Date of Publication
March 3, 2026

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

FEBRUARY 2026

Table Of Contents

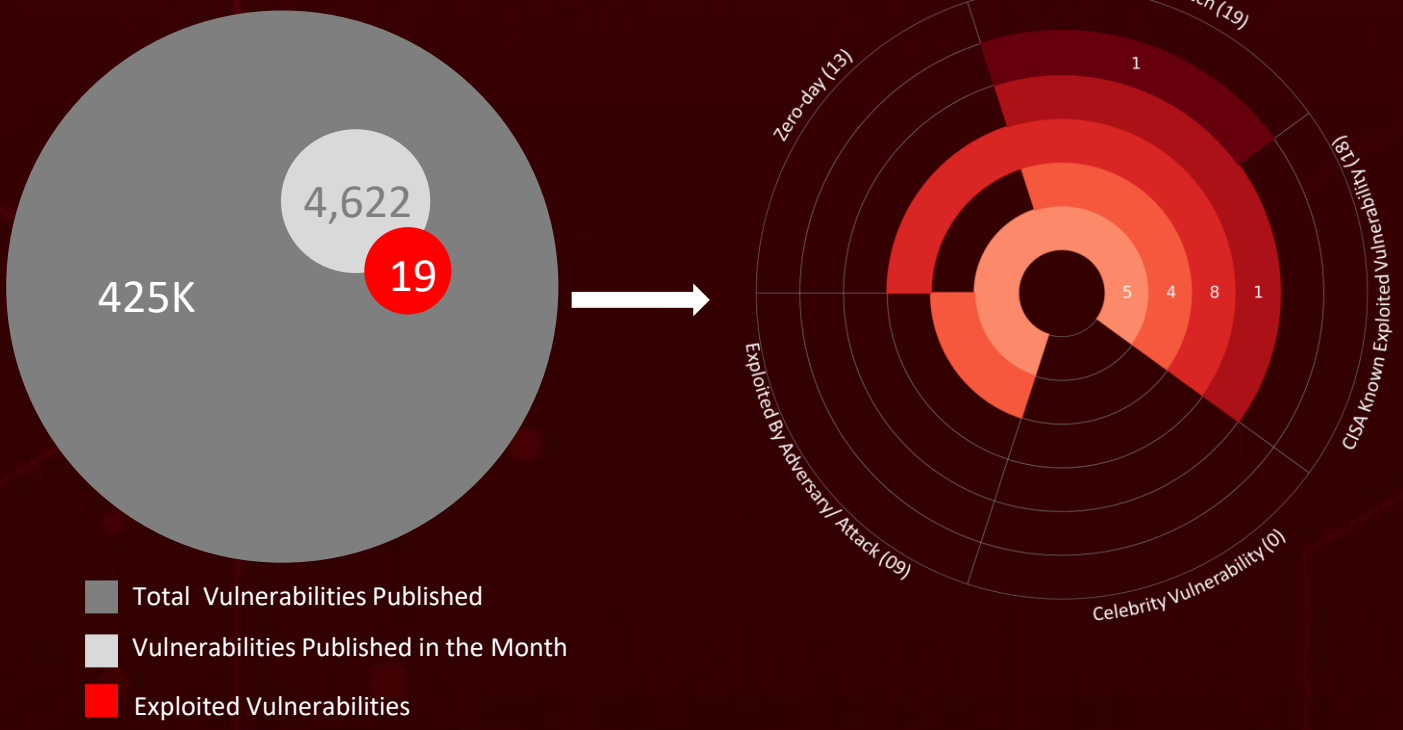
Summary

February reshaped the cybersecurity landscape with active exploitation of **13** zero-days. A rising cyber-espionage threat is gaining attention: **APT28's Operation Neusploit**. This campaign is intensifying attacks across Central and Eastern Europe, using carefully crafted phishing documents that exploit a Microsoft Office vulnerability (**CVE-2026-21509**) to silently infiltrate targeted systems.

Meanwhile, **Amaranth-Dragon**, a China-linked APT group tied to the APT-41 ecosystem, is carrying out highly targeted espionage against **Southeast Asia's government and law** enforcement sectors. By exploiting the **CVE-2025-8088** vulnerability in WinRAR, they can execute arbitrary code and gain unauthorized access.

In response, Apple has urgently patched **CVE-2026-20700**, a critical zero-day memory corruption flaw in its Dynamic Link Editor (dyld) that affects all Apple platforms. On another front, the **UNC6201** group has been exploiting **CVE-2026-22769**, a zero-day in Dell's RecoverPoint for Virtual Machines, since mid-2024, allowing unauthorized root-level access to trusted infrastructure appliances.

Finally, **MuddyWater**, an Iranian state-aligned APT group tied to Ir**an's Ministry of Intelligence and Security (MOIS)**, has launched **Operation Olalampo**. This campaign targets organizations and individuals across the **MENA region**, underscoring the growing threat landscape. With these increasing risks, strengthening defensive measures is more critical than ever in today's digital landscape.



Insights

In February 2026, a geopolitical cybersecurity landscape unfolds, revealing **Thailand, India, Indonesia, Vietnam,** and **Monaco** as the top-targeted countries

Highlighted in **February 2026** is a cyber battleground encompassing the **Technology, Government, Financial, Education,** and **Telecommunications** sectors, designating them as the top industries

22,000 Downloads and Counting: Malicious VS Code Updates Embed **GlassWorm** Malware

CVE-2026-23760 and CVE-2026-24423: SmarterMail Vulnerabilities Are Fueling Ransomware Campaigns

Lotus Blossom Targets Notepad++ to Spread Malware: Chrysalis Backdoor and More

Deepfake Zoom, Telegram Hacks: UNC1069 Uses Cutting-Edge Tactics to Steal from the **FinTech** Sector

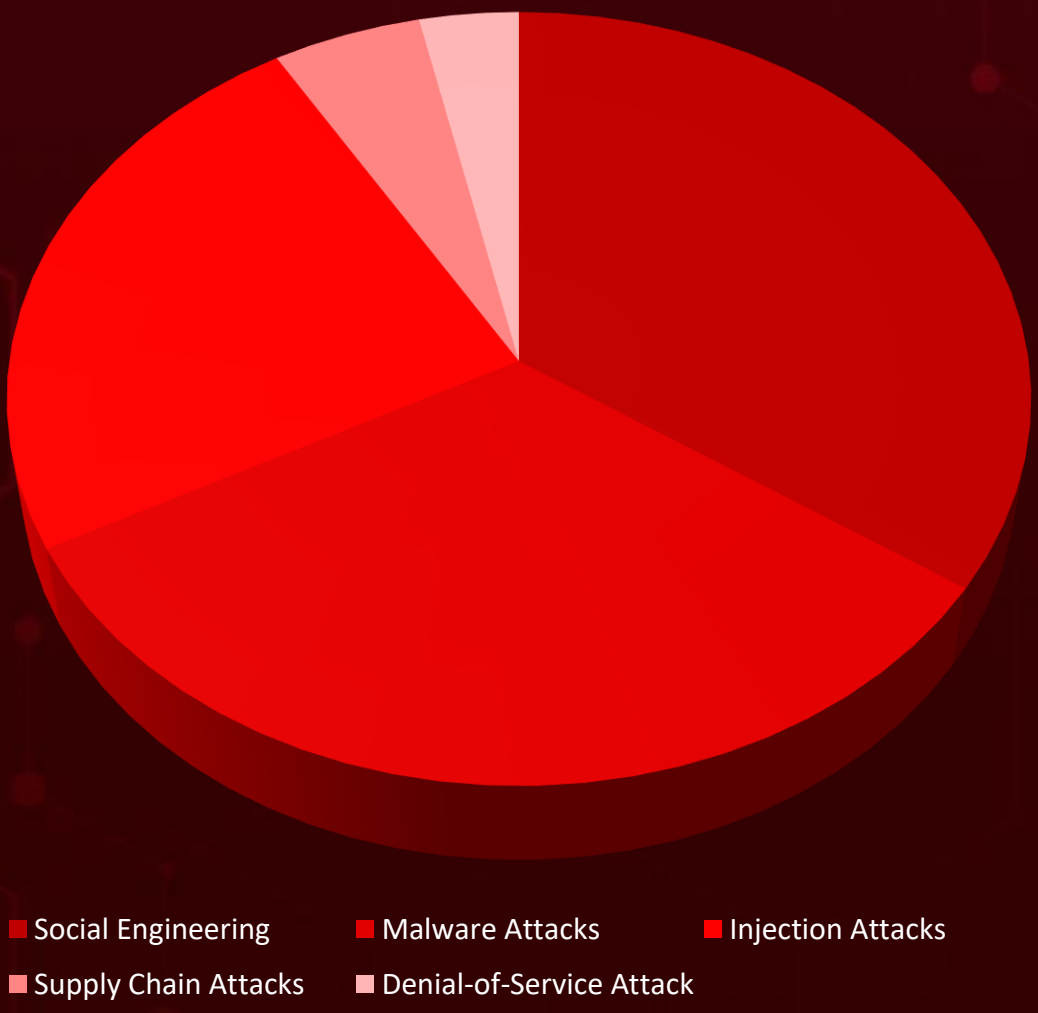
Mercenary Akula: Russia-Aligned Cyber Group Targets **European Financial Institution** with Spear-Phishing Attack

SANDWORM_MODE: A Self-Propagating Worm Targeting Developer Repositories and AI Toolchains

Zero Authentication Required: CVE-2026-20127 Flaw Lets Hackers Take Over Cisco SD-WAN

Cuckoo Stealer Hits macOS: Typosquatted Homebrew Pages Lure Developers into Infostealer Trap

Threat Landscape



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-25253	OpenClaw Remote Code Execution Vulnerability	OpenClaw Clawdbot/Moltbot	✗	✗	✓
CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office, Microsoft 365 Apps for Enterprise	✓	✓	✓
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	WinRAR	✓	✓	✓
CVE-2025-8110	Gogs Path Traversal Vulnerability	Gogs	✓	✓	✓
CVE-2026-24423	SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability	SmarterTools SmarterMail	✗	✓	✓
CVE-2026-23760	SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability	SmarterTools SmarterMail	✗	✓	✓
CVE-2019-11580	Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability	Atlassian Crowd and Crowd Data Center	✗	✓	✓
CVE-2026-21510	Windows Shell Security Feature Bypass Vulnerability	Windows Shell	✓	✓	✓
CVE-2026-21513	MSHTML Framework Security Feature Bypass Vulnerability	MSHTML Framework	✓	✓	✓
CVE-2026-21514	Microsoft Word Security Feature Bypass Vulnerability	Microsoft Office Word	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2026-21519	Desktop Window Manager Elevation of Privilege Vulnerability	Desktop Window Manager	✓	✓	✓
CVE-2026-21525	Windows Remote Access Connection Manager Denial of Service Vulnerability	Windows Remote Access Connection Manager	✓	✓	✓
CVE-2026-21533	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	✓	✓	✓
CVE-2026-20700	Apple Multiple Buffer Overflow Vulnerability	Apple iOS, Apple iPadOS, Apple macOS Tahoe, Apple tvOS, Apple watchOS, Apple visionOS	✓	✓	✓
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support, BeyondTrust Privileged Remote Access	✗	✓	✓
CVE-2026-2441	Google Chromium CSS Use-After-Free Vulnerability	Google Chrome	✓	✓	✓
CVE-2026-22769	Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability	Dell RecoverPoint for Virtual Machines	✓	✓	✓
CVE-2026-20127	Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Controller & SD-WAN Manager	✓	✓	✓
CVE-2022-20775	Cisco SD-WAN Path Traversal Vulnerability	Cisco SD-WAN Software	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BadIIS	Backdoor	-	Microsoft Windows Server, Linux	-	Social Engineering
GlassWorm	Loader	-	macOS	-	Supply Chain Compromise
Chrysalis	Backdoor	-	Notepad++	-	Supply Chain Compromise
MiniDoor	Spyware	-	-	-	Phishing
PixyNetLoader	Loader	-	-	-	Phishing
AsyncRAT	RAT	-	-	-	Social Engineering
Amaranth Loader	Loader	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting Vulnerability
TGAmaranth RAT	RAT	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting Vulnerability
Crimson RAT	RAT	-	-	-	Social Engineering
GymRAT	RAT	-	-	-	Social Engineering
Supershell	Framework	CVE-2025-8110	Gogs	✓	Exploiting Vulnerability
Warlock	Ransomware	CVE-2026-23760	SmarterTools SmarterMail	✓	Exploiting Vulnerability
ShadowGuard	Rootkit	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability
Diaoyu	Loader	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability
Vshell	Framework	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Havoc	Framework	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability
Sliver	Framework	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability
SparkRat	RAT	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	✓	Exploiting Vulnerability
WAVESHAPER	Backdoor	-	macOS	-	ClickFix
SUGARLOADER	Downloader	-	macOS	-	Deployed via HYPERCALL (ClickFix chain)
SILENCELIFT	Backdoor	-	macOS	-	Deployed via HYPERCALL (ClickFix chain)
HYPERCALL	Downloader	-	macOS	-	Deployed via HYPERCALL (ClickFix chain)
DEEPBREATH	Data Miner	-	macOS, Windows	-	Deployed via HYPERCALL (ClickFix chain)
CHROMEPUSH	Infostealer	-	macOS, Windows	-	Deployed via SUGARLOADER
Matanbuchus 3.0	MaaS	-	Windows	-	ClickFix, Social engineering
AstarionRAT	RAT	-	Windows	-	ClickFix
OysterLoader	Loader	-	Windows	-	Fake software websites
BRICKSTORM	Backdoor	CVE-2026-22769	Dell RecoverPoint for Virtual Machines	✓	Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
GRIMBOLT	Backdoor	CVE-2026-22769	Dell RecoverPoint for Virtual Machines	✓	Exploiting Vulnerability
SLAYSTYLE	Web Shell	CVE-2026-22769	Dell RecoverPoint for Virtual Machines	✓	Exploiting Vulnerability
Cuckoo Stealer	Stealer	-	macOS	-	Phishing
MIMICRAT	RAT	-	Windows	-	ClickFix
Lua loader	Loader	-	Windows	-	-
GhostFetch	Downloader	-	Windows	-	Phishing
HTTP_VIP	Downloader	-	Windows	-	Phishing
CHAR	Backdoor	-	Windows	-	Phishing
GhostBackDoor	Backdoor	-	Windows	-	Dropped by GhostFetch
SANDWORM_MODE	Worm	-	macOS, Linux, Windows	-	Typosquatted npm packages

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UAT-8099	Information theft	-	-	BadIIS	Microsoft Internet Information Services (IIS)
Lotus Blossom	Information theft and espionage	China	-	Chrysalis Backdoor	Notepad++
APT28	Information theft and espionage	Russia	CVE-2026-21509	MiniDoor, PixyNetLoader	Microsoft Office
Amaranth-Dragon	Information theft and espionage	China	CVE-2025-8088	Amaranth Loader, TGAmaranth RAT	RARLAB WinRAR
Transparent Tribe	Information theft and espionage	Pakistan	-	Crimson RAT, GymRAT	-
Storm-2603	Financial Gain	China	CVE-2026-23760	-	SmarterTools SmarterMail
TGR-STA-1030	Espionage	Asia	CVE-2019-11580	ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat	Atlassian Crowd and Crowd Data Center
UNC1069	Financial Gain	North Korea	-	WAVESHAPER, SUGARLOADER, SILENCELIFT, HYPERCALL, DEEPBREATH, CHROMEPUSH	macOS, Windows, Telegram, Chromium-Based Browsers (Google Chrome, Brave, Microsoft Edge), Zoom

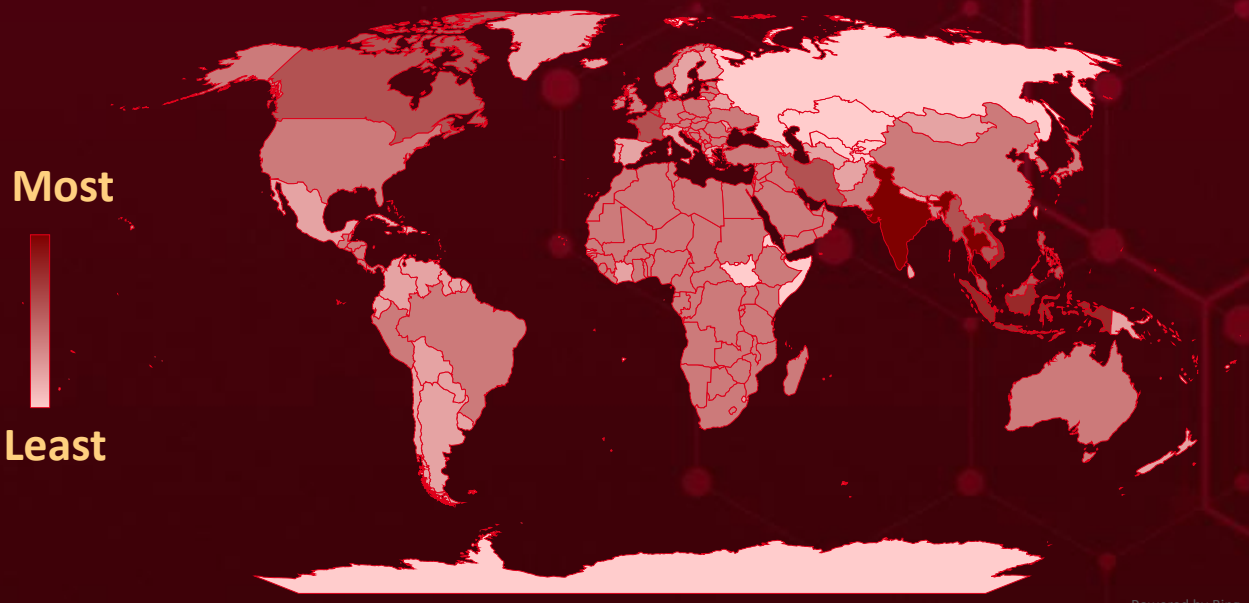
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNC6201	Information theft and espionage	China	CVE-2026-22769	BRICKSTORM, GRIMBOLT, SLAYSTYLE	Dell RecoverPoint for Virtual Machines
MuddyWater	Information theft and espionage	Iran	-	GhostFetch, HTTP_VIP, CHAR, GhostBackDoor	Windows
Mercenary Akula	Information theft, Espionage and Financial gain	Russia	-	-	-
UAT-8616	Information theft, Espionage and Financial gain	-	CVE-2026-20127 CVE-2022-20775	-	Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Manager

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Open-source AI-agent	OpenClaw Clawdbot/Moltbot (Before 2026.1.29)
Microsoft	Productivity Software	Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise
	Operating System Shell	Operating System Shell
	Web Framework	MSHTML Framework
	Window Management Software	Desktop Window Manager
	Remote Desktop Client	Windows Remote Access Connection Manager
	Operating Systems	Apple iOS (Before26.3), Apple iPadOS (Before 26.3), Apple macOS Tahoe (Before 26.3), Apple tvOS (Before 26.3), Apple watchOS (Before 26.3), Apple visionOS (Before 26.3)
WinRAR	Archiver Software	WinRAR Versions up to and including 7.12
Gogs	Version Control System	Gogs (Prior to 0.13.4, all versions through 0.13.3)
SmarterTools	Email Server Software	SmarterTools SmarterMail (Before Build 9511)

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
ATLASSIAN	Identity and Access Management Software	Atlassian Crowd and Crowd Data Center
BeyondTrust	Remote Support Software	BeyondTrust Remote Support: Before 25.3.2, BeyondTrust Privileged Remote Access: Before 25.1.1
	Web Browser	Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)
DELL	Data Protection Software	Dell RecoverPoint for Virtual Machines (RP4VMs) versions before 6.0.3.1 HF1
CISCO	Network Management Software	Cisco Catalyst SD-WAN Controller & SD-WAN Manager (Before 20.9.8.2, 20.12.6.1, 20.12.5.3, 20.12.6.1, 20.15.4.2, 20.15.4.2, 20.15.4.2, 20.18.2.1, 20.18.2.1)

Targeted Countries



Color	Countries
	Thailand
	India
	Indonesia
	Vietnam
	Monaco
	Singapore
	Netherlands
	Belgium
	France
	Cambodia
	Myanmar
	Iran
	Philippines
	Timor-Leste
	Canada
	Luxembourg
	Malaysia
	Israel
	Laos
	Niger
	Tunisia
	Senegal

Color	Countries
	Cameroon
	Benin
	Algeria
	Peru
	Cape Verde
	South Korea
	Central African Republic
	Albania
	Chad
	Bosnia and Herzegovina
	China
	Oman
	Comoros
	Republic of Ireland
	Congo-Brazzaville
	Brunei
	Costa Rica
	Tanzania
	Croatia

Color	Countries
	United Arab Emirates
	Cyprus
	Mauritania
	Czech Republic
	Morocco
	Democratic Republic of Congo
	Botswana
	Djibouti
	North Macedonia
	Egypt
	Palestine
	El Salvador
	Poland
	Equatorial Guinea
	Rwanda
	Estonia
	Seychelles
	Ethiopia
	Slovenia
	Angola

Color	Countries
	Switzerland
	Gabon
	Burkina Faso
	Georgia
	Uganda
	Germany
	United States
	Ghana
	Mali
	Guatemala
	Mauritius
	Guinea
	Montenegro
	Guinea-Bissau
	Mozambique
	Honduras
	Namibia
	Hong Kong
	Nicaragua
	Hungary
	Nigeria

Color	Countries
	Australia
	Norway
	Austria
	Pakistan
	Bahrain
	Panama
	Iraq
	Brazil
	Bangladesh
	Qatar
	Japan
	Romania
	Jordan
	Saudi Arabia
	Kenya
	Serbia
	Kosovo
	Sierra Leone
	Kuwait
	Slovakia
	Yemen
	South Africa

Targeted Industries

Most

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1204** User Execution
T1204.002 Malicious File	**T1566** Phishing	**T1036** Masquerading	**T1041** Exfiltration Over C2 Channel	**T1190** Exploit Public-Facing Application
T1547 Boot or Logon Autostart Execution	**T1573** Encrypted Channel	**T1068** Exploitation for Privilege Escalation	**T1218** System Binary Proxy Execution	**T1059.001** PowerShell
T1005 Data from Local System	**T1082** System Information Discovery	**T1053** Scheduled Task/Job	**T1102** Web Service	**T1140** Deobfuscate/ Decode Files or Information
T1083 File and Directory Discovery	**T1027.013** Encrypted/Encoded File	**T1588** Obtain Capabilities	**T1598.002** Spearphishing Attachment	**T1588.006** Vulnerabilities

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
BadIIS	SHA256	1ab98783a02ad9f127e776c435ef4e24a18ab93c4b4ee5ede722817d4b20771a, 1ece4d8603f5e28a7b0f6a8c83963a57cf23e5d2fadfc138419c3a051a75c93a, 2cc87bd2ae25a5119cb950618850eddeb578954fa780b125c1f51d234fb405e3, 4bc189af91779582a1d29cfe187aa233e7ba50d223261fb9fbe31df5b06dff96, 6be5c8882bc02cf4e86d2ab9d20aa3446b71dd12c73f9c6bf0faf9412d7d23ba, 9a2fd34e22c5f3d3d5fb96e3cd514dad7b03ed7bf53a87e7d8d9b73987d02ece, 11ea6aa2b31677f8a36627d4af709e70cff4a033b0975f63c19b28945e6226b7, 29ffb1d28f98582e81e78e6b2d5502da50c8ebdee0d40005a86b0dadece2923b, 56be91643dd8b86f347cc8d743c568f2d0169781ba999a2f708e503b59ecff76, 70d6bc89451e36889c045f30de22bc02e032788c8938baa0d5802e8f747c3e79, 91e1f4fc92f104ec8b29bb56df87f8e7d8b518c63997e2ea162d3f1cac3fcac1, 416ef6da8a27a99cbce6517d31857c8b8b55f02e9c8118510dc33814fb6f57be, 660ccb6dcfad97bfaddc667c61b1904e99a06eab981d44119092624d42912d68, 9458a75c1e24add9a48e0425e514a5f0cb46a826bff30ea7ea34e69099345f29, 265336511db98a4c40476455e2ae93aaf926abecd8f9b9d741f8d253abb80357, a781581baf6e1e335f22c9ffbb2656a2d9c8e51f463e3a48068210425df1c205, ab03a7caed279fc6411ec19386faff3b65be34c91c3f0550eaef84a663720d0d, bcc393c1686a0f5d493041e98dcafe0098d952d5e93eb4d2ebdb63c0efd2de33, c7a22f5c55ac1373a5964a6598da2a9afd8a61b9d729b9bf52a93c967a7f0eda, cdf454173bac13266e0f7db5de386439f197e2c480e1cc303dd7e806484645da,

Attack Name	TYPE	VALUE
BadIIS	SHA256	e84a16c8e25a4e40926cbb4cc210a09830298b6f99d532035f5136d05ffc008c, e448557d26cf2917efded8e30c67db8094ce1f6db78801742988ea21f3429d7c, 5d320b60d2f40c200e81eaeb67a86a04782bff84582c73e726255dba2dcb821e, 99f2c4773560eb515cfcb0ad45cf8e47c46580ab19494463160f885e048ce830, 565502d2454e4b65d3bd810fccf4b429264562fefa5cfff24c905b76b3b860a6, a34ea8fb565ac6f57eefc987c61159c1e6f1af6a8717ffb42f4b745db3bf9e31, 187e1417fd9d4f4a44e4f7b7172aef056e9d0ab5d7a7addf61c2cfa893f74fd1, 6b60b6df8a1a95f51ffe57255c05d26eb9e113857efac3b29d6ef080b8d414f3, 672ffdf1e9d4848015d29a68111266ef55fc6702dfe7b2053ce677882648dd5d, ebeef831c52b7e930a6456caedf7849814b8d4def2bc0e70a0e7a357621ef6bc, 230b84398e873938bbcc7e4a1a358bde4345385d58eb45c1726cee22028026e9, 48ec6530470b295db455bf2c72dc4fbd18672725f45821304f966d436b428865, 33d3ccf82279d94a8e8e772a0c4963d65a1f3576dbd6ed7b4ab8a0ee4869f97f, d8c0ef6dbf7d4572f92d3a492f32061ab8f3dd46beb9ff5a0bf9bf550935458c
Amaranth Loader	SHA1	00351add8e0bca838e8dac40875b8ad5195805bd, 481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2, 718c5846d3b903e3e9e2df9281f5e25b371465f2, 9afadca9b2dad54004bd376dbee7e98c38dbdf50, b4dc300031edf5dd4968028146b0d608bdd975c5, c54a68d6bcc6d04ff08ad9619706e54923a20248, cd949663598c49141a98b438cf408113602e5c19, ddea99cb2db5e95552dccc8804125f19b30af536
	SHA256	d7711333c34a27aed5d38755f30d14591c147680e2b05eaa0484c958ddaae3b6
TGAmaranth RAT	SHA1	803fb65a58808fd3752f9f76b5c75ca914196305
	SHA256	a3805b24b66646c0cf7ca9abad502fe15b33b53e56a04489cfb64a238616a7bf
Crimson RAT	MD5	5b4a48815446cd40d8e141cbf8582296
	SHA256	1092761df305e910f806834fb774dfb09dc64a4d399d578a0d1bf1dd5daf0f98
	IPv4	93[.]127[.]133[.]9
	Domain	Sharmaxme11[.]org

Attack Name	TYPE	VALUE
ShadowGuard	SHA256	7808B1E01EA790548B472026AC783C73A033BB90BBE548BF3006ABFBCB48C52D
Diaoyu	SHA256	23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe, 66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0
Havoc	SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8, 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c, 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328, b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c
Sliver	MD5	8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1
	SHA1	953bd0859c86e0a3a3da52fe392a7d579a9f937b, 538cb25bfae6501d8c3c7053a293e8ca85a8dba4
	SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd83907411415e5428f7a9
SparkRat	SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697
Matanbuchus 3.0	URL	hxxps[:]//marle[.]io/check/updprofile[.]aspx
	SHA256	6ffae128e0dbf14c00e35d9ca17c9d6c81743d1fc5f8dd4272a03c66ecc1ad1f, ea378496135318ac5ad667a032fa4a9686add9d27fe4a7c549c937611b5099e5
AstarionRAT	Domain	www[.]ndibstersoft[.]com
	SHA256	eecc83add16f3d513a9701e9a646b1885014229ac6f86addd6b10afb64d1d2af
OysterLoader	URLs	hxxps[:]//grandideapay[.]com/api/v2/facade, hxxp[:]//nucleusgate[.]com/api/v2/facade, hxxps[:]//cardlowestgroup[.]com/api/v2/facade, hxxps[:]//socialcloudguru[.]com/api/v2/facade, hxxps[:]//coretether[.]com/api/v2/facade, hxxps[:]//registrywave[.]com/api/v2/facade
MIMICRAT	SHA256	a508d0bb583dc6e5f97b6094f8f910b5b6f2b9d5528c04e4dee62c343fce6f4b
Lua loader	SHA256	5e0a30d8d91d5fd46da73f3e6555936233d870ac789ca7dd64c9d3cc74719f51
GhostFetch	Domain	Promoverse[.]org

Attack Name	TYPE	VALUE
HTTP_VIP	Domain	codefusiontech[.]org, miniquest[.]org
SANDWORM_MODE	SHA256	5ce544f624fd2aee173f4199da62818ff78deca4ba70d9cf33460974d460395c, 5440e1a424631192dff1162eebc8af5dc2389e3d3b23bd26e9c012279ae116e4

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-25253	✗	OpenClaw Clawdbot/Moltbot (Before 2026.1.29)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openclaw:openclaw:*:*:*:*:*:*:*:*	-
OpenClaw Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-669	T1566: Phishing, T1528: Steal Application Access Token, T1059: Command and Line Interface, T1204: User Execution, T1071: Application Layer Protocol	https://github.com/openclaw/openclaw/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21509		Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	MiniDoor, PixyNetLoader
Microsoft Office Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing, T1204: User Execution, T1559: Inter-Process Communication, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8088		WinRAR Versions up to and including 7.12	Amaranth-Dragon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Amaranth Loader, TGAmaranth RAT
RARLAB WinRAR Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8110	✗	Gogs (Prior to 0.13.4, all versions through 0.13.3)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	Supershell
Gogs Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1083: File and Directory Discovery	https://github.com/gogs/gogs/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-24423	✗	SmarterTools SmarterMail (Before Build 9511)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	Warlock ransomware
SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.smartertools.com/smartermail/release-notes/current

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-23760	✗	SmarterTools SmarterMail (Before Build 9511)	Storm-2603
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	Warlock ransomware
SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.smartertools.com/smartermail/release-notes/current

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2019-11580	✗	Atlassian Crowd and Crowd Data Center	TGR-STA-1030 (aka UNC6619)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:crowd:*:*:*:*:*:*:*:*	ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat
Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	-	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21510	✗	Windows Shell	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*	-
Windows Shell Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204.001: Malicious Link, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21513	✗	MSHTML Framework	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
MSHTML Framework Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-693	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21514	✗	Microsoft Office Word	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:* cpe:2.3:a:microsoft:office_long_term_servicing_channel:*:*:*:*:*	-
Microsoft Word Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21514

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21519	✗	Desktop Window Manager	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
Desktop Window Manager Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21519

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21525	✗	Windows Remote Access Connection Manager	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*	-
Windows Remote Access Connection Manager Denial of Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-476	T1499: Endpoint Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21525

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21533	✗	Windows Remote Desktop	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*	-
Windows Remote Desktop Services Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21533

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-20700</td><td>  </td><td rowspan="2">Apple iOS (Before26.3), Apple iPadOS (Before 26.3), Apple macOS Tahoe (Before 26.3), Apple tvOS (Before 26.3), Apple watchOS (Before 26.3), Apple visionOS (Before 26.3)</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:apple:iphone_os:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apple Multiple Buffer Overflow Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-119</td><td>T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.004: Dylib Hijacking</td><td>https://support.apple.com/en-us/126346 , https://support.apple.com/en-us/126348 , https://support.apple.com/en-us/126351 , https://support.apple.com/en-us/126352 , https://support.apple.com/en-us/126353</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-2026-1731</td><td>  </td><td rowspan="2">BeyondTrust Remote Support: Before 25.3.2
BeyondTrust Privileged Remote Access: Before 25.1.1</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:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*
cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-78</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://www.beyondtrust.com/trust-center/security-advisories/bt26-02</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-2441	✗	Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium CSS Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-By Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-22769	✗	Dell RecoverPoint for Virtual Machines (RP4VMs) versions before 6.0.3.1 HF1	UNC6201
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:dell:recoverpoint_for_virtual_machines:*:*:*:*:*:*:*:*	BRICKSTORM, GRIMBOLT, SLAYSTYLE
Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-20127</td><td>  </td><td rowspan="2">Cisco Catalyst SD-WAN Controller & SD-WAN Manager (Before 20.9.8.2, 20.12.6.1, 20.12.5.3, 20.12.6.1, 20.15.4.2, 20.15.4.2, 20.15.4.2, 20.18.2.1, 20.18.2.1)</td><td rowspan="2">UAT-8616</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:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk</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-2022-20775</td><td>  </td><td rowspan="2">Cisco SD-WAN Software (Before 20.6.3 to 20.6.4)</td><td rowspan="2">UAT-8616</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:cisco:sd-wan:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco SD-WAN Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-25
CWE-22</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BadIIS	BadIIS malware is being used in the wild for SEO fraud. Through reverse engineering and infection chain analysis, two clusters were customized by UAT-8099 to target specific regions. The first cluster, BadIIS IISHijack, is named after the original malware file. The second cluster, BadIIS asdSearchEngine, is designed for similar malicious SEO manipulation.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Traffic Hijacking, System Compromise	Microsoft Windows Server, Linux
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-8099			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GlassWorm	GlassWorm is a self-propagating malware campaign that weaponizes the VS Code extension ecosystem. It conceals malicious logic using invisible Unicode characters and distributes trojanized extensions through VSCode and OpenVSX, currently focusing on macOS developers.	Supply Chain Compromise	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	macOS
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Chrysalis	The Chrysalis backdoor was a highly capable malware that used obfuscation, custom API hashing, and RC4 encryption for its configuration data. It communicated over HTTPS for secure command-and-control traffic and maintained persistence via Windows services or registry Run keys. Chrysalis collected system information and supported remote shell access, process execution, file management, directory enumeration, and self-removal to evade detection.	Supply Chain Compromise	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	Notepad++
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Lotus Blossom			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MiniDoor	MiniDoor is a lightweight DLL that drops a malicious Outlook VBA project on the system. It modifies Outlook's registry settings to weaken security, enabling macros to run automatically and ensuring the malicious project executes every time Outlook is launched.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Drops a malicious Outlook VBA project	-
Spyware			**PATCH LINK**
ASSOCIATED ACTOR			-
APT28			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PixyNetLoader	PixyNetLoader uses multiple evasion techniques to avoid detection. The loader activates only when explorer.exe is running and performs timing checks to identify sandbox environments. If the environment seems legitimate, it extracts hidden shellcode from a PNG image using steganography, concealing data within the image pixels.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		drops malicious components	-
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
APT28			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an open-source Windows RAT, ranked 6th in global prevalence in 2024. Its capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft	-
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Amaranth Loader	Amaranth Loader is a custom tool designed to deliver encrypted payloads, primarily deploying the Havoc C2 Framework. It retrieves an encrypted payload, decrypts it using AES, and executes it directly in memory.	Exploiting Vulnerability	CVE-2025-8088
		IMPACT	**AFFECTED PRODUCT**
TYPE		Loads another payload	RARLAB WinRAR
Loader			**PATCH LINK**
ASSOCIATED ACTOR			https://www.win-rar.com/download.html?&L=0
Amaranth-Dragon			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TGAmaranth RAT	TGAmaranth RAT is a fully functional 64-bit DLL remote access tool (RAT) that uses a hardcoded Telegram bot as its C&C. It uses an encrypted bot token to connect to telegram, listens for incoming bot messages, and interprets them as commands.	Exploiting Vulnerability	CVE-2025-8088
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	RARLAB WinRAR
RAT			**PATCH LINK**
ASSOCIATED ACTOR			https://www.win-rar.com/download.html?&L=0
Amaranth-Dragon			

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
Crimson RAT	Crimson RAT is a remote access trojan used for intelligence gathering. It also uses a custom TCP-based command-and-control protocol rather than standard HTTP/HTTPS, complicating network-level detection. Once active, the implant enables system reconnaissance, file exfiltration, remote command execution, and long-term persistence.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, Execute commands	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Transparent Tribe			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GymRAT	GymRAT is a malware that primarily targets Windows systems. It is often distributed via phishing and malicious attachments, enabling remote access to compromised machines. GymRAT's capabilities include keylogging, credential theft, and stealing sensitive data, allowing attackers to control and monitor infected devices.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Steal Data	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Transparent Tribe			

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
Supershell	Supershell is an open-source Command and Control (C2) platform designed to establish a reverse SSH shell that communicates over web services. This mechanism provides attackers with remote control and the ability to execute arbitrary code on a compromised system.	Exploiting Vulnerability	CVE-2025-8110
		IMPACT	AFFECTED PRODUCT
TYPE		Execute Code	Gogs
Framework			PATCH LINK
ASSOCIATED ACTOR			https://github.com/gogs/gogs/releases
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Warlock	Warlock is a ransomware-as-a-service (RaaS) operation that debuted in June 2025 with an ad on a Russian cybercrime forum (“if you want a Lamborghini, please call me”) and swiftly garnered attention by targeting businesses, governments, and other institutions.	Exploiting Vulnerabilities	CVE-2026-23760
		IMPACT	AFFECTED PRODUCTS
TYPE		Financial Loss, Data Encryption, and Exfiltration	SmarterTools SmarterMail
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://www.smartertools.com/smartermail/release-notes/current
-			

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
ShadowGuard	ShadowGuard is a Linux-focused rootkit built using Extended Berkeley Packet Filter (eBPF) technology, allowing it to run directly inside the kernel's trusted environment. Because eBPF programs execute within the kernel's BPF virtual machine rather than as standalone modules, the malware leaves little visible footprint, making detection extremely difficult. This design enables ShadowGuard to operate stealthily while maintaining deep control over compromised systems.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCTS**
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
Rootkit			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Diaoyu	Diaoyu Loader uses a dual-stage execution check to evade automated sandboxes and analysis environments. It first verifies that the system meets a minimum horizontal screen resolution of 1440 pixels, then checks for the presence of a specific file (pic1.png) in its working directory. If these conditions are not met, the malware halts execution, helping it avoid detection in controlled analysis setups.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		Loads Cobalt Strike payload	Atlassian Crowd and Crowd Data Center
Loader			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

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
VShell	VShell is a Go-based command-and-control (C2) framework commonly linked to cyber espionage operations. It enables attackers to maintain remote access to compromised systems, execute commands, and manage files during post-exploitation activities.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	AFFECTED PRODUCT
TYPE		Remote Control	Atlassian Crowd and Crowd Data Center
Framework			PATCH LINK
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Havoc	Havoc is an open-source command-and-control (C2) framework developed by C5pider. It allows operators to generate agents in multiple formats, including Windows executables, DLLs, and shellcode. Its modular architecture lets attackers tailor payloads for different objectives, making it a versatile toolkit for post-exploitation operations.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
Framework			PATCH LINK
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

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
Sliver	Sliver is an advanced malware framework used in cyberattacks, leveraging DLL sideloading and proxying techniques for persistence and stealth. It targets organizations, enabling data exfiltration and espionage while evading detection.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data exfiltration and Espionage	Atlassian Crowd and Crowd Data Center
Framework			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SparkRat	SparkRAT is a cross-platform, open-source remote administration tool written in Go and released via GitHub in 2022. It supports Windows, macOS, and Linux, giving attackers broad remote-control capabilities, including file and process management, file transfer, remote desktop viewing, system reconnaissance, and command execution through a remote terminal.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
RAT			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

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
WAVESHAPER	WAVESHAPER is a C++ backdoor malware, primarily targeting macOS, used by North Korea-linked UNC1069 in cryptocurrency theft campaigns. It runs as a background daemon, collects system details like username, hardware, and processes, then exfiltrates data via HTTP/HTTPS using curl.	ClickFix	-
		IMPACT	AFFECTED PRODUCT
TYPE		Initial access, Payload delivery, System compromise	macOS
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC1069			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SUGARLOADER	SUGARLOADER is a C++-based downloader malware historically linked to North Korean threat actors like UNC1069. It deploys secondary payloads, such as CHROMEPUSH or KANDYKORN, by checking for and decrypting a local config file before connecting to a C2 server.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	AFFECTED PRODUCT
TYPE		Payload Delivery, Persistence	macOS
Downloader			
ASSOCIATED ACTOR			PATCH LINK
UNC1069			-

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
SILENCELIFT	SILENCELIFT is a minimal C/C++ backdoor newly identified in the UNC1069 intrusion toolkit. Beacons host information and lock-screen status to a hardcoded C2 server. When run with root privileges, it can also interrupt Telegram communications on the host. Represents lightweight persistent access alongside the heavier WAVESHAPER backdoor. New to UNC1069's observed toolset.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Access, Reconnaissance	macOS
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HYPERCALL	HYPERCALL is a Golang-based downloader that reads RC4-encrypted configuration and connects to C2 over WebSockets on TCP port 443. Downloads malicious dynamic libraries and reflectively loads them into memory, avoiding disk-based detection. Delivers HIDDENCALL backdoor, SUGARLOADER downloader, and SILENCELIFT beacon during intrusions.	Deployed by WAVESHAPER	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload Delivery	macOS
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

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
DEEPBREATH	DEEPBREATH is a Swift-based data miner that bypasses macOS Transparency, Consent, and Control (TCC) by staging and modifying the TCC database through Finder's Full Disk Access. Steals iCloud Keychain credentials, browser data from Chrome, Brave, and Edge, Telegram databases, and Apple Notes content. Deployed by HIDDENCALL backdoor as part of UNC1069's credential harvesting toolkit.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential theft, Data exfiltration	macOS, Windows
Data Miner			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CHROMEPUSH	CHROMEPUSH is a C++ browser stealer that installs itself as a native messaging host disguised as a Google Docs Offline extension targeting Chromium browsers. Logs keystrokes, captures credentials, extracts cookies, and can record screenshots before exfiltrating data via HTTP POST. Deployed exclusively by SUGARLOADER as the final data theft component in the UNC1069 attack chain.	Deployed via SUGARLOADER	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data theft	macOS, Windows
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

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
Matanbuchus 3.0	Matanbuchus 3.0 Is a MaaS loader with ChaCha20-encrypted strings, in-memory stealth, LOLBin abuse via regsvr32/rundll32, and CMD/PowerShell reverse shell support. Delivered via DLL sideloading through renamed Notepad++ updater, uses MurmurHash3 for dynamic API resolution and Salsa20-encrypted C2 domains. Deploys ransomware precursors like Cobalt Strike, QakBot, DanaBot, and the new AstarionRAT.	ClickFix, Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
MaaS		Ransomware Staging, Payload Delivery	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AstarionRAT	AstarionRAT is a newly discovered full-featured RAT delivered by Matanbuchus 3.0 in a February 2026 ClickFix intrusion. Supports 24 commands covering credential theft, SOCKS5 proxy tunneling, port scanning, in-memory reflective payload execution, and shell access. Uses RSA-encrypted C2 communications disguised as application telemetry. Reached domain controllers in under 40 minutes post-infection.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote control, Credential theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
OysterLoader	OysterLoader is multi-stage C++ loader (aka Broomstick/CleanUp) distributed via fake PuTTY, WinSCP, and Google Authenticator sites as signed MSI installers. Uses TextShell packer for in-memory shellcode loading, custom LZMA decompression, and multiple environment checks before C2 communication. Primarily leads to Rhysida ransomware deployment and also distributes Vidar infostealer.	Fake software websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Payload delivery, Ransomware deployment	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BRICKSTORM	BRICKSTORM is a sophisticated Go/Rust-based backdoor targeting VMware vCenter and ESXi hosts, using DNS-over-HTTPS, nested TLS, WebSockets, and SOCKS proxy for stealth C2 and lateral movement. Self-monitoring function automatically reinstalls or restarts if disrupted, with persistence via modified VMware init scripts. Used to steal VM snapshots for credential extraction and create hidden rogue VMs across government and IT sectors.	Exploiting vulnerabilities	CVE-2026-22769
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Espionage, Persistent access, Data exfiltration	Dell RecoverPoint for Virtual Machines
ASSOCIATED ACTOR			**PATCH LINK**
UNC6201			https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

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
GRIMBOLT	GRIMBOLT is a C#-based persistent backdoor compiled using Native Ahead-of-Time (AOT) compilation and packed with UPX, replacing BRICKSTORM since September 2025. Removes CIL metadata that security tools typically scan, optimized for resource-constrained edge devices while maintaining remote shell and WebSocket C2 capabilities. Shares command-and-control infrastructure with its predecessor BRICKSTORM.	Exploiting vulnerabilities	CVE-2026-22769
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Espionage, Persistent access, Data exfiltration	Dell RecoverPoint for Virtual Machines
ASSOCIATED ACTOR			**PATCH LINK**
UNC6201			https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SLAYSTYLE	SLAYSTYLE is a Java-based web shell deployed as a malicious WAR file through Apache Tomcat Manager using hardcoded default admin credentials in Dell RecoverPoint appliances. Grants root-level command execution on compromised systems, serving as the initial foothold before BRICKSTORM and GRIMBOLT deployment. Attackers then implement iptables-based covert channels and create temporary network interfaces for VMware infrastructure pivoting.	Exploiting vulnerabilities	CVE-2026-22769
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Web Shell		Data theft	Dell RecoverPoint for Virtual Machines
ASSOCIATED ACTOR			**PATCH LINK**
UNC6201			https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

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
Cuckoo Stealer	Cuckoo Stealer is a macOS-specific infostealer and spyware malware active since early 2024, targeting both Intel and Apple Silicon systems via trojanized apps like cleaners and media converters. It steals sensitive data such as Safari credentials, cookies, Keychain passwords, and screenshots, while using obfuscation (XOR-encrypted strings), AppleScript for fake prompts, and Launch Agents for persistence.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Stealer		Data theft	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MIMICRAT	MIMICRAT is a custom C++ remote access trojan delivered via ClickFix campaigns that compromise legitimate websites. It features malleable C2 profiles, Windows token impersonation, SOCKS5 tunneling, and a 22-command dispatch table for post-exploitation. It communicates over HTTPS on port 443, disguised to look like legitimate web analytics traffic.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote access, Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lua Loader	Lua Loader is a custom in-memory loader used in the MIMICRAT ClickFix campaign that embeds its own Lua interpreter. It decrypts an XOR-encoded shellcode payload and executes it entirely in memory, leaving no disk artifacts. The shellcode matches Meterpreter signatures and is used to reflectively load the MIMICRAT RAT into the victim's system.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload delivery, Defense evasion	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GhostFetch	GhostFetch is a first-stage downloader used by MuddyWater (Operation Olalampo) designed to fetch and execute secondary payloads directly in memory. It profiles compromised systems by validating mouse movement, screen resolution, detecting debuggers, VM artifacts, and AV software before proceeding. It ultimately drops an advanced second-stage implant called GhostBackDoor.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload delivery, Sandbox evasion	Windows
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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
HTTP_VIP	HTTP_VIP is a native downloader attributed to MuddyWater that performs system reconnaissance and connects to an external C2 server for authentication. It deploys AnyDesk from the C2 server, and newer variants can retrieve victim information, start an interactive shell, download/upload files, capture clipboard contents, and update beaconing intervals.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Reconnaissance, Remote access, Data exfiltration	Windows
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CHAR	CHAR is a Rust-based backdoor used by MuddyWater, controlled via a Telegram bot (named "Olalampo") to execute cmd.exe or PowerShell commands and change directories. Group-IB's analysis revealed signs of AI-assisted development, including emojis in debug strings. It shares structural similarities with the previously known BlackBeard/Archer RAT malware.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload delivery, Sandbox evasion	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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
GhostBackDoor	GhostBackDoor is a second-stage implant delivered by GhostFetch in MuddyWater's Operation Olalampo campaign. It supports an interactive shell, file read/write operations, and the ability to re-run GhostFetch. It adapts its installation method based on the target's privilege level, installing as a service with admin access or using the startup registry folder for standard users.	Dropped by GhostFetch	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		System compromise, Data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SANDWORM_MODE	SANDWORM_MODEA is a self-propagating npm supply chain worm spread through 19 typosquatted packages that steals credentials, infects projects, and propagates across developer environments. It uniquely poisons AI development toolchains by injecting a rogue MCP server into AI coding assistants like Claude Code and Cursor, manipulating them into silently exfiltrating credentials. It also contains a dormant destructive dead switch capable of wiping the home directory.	Typosquatted npm packages	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Worm		Credential theft, Supply chain compromise, AI toolchain poisoning	macOS, Linux, 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.

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UAT-8099</td><td>-</td><td rowspan="2">Education, Technology, Telecommunications</td><td rowspan="2">India, Thailand, Vietnam, Canada, Brazil, Pakistan, Japan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>BadIIS</td><td>Microsoft Internet Information Services (IIS)</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011:Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1505: Server Software Component; T1505.003: Web Shell; T1505.004: IIS Components; T1136: Create Account; T1136.001: Local Account; T1078: Valid Accounts; T1078.003: Local Accounts; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1027: Obfuscated Files or Information; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1071: Application Layer; Protocol T1071.001: Web Protocols; T1572: Protocol Tunneling; T1491: Defacement; T1491.002: External Defacement</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Lotus Blossom (also known as LOTUS PANDA, Billbug, Bronze Elgin, Spring Dragon, Raspberry Typhoon, Thrip)</td><td>China</td><td rowspan="3">Government, Financial Services, Information Technology, Telecom, Aviation, Critical Infrastructure, Media</td><td rowspan="3">Australia, Belize, Brunei, Cambodia, Costa Rica, El Salvador, Guatemala, Honduras, Indonesia, Laos, Malaysia, Myanmar, Nicaragua, Panama, Philippines, Singapore, Thailand, Timor-Leste, Vietnam</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>Chrysalis Backdoor</td><td>Notepad++</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1204: User Execution T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1106: Native API; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process ; T1543.003: Windows Service; T1574: Hijack Execution Flow ; T1574.002: DLL; T1027: Obfuscated Files or Information ; T1027.007: Dynamic API Resolution; T1140: Deobfuscate/Decode Files or Information; T1036: Masquerading; T1055: Process Injection; T1620: Reflective Code Loading; T1480: Execution Guardrails ; T1480.002: Mutual Exclusion; T1083: File and Directory Discovery; T1082: System Information Discovery; T1005: Data from Local System; T1071: Application Layer Protocol ; T1071.001: Web Protocols; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1070: Indicator Removal ; T1070.004: File Deletion</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)	Russia	All	Central and Eastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-21509	MiniDoor, PixyNetLoader	Microsoft Office

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0042: Resource Development; T1566: Phishing T1566.001: Spearphishing Attachment; T1203: Exploitation for Client Execution; T1106: Native API; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1546: Event Triggered Execution; T1546.015: Component Object Model Hijacking; T1137: Office Application Startup ; T1137.006: Add-ins; T1574: Hijack Execution Flow; T1574.001: DLL; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.002: Mutual Exclusion; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.003: Steganography; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1114: Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1588: Obtain Capabilities; T1588.006: Vulnerabilities

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Amaranth-Dragon	China	Government, Law Enforcement	Cambodia, Thailand, Laos, Indonesia, Singapore, Philippines, Brunei, Malaysia, Myanmar, Timor-Leste, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-8088	Amaranth Loader, TGAmaranth RAT	RARLAB WinRAR
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spear-phishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1203: Exploitation for Client Execution; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1140: Deobfuscate/Decode Files or Information; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1055: Process Injection; T1055.012: Process Hollowing; T1620: Reflective Code Loading; T1056: Input Capture; T1057: Process Discovery; T1082: System Information Discovery; T1113: Screen Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel		

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Transparent Tribe (also known as APT36, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134)	Pakistan	Startups, Technology, Government, Defense, Military, Education	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Crimson RAT, GymRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0003: Persistence; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1553: Subvert Trust Controls; T1553.005: Mark-of-the-Web Bypass; T1027: Obfuscated Files or Information; T1027.001: Binary Padding; T1027.002: Software Packing; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1547: Boot or Logon Autostart Execution; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1016: System Network Configuration Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1113: Screen Capture; T1125: Video Capture; T1123: Audio Capture; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-2603	China	All	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-23760	-	SmarterTools SmarterMail
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; TA0040: Impact; TA0042: Resource Development; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1036: Masquerading; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1486: Data Encrypted for Impact; T1588: Obtain Capabilities; T1588.006: Vulnerabilities			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
TGR-STA-1030 (aka UNC6619)</td><td>Asia</td><td rowspan="3">Government, Foreign Affairs, Finance, Interior, Justice, Trade, Economy, Energy, Immigration, Mining, Natural Resources, Law Enforcement, Border Control, Counter-terrorism, Defense, Telecommunications, Aviation, Financial Services, Technology, Public Sector IT, Parliament, Diplomatic Services</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2019-11580</td><td>ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat</td><td>Atlassian Crowd and Crowd Data Center</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0003: Persistence; TA0011: Command and Control; TA0042: Resource Development; TA0004: Privilege Escalation; TA0043: Reconnaissance; T1566: Phishing; T1566.002: Spearphishing Link; T1190: Exploit Public-Facing Application; T1204: User Execution; T1204.002: Malicious File; T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1014: Rootkit; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1564.003: Hidden Window; T1518: Software Discovery; T1518.001: Security Software Discovery; T1505: Server Software Component; T1505.003: Web Shell; T1105: Ingress Tool Transfer; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1572: Protocol Tunneling; T1090: Proxy; T1090.002: External Proxy; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1068: Exploitation for Privilege Escalation; T1595: Active Scanning; T1595.002: Vulnerability Scanning</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC1069 (alias CryptoCore, MASAN)</td><td>North Korea</td><td rowspan="3">Cryptocurrency, FinTech, Financial Services, High Tech, Manufacturing, Transportation</td><td rowspan="3">United States, Canada, Norway, Austria, Netherlands, United Kingdom, France, Belgium, Ireland, Luxembourg, Monaco, South Korea, India, Israel, Hong Kong</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>WAVESHAPER, SUGARLOADER, SILENCELIFT, HYPERCALL, DEEPBREATH, CHROMEPUSH</td><td>macOS, Windows, Telegram, Chromium-Based Browsers (Google Chrome, Brave, Microsoft Edge), Zoom</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1566: Phishing, T1566.003: Spearphishing via Service, T1566.004: Spearphishing Voice, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1059.002: AppleScript, T1218: System Binary Proxy Execution, T1218.005: Mshta, T1543: Create or Modify System Process, T1543.004: Launch Daemon, T1176: Browser Extensions, T1027: Obfuscated Files or Information , T1027.002: Software Packing, T1620: Reflective Code Loading, T1036: Masquerading , T1036.005: Match Legitimate Name or Location, T1555: Credentials from Password Stores, T1555.001: Keychain, T1555.003: Credentials from Web Browsers, T1056: Input Capture T1056.001: Keylogging, T1005: Data from Local System, T1185: Browser Session Hijacking, T1074: Data Staged , T1074.001: Local Data Staging , T1041: Exfiltration Over C2 Channel, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1071.004: DNS, T1102: Web Service</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC6201</td><td>China</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>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>CVE-2026-22769</td><td>BRICKSTORM, GRIMBOLT, SLAYSTYLE</td><td>Dell RecoverPoint for Virtual Machines</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1190: Exploit Public-Facing Application, T1078: Valid Accounts T1078.001: Default Accounts, T1059: Command and Scripting Interpreter, T1037: Boot or Logon, Initialization Scripts T1037.004: RC Scripts, T1505: Server Software Component , T1505.003: Web Shell, T1027: Obfuscated Files or Information , T1027.002: Software Packing, T1205: Traffic Signaling , T1205.001: Port Knocking, T1021: Remote Services, T1599: Network Boundary Bridging, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1572: Protocol Tunneling, T1068: Exploitation for Privilege Escalation, T1587: Develop Capabilities , T1587.001: Malware, T1588: Obtain Capabilities , T1588.006: Vulnerabilities</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
MuddyWater (aka Earth Vetala, Mango Sandstorm, MUDDYCOAST, Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Boggy Serpens, Yellow Nix)</td><td>Iran</td><td rowspan="3">Energy, Marine Services, System Integrators, Government</td><td rowspan="3">Middle East and North Africa (MENA), META (Middle East, Turkey, Africa)</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>GhostFetch, HTTP_VIP, CHAR, GhostBackDoor</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1587: Develop Capabilities, T1587.001: Malware, T1566: Phishing , T1566.001: Spear-phishing Attachment, T1190: Exploit Public-Facing Application, T1204: User Execution , T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1106: Native API, T1547: Boot or Logon Autostart , T1140: Deobfuscate/Decode Files or Information, T1620: Reflective Code Loading, T1027: Obfuscated Files or Information , T1027.013: Encrypted/Encoded File, T1497: Virtualization/Sandbox Evasion , T1497.001: System Checks, T1036: Masquerading, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1555: Credentials from Password Stores, T1115: Clipboard Data, T1005: Data from Local System, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1102: Web Service, T1219: Remote Access Software, T1573: Encrypted Channel, T1029: Scheduled Transfer, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Mercenary Akula (aka UAC-0050, DaVinci Group, Fire Cells Group)</td><td>Russia</td><td rowspan="3">Financial Services</td><td rowspan="3">Western Europe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft, Espionage and Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1589: Gather Victim Identity Information, T1589.003: Employee Names , T1566: Phishing , T1566.002: Spearphishing Link, T1204: User Execution , T1204.002: Malicious File , T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1036: Masquerading , T1036.007: Double File Extension, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1218: System Binary Proxy Execution , T1218.011: Rundll32, T1562: Impair Defenses , T1562.004: Disable or Modify System Firewall, T1672: Email Spoofing, T1219: Remote Access Software, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1102: Web Service, T1005: Data from Local System, T1560: Archive Collected Data , T1560.001: Archive via Utility, T1657: Financial Theft</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-8616	-	Financial Services	Western Europe
	MOTIVE		
	Information theft, Espionage and Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-20127 CVE-2022-20775	-	Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Manager
TTPs			
T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts, T1098: Account Manipulation , T1098.004: SSH Authorized Keys, T1136: Create Account, T1070: Indicator Removal , T1070.003: Clear Command History, T1601: Modify System Image , T1601.001: Patch System Image, T1036: Masquerading, T1021: Remote Services , T1021.004: SSH, T1529: System Shutdown/Reboot , T1588: Obtain Capabilities , T1588.006: Vulnerabilities			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.003: Employee Names
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
		T1608.005: Link Target
		T1584.003: Virtual Private Server
	T1589: Gather Victim Identity Information	T1589.003: Employee Names
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
		T1590.002: DNS
		T1598.002: Spearphishing Attachment
		T1598.004: Spearphishing Voice
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.005: Link Target
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
		T1195.002: Compromise Software Supply Chain
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	

Tactic	Technique	Sub-technique
TA0002: Execution	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1136: Create Account	T1136.001: Local Account
	T1137: Office Application Startup	T1137.006: Add-ins
	T1176: Browser Extensions	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
		T1543.004: Launch Daemon
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.004: Dylib Hijacking
		T1574.006: Dynamic Linker Hijacking
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.004: Launch Daemon
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.004: Dylib Hijacking
		T1574.006: Dynamic Linker Hijacking
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.002: Software Packing
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation
		T1027.013: Encrypted/Encoded File

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.007: Double File Extension
	T1055: Process Injection	T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.007: Msiexec
		T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
		T1553.002: Code Signing
		T1553.005: Mark-of-the-Web Bypass
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
		T1562.004: Disable or Modify System Firewall
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.004: Dylib Hijacking
		T1574.006: Dynamic Linker Hijacking
	T1599: Network Boundary Bridging	
	T1601: Modify System Image	T1601.001: Patch System Image
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
TA0006: Credential Access	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.004: SSH
	T1072: Software Deployment Tools	
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1123: Audio Capture	
	T1125: Video Capture	
	T1185: Browser Session Hijacking	
	T1557: Adversary-in-the-Middle	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1029: Scheduled Transfer	
	T1041: Exfiltration Over C2 Channel	
TA0011: Command and Control	T1001: Data Obfuscation	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.002: External Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1132: Data Encoding	T1132.001: Standard Encoding
		T1132.002: Non-Standard Encoding
	T1219: Remote Access Software	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1491: Defacement	T1491.002: External Defacement
	T1499: Endpoint Denial of Service	
	T1529: System Shutdown/Reboot	
	T1565: Data Manipulation	T1565.001: Stored Data Manipulation
	T1657: Financial Theft	

Top 5 Takeaways

#1

In February 2026, **13 zero-day vulnerabilities** surfaced. These zero-days were found across products from **Microsoft Windows, Apple, Google Chrome, Dell, WinRAR, Gogs, and Cisco.**

#2

Newly identified malware active in February included a broad mix of **Backdoors, RAT, and Loaders**. Key discoveries were **Chrysalis, WAVESHAPER, SILENCELIFT, GRIMBOLT, GhostBackDoor, Amaranth Loader, OysterLoader, TGAmaranth RAT, AstarionRAT,** and **MIMICRAT**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

#3

Cyberattacks concentrated heavily on **Thailand, India, Indonesia, Vietnam, and Monaco**, which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4

Technology, Government, Financial, Education, and Telecommunications sectors absorbed the bulk of targeted activity, with ransomware operations, data theft, and espionage campaigns driving operational disruption. Attackers continued refining techniques and expanding pressure across these industries.

#5

Activity during the period was dominated by **APT28, Amaranth-Dragon, Storm-2603, and UNC6201**, all well-resourced groups known for sustained, high-impact operations. Their campaigns shaped a threat landscape defined by disciplined tradecraft, rapid exploitation cycles, and a clear focus on high-value targets across public and private sectors.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **19 significant vulnerabilities** and block the indicators related to the **12 active threat actors, 38 active malware,** and **183 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 **19 significant vulnerabilities**

• Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Social engineering: is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

Supply chain attack: Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

Eavesdropping: Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
CVE - Common Vulnerabilities and Exposures
CPE - Common Platform Enumeration
CWE - Common Weakness Enumeration

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
BadIIS	SHA256	1ab98783a02ad9f127e776c435ef4e24a18ab93c4b4ee5ede722817d4b20771a, 1ece4d8603f5e28a7b0f6a8c83963a57cf23e5d2fadfc138419c3a051a75c93a, 2cc87bd2ae25a5119cb950618850eddeb578954fa780b125c1f51d234fb405e3, 4bc189af91779582a1d29cfe187aa233e7ba50d223261fb9fbe31df5b06dff96, 6be5c8882bc02cf4e86d2ab9d20aa3446b71dd12c73f9c6bf0faf9412d7d23ba, 9a2fd34e22c5f3d3d5fb96e3cd514dad7b03ed7bf53a87e7d8d9b73987d02ece, 11ea6aa2b31677f8a36627d4af709e70cff4a033b0975f63c19b28945e6226b7, 29ffb1d28f98582e81e78e6b2d5502da50c8ebdee0d40005a86b0dadece2923b, 56be91643dd8b86f347cc8d743c568f2d0169781ba999a2f708e503b59ecff76, 70d6bc89451e36889c045f30de22bc02e032788c8938baa0d5802e8f747c3e79, 91e1f4fc92f104ec8b29bb56df87f8e7d8b518c63997e2ea162d3f1cac3fcac1, 416ef6da8a27a99cbce6517d31857c8b8b55f02e9c8118510dc33814fb6f57be, 660ccb6dcfad97bfaddc667c61b1904e99a06eab981d44119092624d42912d68, 9458a75c1e24add9a48e0425e514a5f0cb46a826bff30ea7ea34e69099345f29, 265336511db98a4c40476455e2ae93aaf926abecd8f9b9d741f8d253abb80357, a781581baf6e1e335f22c9ffbb2656a2d9c8e51f463e3a48068210425df1c205, ab03a7caed279fc6411ec19386faff3b65be34c91c3f0550eaef84a663720d0d, bcc393c1686a0f5d493041e98dcafe0098d952d5e93eb4d2ebdb63c0efd2de33, c7a22f5c55ac1373a5964a6598da2a9afd8a61b9d729b9bf52a93c967a7f0eda, cdf454173bac13266e0f7db5de386439f197e2c480e1cc303dd7e806484645da,

Attack Name	TYPE	VALUE
BadIIS	SHA256	e84a16c8e25a4e40926cbb4cc210a09830298b6f99d532035f5136d05ffc008c, e448557d26cf2917efded8e30c67db8094ce1f6db78801742988ea21f3429d7c, 5d320b60d2f40c200e81eaeb67a86a04782bff84582c73e726255dba2dcb821e, 99f2c4773560eb515cfcb0ad45cf8e47c46580ab19494463160f885e048ce830, 565502d2454e4b65d3bd810fccf4b429264562fefa5cfff24c905b76b3b860a6, a34ea8fb565ac6f57eefc987c61159c1e6f1af6a8717ffb42f4b745db3bf9e31, 187e1417fd9d4f4a44e4f7b7172aef056e9d0ab5d7a7addf61c2cfa893f74fd1, 6b60b6df8a1a95f51ffe57255c05d26eb9e113857efac3b29d6ef080b8d414f3, 672ffdf1e9d4848015d29a68111266ef55fc6702dfe7b2053ce677882648dd5d, ebeef831c52b7e930a6456caedf7849814b8d4def2bc0e70a0e7a357621ef6bc, 230b84398e873938bbcc7e4a1a358bde4345385d58eb45c1726cee22028026e9, 48ec6530470b295db455bf2c72dc4fbd18672725f45821304f966d436b428865, 33d3ccf82279d94a8e8e772a0c4963d65a1f3576dbd6ed7b4ab8a0ee4869f97f, d8c0ef6dbf7d4572f92d3a492f32061ab8f3dd46beb9ff5a0bf9bf550935458c
GlassWorm	SHA256	ad6d0679b5b9d2b2458047d4a9adc2d9920abbcf71f9b987b917f07d325ec3f3, 9707200067f6903f70c65721338dc1de18f1cab687a85c868d632cf12bb2f278, b62acc93eb77a4ffb88cf49a8bcef574e6216e10714433a9cb1230bdb2c90546, 6beaf047e948c366cb21d16818e1d0bb0ebbd928f40fe22c521344ad9c38f32e, e46ab145387e8ae996a202520f73088ae735f88f18fab1ed60469334d58d727d, 4210121526cb985d0026469de0dc5f3767ce792149164df8fd0b43b4d6f30959, c8c523ff27a7fc4bef39dce97261c97bf724556cf32d0030090c168f82b20c7a, da4aefbcda028808dc892ad5a10bb528f129883ab9c29bb6800d298d3c26f848, d84cbd286724fe8c38f4e389ce9f582df93cac37172823f4eecacdcef0a5975d,

Attack Name	TYPE	VALUE
GlassWorm	SHA256	6f698f6983fc7ece0cade5f0c1bc7a66f7400229e0e99271ea9df6bece9473cf, ca2a7d82456036d905b5ea0e25678d8e6af165dc5d2a850450f22e2e63cb2767, 130d1f487072e512611489c4cd725bdfb59c31327d056bdbd22bea4f8fab576b, a3e5d8643dffb775a32fe73b08319dd6b201ec0f0215a048a22f0c47b9a08066
Chrysalis	SHA256	a511be5164dc1122fb5a7daa3eef9467e43d8458425b15a640235796006590c9, 8ea8b83645fba6e23d48075a0d3fc73ad2ba515b4536710cda4f1f232718f53e, 77bfea78def679aa1117f569a35e8fd1542df21f7e00e27f192c907e61d63a2e, 3bdc4c0637591533f1d4198a72a33426c01f69bd2e15ceee547866f65e26b7ad, 0a9b8df968df41920b6ff07785cbfebe8bda29e6b512c94a3b2a83d10014d2fd
MiniDoor	MD5	f05d0b13c633ad889334781cf4091d3e
	SHA1	7bbb530eb77c6416f02813cd2764e49bd084465c
	SHA256	bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e
PixyNetLoader	MD5	859c4b85ed85e6cc4eadb1a037a61e16
	SHA1	da1c3e92f69e6ca0e4f4823525905cb6969a44ad
	SHA256	0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e, a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1
AsyncRAT	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ececf197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87

Attack Name	TYPE	VALUE
Supershell	IPv4	119[.]45[.]176[.]196
	SHA1	d8fcd57a71f9f6e55b063939dc7c1523660b7383, efda81e1100ea977321d0f2eeb0dfa7a6b132abd
Amaranth Loader	SHA1	00351add8e0bca838e8dac40875b8ad5195805bd, 481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2, 718c5846d3b903e3e9e2df9281f5e25b371465f2, 9afadca9b2dad54004bd376dbee7e98c38dbdf50, b4dc300031edf5dd4968028146b0d608bdd975c5, c54a68d6bcc6d04ff08ad9619706e54923a20248, cd949663598c49141a98b438cf408113602e5c19, ddea99cb2db5e95552dccc8804125f19b30af536
	SHA256	d7711333c34a27aed5d38755f30d14591c147680e2b05eaa0484c958ddaae3b6
TGAmaranth RAT	SHA1	803fb65a58808fd3752f9f76b5c75ca914196305
	SHA256	a3805b24b66646c0cf7ca9abad502fe15b33b53e56a04489cfb64a238616a7bf
Crimson RAT	MD5	5b4a48815446cd40d8e141cbf8582296
	SHA256	1092761df305e910f806834fb774dfb09dc64a4d399d578a0d1bf1dd5daf0f98
	IPv4	93[.]127[.]133[.]9
	Domain	Sharmaxme11[.]org
Warlock	SHA256	d1f9ace720d863fd174753e89b9e889d2e2f71a287fde66158bb2b5752307474
ShadowGuard	SHA256	7808B1E01EA790548B472026AC783C73A033BB90BBE548BF3006ABFBCB48C52D
Diaoyu	SHA256	23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe, 66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0
Havoc	SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8, 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c, 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328, b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c
Sliver	MD5	8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1
	SHA1	953bd0859c86e0a3a3da52fe392a7d579a9f937b, 538cb25bfae6501d8c3c7053a293e8ca85a8dba4

Attack Name	TYPE	VALUE
Sliver	SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd83907411415e5428f7a9
SparkRat	SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697
WAVESHAPER	SHA256	b525837273dde06b86b5f93f9aeC2C29665324105b0b66f6df81884754f8080d
SUGARLOADER	Domain	breakdream[.]com, dreamdie[.]com
	SHA256	1a30d6cdb0b98feed62563be8050db55ae0156ed437701d36a7b46aabf086ede
SILENCELIFT	Domain	support-zoom[.]us
	SHA256	c3e5d878a30a6c46e22d1dd2089b32086c91f13f8b9c413aa84e1dbaa03b9375
HYPERCALL	Domain	supportzm[.]com, zmsupport[.]com
	SHA256	c8f7608d4e19f6cb03680941bbd09fe969668bcb09c7ca985048a22e014dffcd, 03f00a143b8929585c122d490b6a3895d639c17d92C2223917e3a9ca1b8d30f9
DEEPBREATH	SHA256	b452C2da7c012eda25a1403b3313444b5eb7C2c3e25eee489f1bd256f8434735
CHROMEPUSH	Domain	cmailer[.]pro
	SHA256	603848f37ab932dccef98ee27e3c5af9221d3b6ccfe457ccf93cb572495ac325
Matanbuchus 3.0	URL	hxxps[:]//marle[.]io/check/updprofile[.]aspx
	SHA256	6ffae128e0dbf14c00e35d9ca17c9d6c81743d1fc5f8dd4272a03c66ecc1ad1f, ea378496135318ac5ad667a032fa4a9686add9d27fe4a7c549c937611b5099e5
AstarionRAT	Domain	www[.]ndibstersoft[.]com
	SHA256	eecc83add16f3d513a9701e9a646b1885014229ac6f86addd6b10afb64d1d2af
OysterLoader	URLs	hxxps[:]//grandideapay[.]com/api/v2/facade, hxxp[:]//nucleusgate[.]com/api/v2/facade, hxxps[:]//cardlowestgroup[.]com/api/v2/facade, hxxps[:]//socialcloudguru[.]com/api/v2/facade, hxxps[:]//coretether[.]com/api/v2/facade, hxxps[:]//registrywave[.]com/api/v2/facade

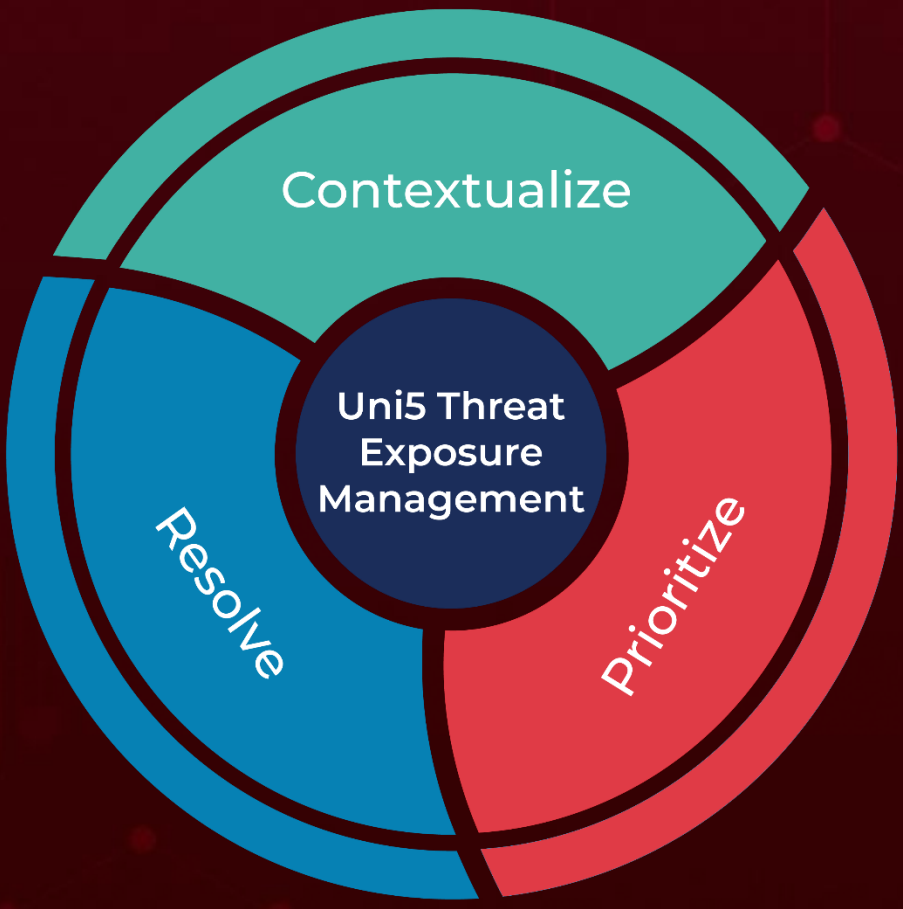
Attack Name	TYPE	VALUE
BRICKSTORM	SHA256	aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759, 90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830
GRIMBOLT	SHA256	24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c, dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591
	IPv4	149[.]248[.]11[.]71
SLAYSTYLE	SHA256	92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a
Cuckoo Stealer	SHA256	545dd5cba264bf242bc837330ca34247e202f7ac25f03eec63bf5842357519f1
MIMICRAT	SHA256	a508d0bb583dc6e5f97b6094f8f910b5b6f2b9d5528c04e4dee62c343fce6f4b
Lua loader	SHA256	5e0a30d8d91d5fd46da73f3e6555936233d870ac789ca7dd64c9d3cc74719f51
GhostFetch	Domain	Promoverse[.]org
HTTP_VIP	Domain	codefusiontech[.]org, miniquest[.]org
CHAR	SHA256	3a19c19d9f3bac6628a968110477ee01e5867b2534e914e1be5c4485947bd819
SANDWORM_MODE	SHA256	5ce544f624fd2aee173f4199da62818ff78deca4ba70d9cf33460974d460395c, 5440e1a424631192dff1162eebc8af5dc2389e3d3b23bd26e9c012279ae116e4

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

March 3, 2026 • 8:30 AM

More at www.hivepro.com