberattacks hit **143 countries** in March, with **Turkey, Japan, Russia, the United Arab Emirates,** and the **United States** facing the brunt of the threats. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region was immune as adversaries expanded their reach globally.

#4

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

#5

Ransomware is on the rise, with relentless variants like **Medusa**, **SuperBlack**, **RansomHub**, and **VanHelsing** claiming new victims. As attacks grow more sophisticated, organizations must act fast strengthening defenses, securing backups, and refining disaster recovery plans to stay ahead of the threat.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **43 significant vulnerabilities** and block the indicators related to the **12 active threat actors, 35 active malware,** and **217 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 **43 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).

Hive Pro Threat Advisories (MARCH 2025)

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

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
Havoc Demon	SHA256	cc151456cf7df7ff43113e5f82c4ce89434ab40e68cd6fb362e4ae4f70ce65b3
KaynLdr	SHA256	A5210aaa9eb51e866d9c2ef17f55c0526732eacb1a412b910394b6b51246b7da
Sosano	SHA256	0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c
Poco RAT	MD5	a5073df86767ece0483da0316d66c15c, 2a0f523b9e52890105ec6fbccd207dcd, e0bf0aee954fd97457b28c9233253b0a, ec8746a1412d1bd1013dfe51de4b9fd1, fea98ca977d35828e294b7b9cc55fea9, c41645cba3de5c25276650a2013cd32b, 8778b9430947c46f68043666a71a2214, d8ec2df77a01064244f376322ba5aaf1, bbfbd1ece4f4aa43d0c68a32d92b17e5, 32c6c0d29593810f69d7c52047e49373
	SHA1	d0661df945e8e36aa78472d4b60e181769a3f23b, f3a495225dc34cdeba579fb0152e4ccba2e0ad42, ce611811d9200613c1a1083e683faec5187a9280, f719b736ed6b3351d1846127afec8e0c68e54c1d, 63b4d283eaf367122ce0dec9fc0e586e63ef0c78, d8021edcb42b6472dded45f7a028aff6dfe5aaa6, da3ea31e96fba64fcd840e930a99e705eb60c89b, ce60069d5fdef4acced66e6fc049f351c465ee1e, 2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154, 4bf76e731d655f67c9e78a616cf8b21002a53406
	SHA256	05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a, 08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb, 0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a, 0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3, 0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8, 121d941ba5a6ff8d99558e0919f49b926fbcd00e3007aad14ac85e799d55473c, 12e849ffba407d5db756879fd257c4b736eb4b6adac6320d2f1916d6a923fa46, 13306775fdf506b706693deccb44ec364fe04dbf3c471227c2439c2462e19080,

Attack Name	TYPE	VALUE
Poco RAT	SHA256	1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ced3e4a7670846205b3ac70, 18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b37932f473c787e24e57e8397
PolarEdge Botnet	SHA256	eda7cc5e1781c681afe99bf513fcaf5ae86afbf1d84dfd23aa563b1a043cbba8, 13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13, 464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd, 932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5, 121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef
	Domains	longlog[.]cc,landim[.]cc, hitchil[.]cc,Logchim[.]cc, ssofhoseuegsgrfnu[.]ru, aipricadd[.]top, firebasesafer[.]top, largeroofs[.]top, siotherlentsearsitech[.]shop, asustordownload[.]com, gardensc[.]cc, headached[.]cc, durianlink[.]cc, nternetd[.]cc,suiteiol[.]cc, centrequ[.]cc, icecreand[.]cc
	IPv4	119[.]8[.]186[.]227, 159[.]138[.]119[.]99, 43[.]129[.]205[.]244, 122[.]8[.]183[.]181, 195[.]123[.]212[.]54
SilentCryptoMiner	MD5	a2a9eeb3113a3e6958836e8226a8f78f, 5c5c617b53f388176173768ae19952e8, ac5cb1c0be04e68c7aee9a4348b37195
	SHA256	44B212683CDEF95C55DD2E645B414B5179B589C64F1DBD6F5B4252BD4CA59790, 9D93E3AB8D0D9BD84F9F0F9FA2F997DF187CCCE49F9A2BDE7B49AD17E3A3CE08, F5232578BF310696F4E1D89F2A51369EFC32819DAF83A3BE38C3C11962F3A8BE
StealerBot	MD5	3a036a1846bfeceb615101b10c7c910e, 47f51c7f31ab4a0d91a0f4c07b2f99d7, f3058ac120a2ae7807f36899e27784ea,

Attack Name	TYPE	VALUE
StealerBot	MD5	0fbb71525d65f0196a9bfbffea285b18, 1ed7ad166567c46f71dc703e55d31c7a, 2f0e150e3d6dbb1624c727d1a641e754, bf16760ee49742225fdb2a73c1bd83c7, b3650a88a50108873fc45ad3c249671a, 4c40fcb2a12f171533fc070464db96d1, eef9c0a9e364b4516a83a92592ffc831
	SHA256	5740947bb9267e1be8281edc31b3fb2d57a71d2c96a47eeeaa6482c0927aa6a4
PureCrypter RAT	SHA256	3acd90196dcf53dd6e265dc9c89b3cb0c47648a3b7ac8f226c6b4b98f39f2fc8
Remcos RAT	SHA256	35612c79bde985c957ba521bbc7aa8541c31fb235ca7a91d0ee225f988921eb4, 613fb5ffbce15d7c71a019dd0f80256b2d05772e4f62c2fbf7c74164f1227755, f28ffdb035e739806d6c9bfc9ef2cd86f7fac2656018c8d0f2706647bcf5332f, 5433726d3912a95552d16b72366eae777f5f34587e1bdaa0c518c5fcbc3d8506
Medusa Ransomware	SHA256	d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, 5f9d864d11c79b34c4502edba7d0e007197d0df086a6fb9d6bfda84a1771ff0f
SuperBlack	SHA256	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404, f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513, 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2, 782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045, d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88
SocGholish	Domains	rednosehorse[.]com, apiexplorerzone[.]com, smthwentwrong[.]com, newgoodfoodmarket[.]com, foundedbrounded[.]org, packedbrick[.]com, newgreenvibes[.]com, rapiddevapi[.]com, digdonger[.]org, blackshelter[.]org, blacksaltys[.]com, brickedpack[.]com, blessedwirrow[.]org

Attack Name	TYPE	VALUE
RansomHub	IPv4	38[.]180[.]81[.]153, 108[.]181[.]115[.]171, 38[.]180[.]195[.]187, 185[.]174[.]101[.]240, 194[.]36[.]209[.]227, 92[.]118[.]112[.]143, 185[.]174[.]101[.]69, 92[.]118[.]112[.]208, 108[.]181[.]182[.]143, 173[.]44[.]141[.]226, 162[.]252[.]173[.]12, 23[.]227[.]193[.]172, 185[.]33[.]86[.]15, 45[.]66[.]248[.]150, 5[.]8[.]63[.]178, 88[.]119[.]175[.]70, 185[.]219[.]220[.]175, 45[.]82[.]85[.]50, 104[.]238[.]61[.]144, 193[.]203[.]49[.]90, 38[.]146[.]28[.]93, 88[.]119[.]175[.]65, 37[.]1[.]212[.]18
	SHA256	2d4fa520c03b358223d8210f2e9bad572e4914efd6e70cb7db85a377e891e69a, 9e0a89c1b98f448865a73049a2b90bdfcd1b9846c4506441cfa6f0e429c1b329, 0ad9ab7aa9ecbc79bca0bfce5be58e0aa2606bdab3898daac43a6fa1231af164, 290b3fe64fd0875b2dc6bc0ad77dd52a70ad91a81dc24220523d38bf6c538afa, 35e853cc67bf1869127ed341ea7b1a5cbf7032523288d514dc4685924f898db2, 9e0274c4e57381e97ccceadba37b64da35cfc379f80abc53e40f310a5e6b690b, a46c3639ba099953def013430063ea018f616c10e4b1cb4fe9a26d261f9dab0d, bd82216f1341159e950e9e7a68015c54c4995c8fd7c12c28a839c5068b0919ad, df4c29cce2cf1a158ed0cefc860dc54f6fbb9bdafdc3bf5af60b506f78e69e4f, 6d215534002fe7627763f5dd971d529d2f2186431244108d1fd8b5e9e2c9a3b2, 24be73b64509dbad476b2873edf500554fed5885826b21e2f538993900d9a364,

Attack Name	TYPE	VALUE
RansomHub	SHA256	84099559a6d1dd1fec8a5c065da9f0747fab8ebb7368c197224fa33035eabe8d, 3c9f0907304f7af7a7b88f931b6733698e86492d02e98e440e87e3ffe2153dbc, c4d51f5a4dc95b0ac4b4f44a74d282d84898ddf56293a7dfddd5cb5eb90ec989, 262a4dff66ceb25d35d5ca8d8d148c1fee88ea2ee1187877a5a0c8d6a0dd24b5, de4d1f58fa8fa9eb156a37a8d9a3396d58e804f92e5eee25878a36a116f66362, Ab84aeee213b902fde9740c466cd53af4bae6d5ea81a2b84c4d534b08b2fa049
r77	SHA256	02a920314eabfff8ab4baebb18143cd81a97d27b2d3000cbca3bc0a38b01fa42, 072272ed6f66e69ee0ebcd98cdbe4ae7fa0ac0ce0c64ac9c55832d8343e74495, 13af06e041e8afecb9d415230d7619dc60be5c509f0a1a1305643e84044da53f, 267ede33a5df55f5bbe84ad1bc7bac166f60a7c981ca11ed1da45db783962a28, 2aa37e753ce1273f6ee4968bec7e2381b79a85ffbd1ee3da1fe9b4c1ea3ec4cd, 3300bfc229fd5e76fa2acc97fb45e4866226dde11bfcaccd8f5f54aec1f945fe, 48528810e3c4827e526919bf312030fd69cbee63256c4a45ee8e9382fc04df3d, 5edef7f39c4e95f2e575d9019825dbb42f12f6fc6d70e91de946313517a04d6a, 62263be578e786f6001a03dff5d793e2dc07167cc89b5abdb27de569dad96380, 634a4bdde5464a8fdca9d9c8dee4981344d23c6c128cc484e06dae4b7a8504e9, 7d60f137ef308c08065ea99a9ec6193a5bb81126430267e0e88c43ac2804c206, 7dae41ea7e76518b6c8733c6fe5d9442186e067ee02ce265899df15907f3272e, 877a2f157e0f8d0e13dc846db7883ccfb3cb65cc41b35dd93ad5b600af82c2fb, b45b9a81c47d422028df8c4e1c6633d362d5cc55b4b646764f33e62780910692, b91c76ec6f758683ee33fbe8e70396203c93a5aeb53be6b860e683a62c0585e0, c8dc159ba12067f50d604185203fa75e453150a87aa8575e17ae77741034481b, d6a9816b0df03fee5229e490ff3bfa2a016c0eeb9658b09fd6538a34e469579f, E97a4629d0932ecf65a8e3e587138b7ede3216894441c57ae3aacd6a21a97f44

Attack Name	TYPE	VALUE
StilachiRAT	SHA256	394743dd67eb018b02e069e915f64417bc1cd8b33e139b92240a8cf45ce10fcb
ANEL	SHA1	018944fc47ee2329b23b74da31b19e57373ff539
	IPv4	45[.]32[.]116[.]146, 208[.]85[.]18[.]4
AsyncRAT	TOR Address	vu4fleh3yd4ehpfpciinnwbnh4b77rdeypubhqr2dgfibjtvxpdxozid[.]onion, u4mrhg3y6jyfw2dmm2wnocz3g3etp2xc5thzx77uelk7mrk7qtjmc6qd[.]onion
	SHA256	1791d00fbe569489f48cf5e56b9a2a9b71d3c17096df4982668f51d512b820c5
ClearFake	SHA256	77ce187e20054b9a0e6ccf45942fc3873232e9c4b4e8861bb8db43f1ae7d48d1, 57f5ff194e45038b1bd4a10f7caf52c34470715b2344ccea1658a3f8c9dbceec, cede348dc4d9ff389b5adc284771cd7c6c992e9b8c4fa300b77c152c418d45a9, ae669a68c740edab53cce8e0ae6c7d7f29fe725bdb67693fc29eec6cb7a81c9f, fdab43ddf837ce4935864f7f903870a3d464f6236ee678d97d90c273795baf57, 7e6e3332507ce55cd93fc10899bbb2a10cc15c3f9f5d30c63cedb81864950228, e6205badc1105f9e081e79fb0cfe7149ec5e368fd19a82828507ab8870355716, b4d4aa20a71250f9f2ef3ebff78812de8365dc254dc75d3e75fb8aa5e31ea03c, e2d844d44d9dcc28e7c6a7ce701c57c71930975be535060c77789954c8efb348
Emmenhtal	SHA256	5014963128c4f8804d881967cc77e85252f4c9ef91dee9c9db5360b8ab7e1510, c072a21f1f55aba61c5f4a6d0015d4921ce1aeee72827aa300a8cfd8b4fbaead, 037aa969f2a8170b56541a85db7bc1a3d4fa4f290d8b8dc86f26ed070e953ce8, 19acd7918f928a2ebd75c4090acfd949fcfff99700770e654bc073307afac133, 466d600cf46bd0178406aac5669440a62e05af407df6e32b5f12297a60f7611e, aac6af9f1697771d0eca4c2ce2b4fef0e98cfc444ff9998554162b49c5722569, e8bd23f084848d1b77d55ecf325d90aa5b3c2ee67ba901fe4aa65c05fb70c6c0,

Attack Name	TYPE	VALUE
Emmenhtal	SHA256	a2b2c6ccfe8022689916d9285e0ba811d0f2b6a03108c2ff700d9bae5f6f3c80, 6621ddc660f21e7600e8b9f810a41212d0cc65a3751df048e36e1cf6540b8a96, 5d5894a9f5fa6f25cc076aeccbd1db45e50523f291f43550fd0c8be3bc11c6c3, 198b2b9f367f8fdac0d55fd7f3b2b690586bc68f97ffe17128f997579426ba5a, 3d55789d319dd3102996cc14c4ba61ddb6c2536b61dc461bb525ae13abb02e05, 0a26b3748010a5ee278a0b6954b3f769052766260ff2d717f5799f3c5b1febd5, b6e45a7ad3f9a1f32b9ed31e58b59d6993e23fa58983b829c5e3a1f5492f71ba, 21bcfcff9376297ee0011810f48beb7b7cdacba29d18d740a4acf25a445f6d5d, 448f1eafa2b65e0c3c26d1aacaa8a28057b878cf169d178cff8ff9a271b8dbef, b15459f4de3837c458bf71fa0a23010a72dedbbf202922284bd4c9eae364b68a, af904284be685f5e4e47e5629612d6b4b5afbf13499878001bdfc945d4c6a8dd, e455c87db7eff0ae358e096a9c93d6f9bae6a8273e634673cace810944407b02, 4f9ec5212d6eac6586ca4a32cd3ef4669c08b5b526f70940b05874939e5eb717, 66f95434038fec4bade6bf3947398d6bb6905fa3451cd105f641ec83c3d24bd9
Lumma	IPv4	195.123.226[.]91, 94[.]158[.]244[.]69, 185[.]99[.]133[.]246, 144[.]76[.]173[.]247, 195[.]123[.]226[.]167, 195[.]123[.]227[.]138, 82[.]117[.]255[.]80, 77[.]73[.]134[.]68, 217[.]12[.]206[.]230, 82[.]118[.]23[.]50, 45[.]9[.]74[.]78
	Domains	stagedchheiqwo[.]shop, evoliutwoqm[.]shop, millyscroqwp[.]shop, traineiwnqo[.]shop, condedqpwqm[.]shop,

Attack Name	TYPE	VALUE
Lumma	Domains	locatedblsoqp[.]shop, caffegclasiqwp[.]shop, stamppreewntnq[.]shop, cancedhoeysopzv[.]shop, parallelmercywksoffw[.]shop, notoriousdcellkw[.]shop, barebrilliancedkoso[.]shop, landdumpycolorwskfw[.]shop, liabiliytshareodlkv[.]shop, conferencefreckewl[.]shop, ohfantasyproclaiwlo[.]shop, flourhishdiscovrw[.]shop, secretiveonnicuw[.]shop, professinowpqqz[.]shop, gservice-node[.]io
	URLs	hxxp[:]//185[.]99[.]133[.]246/c2sock, hxxp[:]//195[.]123[.]226[.]91/c2sock, hxxp[:]//gstatic-node[.]io/c2sock, hxxp[:]//winhxxp[.]dll/c2sock, hxxp[:]//82[.]117[.]255[.]80/c2sock, hxxp[:]//aloowforest[.]xyz/c2sock, hxxp[:]//speedtestip[.]xyz/c2sock, hxxp[:]//stoppublick[.]xyz/c2sock, hxxp[:]//many-verses[.]xyz/c2sock, hxxp[:]//worldofpoetry[.]xyz/c2sock, hxxp[:]//crazypictures[.]xyz/c2sock, hxxp[:]//skicloud-my[.]xyz/c2sock, hxxp[:]//solopodvip-my[.]xyz/c2sock, hxxp[:]//clonecloud-my[.]xyz/c2sock, hxxp[:]//2flowers-my[.]xyz/c2sock, hxxp[:]//vipcloud-my[.]xyz/c2sock, hxxp[:]//agustfreeday-my[.]xyz/c2sock, hxxp[:]//gservice-node[.]io/c2shxxp[:]//195[.]123[.]227[.]138/c2sock, hxxp[:]//flowers-my[.]xyz/c2sock ock,
	SHA256	f6c9d98e75dce75eba90605da3f40089b6780adf804744519685244641be7b75, 1c7af5b8d0a12ddeba1f4d5ee756426da50c6e7c9e5696947874bd8c02575669, 6d108056b6c58e37227148939551df54a907598657fffc30ec409e8a79f44801, 46757e45afca3dd3f90bf6a225c9739d4875a8a5a8b6405fe9c48935e9451894,

Attack Name	TYPE	VALUE
Lumma	SHA256	c6e189e2226e357594ada121409340974429c8fb119fffdeaf8e511de868d911, c8804d07da4504d50a02f92e754d96f3aff37cd7297fe79e2fe6a23d81687590, ad26040171ad3cf68f4db6c3e72d177518008bf93467503c22d501267d1a1293, 1425c3c9b00d5fc21ae57da1a7fd1df3805d517f4e6470f4c290bd914b2be710, f43e8b43b3b7b1013fdefda62f9a25228ef0f4d3972ab661c41d8540d0095a06, 6cd1a9abfdbc95d7848fc8001e48261802560efaae002396218a8849514bcb63, 756604381d719d4fe57d3d0f7ee63695c9530b1ddd46f2861fd582483be5bcd7, acea7a8e76d813848155ac7e92c0dd0cba5fc03cb6a408b3f0dd597bc2bfb68b, 3465e531cd286ec9c75edc965e7e8884657eabe8692100a137cf726dedfcab17, 68f05abc3ccc9c5e3dfa8df461cb60a9324729442e49791fbc5839e144962847, 601345e4fd37fdb42ff4c6ab6dafd08e2412f3115dd02eb20df779c9e60f5d72, f24ecd129dcf980bb3d72f421f17424981a42934c68080b62c8c3d232d96fb47, a66fb090776da483f24cd9a11f98ba0c35229c2c7ffae94c04de6336691f371a, e2f98c2cd563d6849f43f8a5f85166691ab5d51e4c8f562cdbb05200c51b9cd8, 54477f87e432fbbcdd84b0a822c48d5405e879d3626f3cf37b049d5c175907d6, 2f97bf87efdd2353adb4eba111d208a59d096b6a0a33a03969044d9cb6cab92b, b2e2283b170cc6b96c927e39a52b06a93e94f5e820c302179d203368db54ec83, 2c9ddb4d501ab5ea6c85d3c23936843e689d4c26689caa7b07f940c76d442f07, 4cbef2761ec4bfedad02e89e06c686854c44d54d1a6d777a71836d2ae927a0fb, 337def67e434d226038b112792f0c7dbfb8faf218091c3951f253e7015b6dec8, dc0ec0af7398e1c71dddd1d08fe3f4143735ddb14bdbb9375cf323ea1c0a6c0f, 3e324926b14e2a9a9fb875f4fa35fdd24a5ef23d9f2acafcda1457fa50a58ca9,

Attack Name	TYPE	VALUE
Lumma	SHA256	c26c1aea0390a93ead8a6ae1732b5a82043a702dc8f26165b965421bc732898c, 3bb89cd70ed5ca7ef46aead3267bb4ebe34cea0a1c47bf88145b33594d8acf4a, ca1cf4688ed550e6cc66e4b94ea44f318bcf9eaa7e2934b66bd469c155a46b95, 3e239f29816d3dcb86bcf6e2dd2f526b94548b83c590cb20657838c81b166a34, e08b354293c3d06834c9ce98dd1e600ce54f1e654b5e6d038f0a69977dabfcd1, 9ed1a10724d0eef682e94be482c642c6f579ab18582b734774ec22fce2983a14, c2bf90879de30dabb28d9d1c8a35900729d19c751e47c1d7d510a03437a2c7f1, 3426aec404b419862da4500c4a9247f9f1c7599742db703c891bcfd9243f63c5, affd6f4ee52186f5d78f741370933cff89b844b3208dc6864fb315c629f4f921, 5e180d43941c22647f3c5208f00e1f32c8977671b5f1826996c7cff6790a3d49, c592b7a2c546d06be939eda1b77f29d36cb07c33b06b195627aa8acb555c4978, 0b4ad9ef5302cd68f4d944dc9687407f2b473464056e9a77d995222c255c5b1b, 5d05d4ce37e2e191dc3dda9bd89128037497e9daf55f4a0266fcfb5a014ca0c3, 522ab104084272913dd20cbc7e7871e742236bf241df49cd6265f978f68f6b40, 44a472744c8b51fa4bcccc671417e58cc23d8499afe07de7c598d2f131d18a10, cbb058cb06474788dd76943595e257b4ccb787832e64eb0e7390dc064f3b3edd, ae1c25c83c3afed2cd5b38359c7223b633c94aeb60ee56791aa7280e43ff25c9, 00249eafeb335b3cabdde5b3f3836e935b6bfca1a081aa444d53af85b9ce47f7, 6975cd30a118ebd3457e8f833ad305675c1a28b4eab373fd11cf826fc39a831f, fdc722383256195ef8d521fd1af4766004e587845b4e6c269b5e6e25243870ea, 234726abf310eddea749608e99a73c94f7c5ab69b8da6ea9f6d8956b1aff6054, 45d2434ae21664bf7b661cdddf75a7febe700f3e47427bbcd5e45a274b7d2ec9,

Attack Name	TYPE	VALUE
Lumma	SHA256	773fedf94f6477fd1616e7271eb5b4bca5a95f39e48b5d80d433d607035cc0f0, b8c95e977a6c52dcdfa02450b3ef6800f4b3e26d088bca95546381d1d62590c9, 80b97f3ab2987d7ec58ebb8c59e9b3454532421f2637a8620d1e7440a83ac887, 99fadadbb3c9f176961ef333b7909d82b932f8dcbde1394f5756503e808509b6, f94f4fc9852729490aec1fa67fc3550f8fa9414ea9b74da60a5813f3973ecda5, 257d1e121449b6d1df1b55827b698bc0ca4560d92e4d7283f3218178b70f85e3
Vidar	IPv4	95[.]216[.]180[.]153, 45[.]84[.]1[.]88, 103[.]125[.]190[.]248
	Domain	ip-api[.]com, tiny[.]cc, l3monrat[.]com
	URLs	hxxp[:]//ip-api[.]com/line/, hxxp[:]//ctrlgem[.]xyz/gate[.]php, hxxps[:]//steamcommunity[.]com/profiles/76561199786602107, hxxps[:]//t[.]me/lpnjoke, hxxps[:]//t[.]me/neoschats, hxxps[:]//steamcommunity[.]com/profiles/76561199644883218, hxxp[:]//ctrlgem[.]xyz/request, hxxp[:]//103[.]125[.]190[.]248/i1//7[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//5[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//4[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//3[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//2[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//1[.]jpg, hxxp[:]//103[.]125[.]190[.]248/i1//6[.]jpg, hxxps[:]//steamcommunity[.]com/profiles/76561199809363512, hxxps[:]//t[.]me/k04ael, hxxps[:]//steamcommunity[.]com/profiles/76561199802540894, hxxps[:]//t[.]me/fu4chmo, hxxp[:]//tiny[.]cc/93p3001/7[.]jpg, hxxp[:]//tiny[.]cc/93p3001/5[.]jpg

Attack Name	TYPE	VALUE
Vidar	SHA256	536ba33ec4d2ed30d81221f34f372abd9e643fe566d4c6194182d938e3a9f84a, b9b2564b8f1b3cc417fea37afc8731da4faca6ef0473169c6accf856384f63c3, ff50944a3292f3cd42ec1cf1fe2768a5bbecade3f7778a05706878746398ee0b, 2d320815277c9cca9e13eec61aed3db4de40e57aa338d00355bb71c3afa333c4, 930b9d517b41463be78b6472d7bae7918db1626245658059e7f1d380eab99ea0, fc692e62d466b316c3d0174fdbe6fa6d778e47e29b356a39d9a8f3df1e4a571d, cdf481b6922c8c27c51bbcdec94f6ec41b1bfe9771beff223068ad02a14585d4, f24ecd129dcf980bb3d72f421f17424981a42934c68080b62c8c3d232d96fb47, 09c69b0ce8731e58583a76faf1785568db9de0cad9aff40c4316a7d6046c2a65, 9ed1a10724d0eef682e94be482c642c6f579ab18582b734774ec22fce2983a14, fcb41b6beaad2db4ac83aec31f4382cf885d3e00ce49bd5e38e3b4b03909545c, 5e180d43941c22647f3c5208f00e1f32c8977671b5f1826996c7cff6790a3d49, 92e3340d62d04a24e68d37731b0512ffd954c749d7df2801f099010a39241db1, 81f4008e3f54f50688bbfa5248087c8d1e11bf05a1744a1f8a76ea20b5c35312, 2b8ae461d311aa9680a156040dd008c20ca24792e0c4d7a1d54cd68d0f60898c, ebc05061c233aaffdc44bb285e96458788e5640caa91797fa7e524d3dbf8d14c
ShadowPad	SHA1	d61a4387466a0c999981086c2c994f2a80193ce3, 918ddd842787d64b244d353bfc0e14cc037d2d97
	IPv4	213[.]59[.]118[.]124
	SHA256	9447b75af497e5a7f99f1ded1c1d87c53b5b59fce224a325932ad55eef9e0e4a
SodaMaster	SHA256	76d6b638a9a22dce8edab0145fcdb09adb986fb98222fab0127df60c2fed8112
	SHA1	3630f62771360540b66701abc8f6c868087a6918, 3c08c694c222e7346bd8633461c5d19eae18b661, 5401e3ef903afe981cfc2840d5f0ef2f1d83b0bf, a4f68d0f1c72c3ac9d70919c17dc52692c43599e, d8b631c551845f892ebb5e7d09991f6c9d4facad
	IPv4	162[.]33[.]178[.]23,

Attack Name	TYPE	VALUE
SodaMaster	IPv4	78[.]141[.]202[.]70, 192[.]46[.]223[.]211, 168[.]100[.]10[.]136
VenomRAT	SHA256	075f991f42c1509d545a8e164875e6464c7394dbc1e8550ba8cd50d6b5b5f2ea
	IPv4:PORT	81[.]19[.]131[.]153:50037, 217[.]64[.]148[.]159:50037
	Domain	ggggg[.]gettt:50037
Betruger	SHA256	ae7c31d4547dd293ba3fd3982b715c65d731ee07a9c1cc402234d8705c01dfca, b058c128c801e2ee03874e183239ff369c599f3a2324905ff73f99d16d3b1a16,
China Chopper	SHA1	23c4049121a9649682b3b901eaac0cc52c308756, 9022f78087e1679035e09160d59d679dc3ac345d, be52275b0c2086735dac478dc4f09fd16031669a, c879a8eb6630b0cd7537b068f4e9af2c9ca08a62, 25a593b9517d6c325598eab46833003c40f9491a, a9bbea73504139ce91a0ec20fef303c68a131cd4, 334a88e288ae18c6e3fd7fb2d1ad9548497d52ce, 4aeeae023766153a91b83d02b1b24da20c0dd135, 3cac6ff7cddcb8f82409c79c85d976300fc60861, 55eeaa904bc6518a2715cc77648e6c5187416a46, ff7b2c3938306261881c42e78d0df51d9bcdd574, 089439168d3c75b4da94ab801f1c46ad6b9e1fdc, a5c36b8022751cfeb4a88a21153847df3870c7c0, ad3dbec2b621807fa9a2f1b2f575d7077e494626, 4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb
INMemory	SHA1	f31920d636224356e8c7a182c2b9b37e42a09181, 9dc3d272652851428f5cc44f2fd9458bff1d6a78, 4dd22a08a5b103e1f2238aed7f7ce66c5a542533, 02065bbdb3209e0522db3225600b8e79f8a10293, 81622512757f897206a84b29ee866fb933fa3d48, 151dc47b213aaec3751ffd1427737c65757ab410, 492cbe143f795888d8e5006ac595f65f4565ed6e
VanHelsing	Bitcoin Wallet	bc1q0cuvj9eglxk43v9mqmyjzzh6m8qsvsanedwrru
	TOX Address	FEE914521FB507AB978107ACE3B69B4CA41DA89859408BAE23E1512E8C2E614A26C5FFD482A3
	TOR Address	vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd[.]onion, vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid[.]onion, vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad[.]onion,

Attack Name	TYPE	VALUE
VanHelsing	TOR Address	vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad[.]onion, vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd[.]onion, vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad[.]onion, vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd[.]onion
	SHA256	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17, 99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98
	SHA1	4211cec2f905b9c94674a326581e4a5ae0599df9, 79106dd259ba5343202c2f669a0a61b10adfadff, e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948
	MD5	3e063dc0de937df5841cb9c2ff3e4651, 5c254d25751269892b6f02d6c6384aef, cd9563b4cbc415b3920633b93c0d351b
EncryptHub	Domains	encrypthub[.]net encrypthub[.]org raw[.]githubusercontent[.]com
Rhadamanthys	SHA256	cbb84155467087c4da2ec411463e4af379582bb742ce7009156756482868859c, 015f0fdf24a19b98447fab5fa16abf929c1cf9be33e9455ce788909dd5a8dbfe, b1fa0ded2f0cc42a70b7a0c051f772cd6db76b15d50ec119307027e670998728, f381a3877028f29ec7865b505b5c85ce77d4947d387d3f30071159fa991f009a, b4f66a5e2876e04db93aae029049a07efed2d6dca05c89c393fe5aba03b949a7, bad43a1c8ba1dacf3daf82bc30a0673f9bc2675ea6cdedd34624ffc933b959f4, fcfb94820cb2abbe80bdb491c98ede8e6cfa294fa8faf9bea09a9b9ceae35bf3, d639cd267b05b4cd420e4547dd7aa4d99fff2d070598de044c7cf0d1b99cd264, 5f6dbe487af0fe7d1cf9beca7e31fcd804d6bdfe9a80308d7aeb3ed9abd9bba3, ab58281273e7299f86cfadc1c8235789379543339035c5b4d80becd785bad552,
Stealc	SHA256	725df91a9db2e077203d78b8bef95b8cf093e7d0ee2e7a4f55a30fe200c3bf8f

Attack Name	TYPE	VALUE
MSC EvilTwin	SHA256	5588d1c5901d61bb09cd2fc86d523e2ccbc35a0565fd63c73b62757ac2ee51f5, b1b3d27deb35dd8c8fed75e878adae3f262475c8e8951d59e5df091562c2779b, 7f8bd2d63bb95d61fcbdb22827c3a3e46655f556da769d3880c62865e6fde820, 43eab8488dce80c1086aafdf4594b1a438347e32275abeaa8b2bb14475fb3f98, 1b3309c7a4c3940eff1e1ab1905641b23ea743c4f11d82107ce36fa1ec2299e9, 2aeb9aeca5739ea1cb5a30d284d65e36fe18f47db9e5e504063d982b9c3bc3e9, 9b830c2979cbce45573aa21d765adda76f52db254155ae49648ef5050ceaf774, 4e6f35ab5eb9242335bee01d6df9b50f665043f9930a630df7e170b904f52a24, d76c25e2761210783055b43349370253d794e94ee913a2be7596b9554eacf107, 5357279bad530c3af89713aaf6befe19a22e438f22952aed46097590130551fa, 413dea8ea8cb09cd3ac49531a8e0a13f767c09f78fb77856f4668377532a64ef, 0943b0f328282504c2661cd56e4bd83e3b3e5a4cce89e2e5523f83a2d535a07e, f5c97f23543e904944120ef738f300049eae85c3b0bf8b86b346572f7bc6dec1, 9e9ca325f44eeff4087bb67052536ba565da18e70e5b29c79ed77c14c5548131, 94ee2227696da3049ff67592834b4b6f98186f91e6d1cd1eeec44f24b9df754b, cedf4589428ae05d3d2dca1d1bd7fa28f6cafe54a077a6090f873053e04fd5ce, bb563180196989dcee91417aa56d6f1bfc9320b2427536c200dffcd784774906, 9d2aaa8672d583af4c03c23127d6cac509799a49ff9293ed63628d5b710b7528, 3761060c509b9444bdd3d0e65d7f68e39ff5c52fa87fdc59db02c1553e21e403, 47e4142fa6ab10a2d7dc0423d41f9bdbb3ced0f4fae5c58b673386d11dd8c973, 6b99530953010dd8061a3a328c04c30653bba26439dd30a752262582b0d02933, 045a1cbcc99c53c092bb61d43b89a6f7308fd01d9ceaeb9a72bbf81669dcbef8,

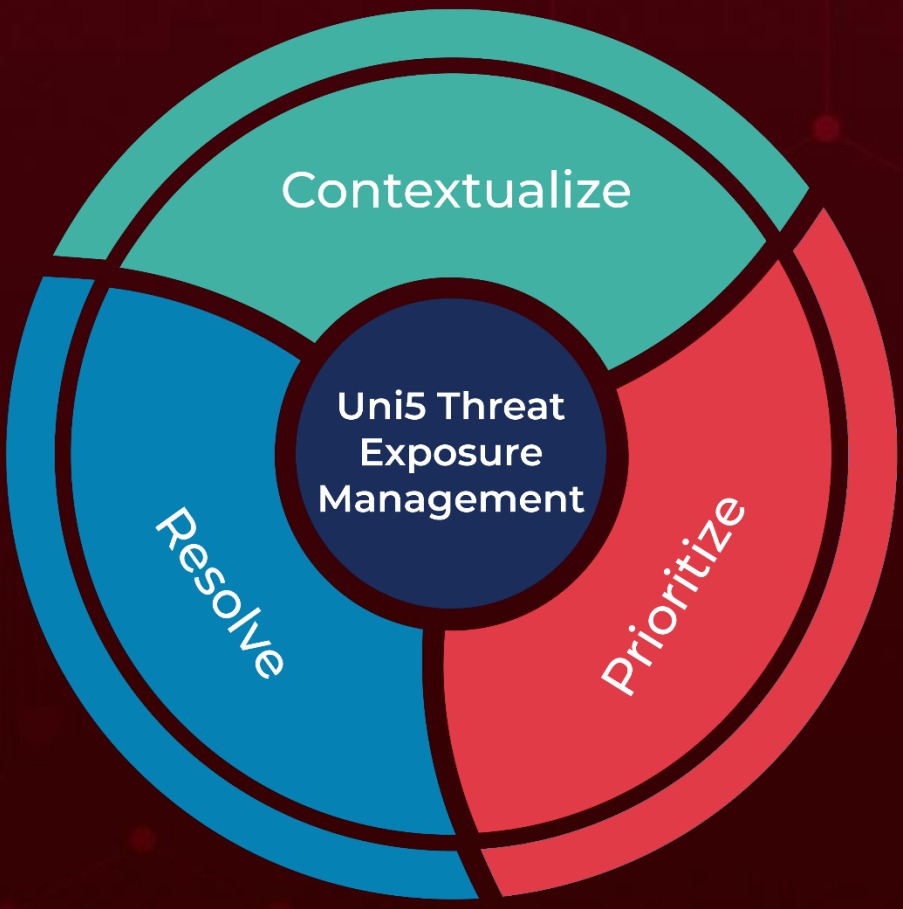
Attack Name	TYPE	VALUE
MSC EvilTwin	SHA256	cd301bdc07518027567a5ed242ae2075f9f0bdf73315e99d4d949280f151fefe, 405d1dcdbba56bce99a308734c39ac8ca62ffb55dbd69565293a79b468e4dad1, b3ed3f2bc5334e54ca8d6020d37da0764f123fa5717638229422bd95a028097b, ba195a227fb76e8820d6db36cd00c89095b88faf01471fcdd9c0c7de61a63a5d, af4d26b987093be6b442e655ffdafa8e1542e80f6a47a6895aa523f2f180025c, cfafc9b2d6cbc65769074bab296c5fbacc676d298f7391a3ff787307eb1cbce0, 86e4115111e88bbaf09fe73cfc8255a4aac64f7ffed4a3229bbc8d626566f0c8, cd301bdc07518027567a5ed242ae2075f9f0bdf73315e99d4d949280f151fefe, 691087ec9b50022d3e23695c0b41e2927cb4c4825a1f5fd7e2f21ae3465e8973, e31ce5803bb68222eeac117614ddb92ed3c137bcf129f873d44960ab9d8bab33

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

April 2, 2025 . 10:30 AM

More at www.hivepro.com