Hive Pro

HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

10 to 16 MARCH 2025

Table Of Contents

Summary

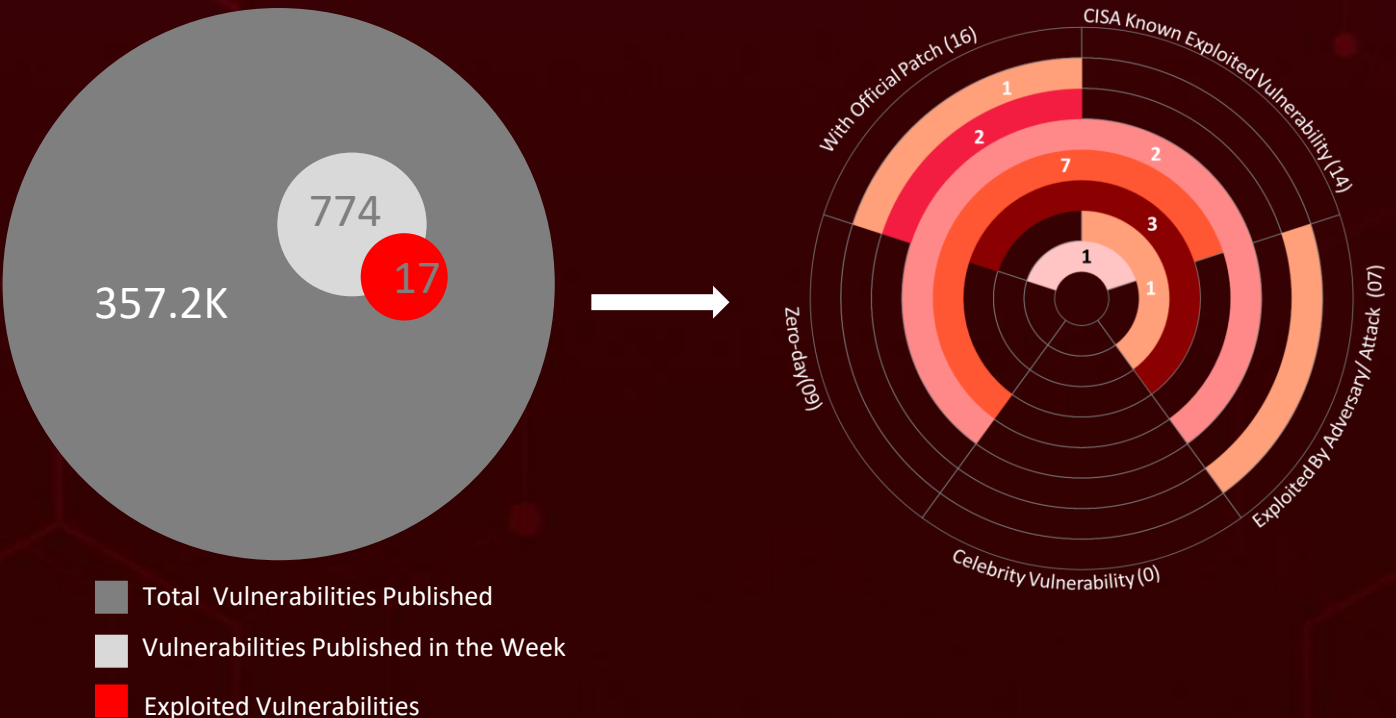HiveForce Labs has identified a surge in cyber threats, with **seven** attacks executed, **seventeen** vulnerability uncovered, and **three** active adversaries exposed in the past week alone highlighting the relentless nature of cyberattacks.

HiveForce Labs has uncovered a surge in cyber threats, including an actively exploited zero-day vulnerability in Apple's WebKit engine. Tracked as **CVE-2025-24201**, this flaw allows attackers to escape the Web Content sandbox using malicious web pages, enabling stealthy exploitation in the wild. Meanwhile, the **SuperBlack** ransomware, a modified LockBit 3.0 variant, is being deployed by the **Mora_001** threat actor in aggressive double extortion campaigns.

Adding to the growing threat landscape, **Blind Eagle**, a cunning cybercriminal group, is leveraging **CVE-2024-43451**, a newly patched Windows flaw, to bypass defenses and compromise over 1,600 victims. This group isn't just exploiting vulnerabilities it actively studies security fixes, striking before organizations can implement protections. These evolving threats underscore the urgency of timely patching, proactive defense strategies, and heightened cybersecurity awareness to counter the relentless wave of cyber exploitation.

774

17

357.2K

With Official Patch (16)

CISA Known Exploited Vulnerability (14)

Exploited By Adversary / Attack (07)

Celebrity Vulnerability (0)

Zero-day (09)

1

2

7

2

3

1

1

- Total Vulnerabilities Published
- Vulnerabilities Published in the Week
- Exploited Vulnerabilities

⚙️ High Level Statistics

7
Attacks
Executed

17
Vulnerabilities
Exploited

3
Adversaries in
Action

- **PolarEdge Botnet**
- **SilentCryptoMiner**
- **StealerBot**
- **PureCrypter RAT**
- **Remcos RAT**
- **Medusa**
- **SuperBlack**

- **CVE-2024-4577**
- **CVE-2023-20118**
- **CVE-2017-11882**
- **CVE-2025-24201**
- **CVE-2024-43451**
- **CVE-2025-24983**
- **CVE-2025-24984**
- **CVE-2025-24985**
- **CVE-2025-24991**
- **CVE-2025-24993**
- **CVE-2025-26633**
- **CVE-2025-26630**
- **CVE-2025-27363**
- **CVE-2024-1709**
- **CVE-2023-48788**
- **CVE-2025-24472**
- **CVE-2024-55591**

- **SideWinder**
- **Blind Eagle**
- **Mora_001**

⚙ Insights

A Digital Predator
Medusa ransomware escalates its tactics, luring cybercriminals with big payouts and relentless follow-ups.persistent access

SideWinder Strikes Again
This persistent APT exploits CVE-2017-11882 to deploy StealerBot, targeting critical sectors across Asia, the Middle East, and Africa.

March Patch Tuesday
Microsoft patches 57 vulnerabilities and 10 third-party flaws, closing six zero-day exploits.

PolarEdge Botnet
A hidden flaw turns Cisco, ASUS, QNAP, and Synology routers into stealthy cyber weapons, infecting 2,000+ devices.
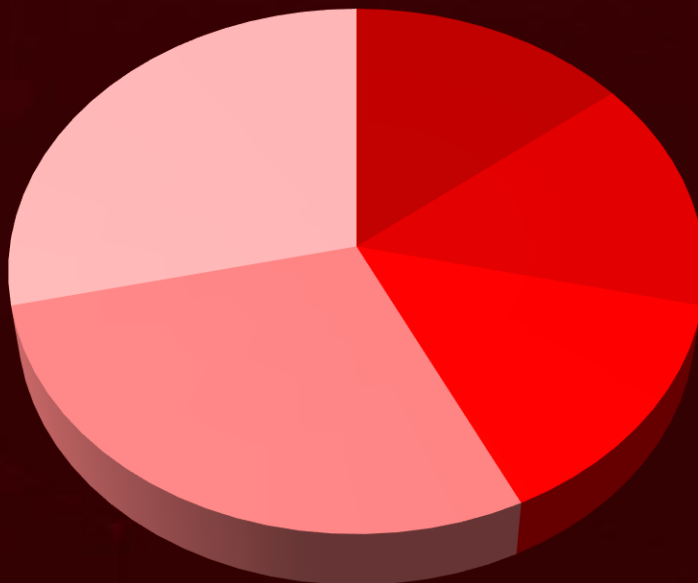
CVE-2025-24201 Exploited
A zero-day in WebKit, actively exploited to bypass sandboxing, now fixed, update immediately.

Blind Eagle Strikes Fast
Exploiting CVE-2024-43451, this group hits 1,600+ victims before defenses catch up.

Threat Distribution

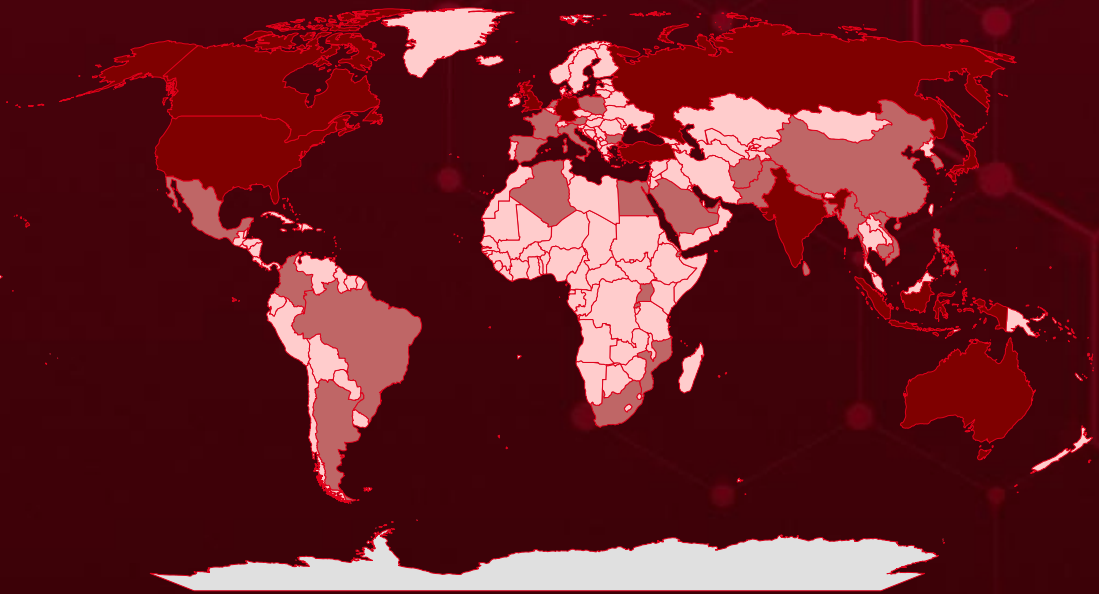■ Botnet ■ CryptoMiner ■ Toolkit ■ RAT ■ Ransomware

🌐 Targeted Countries

Most

Least

Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin
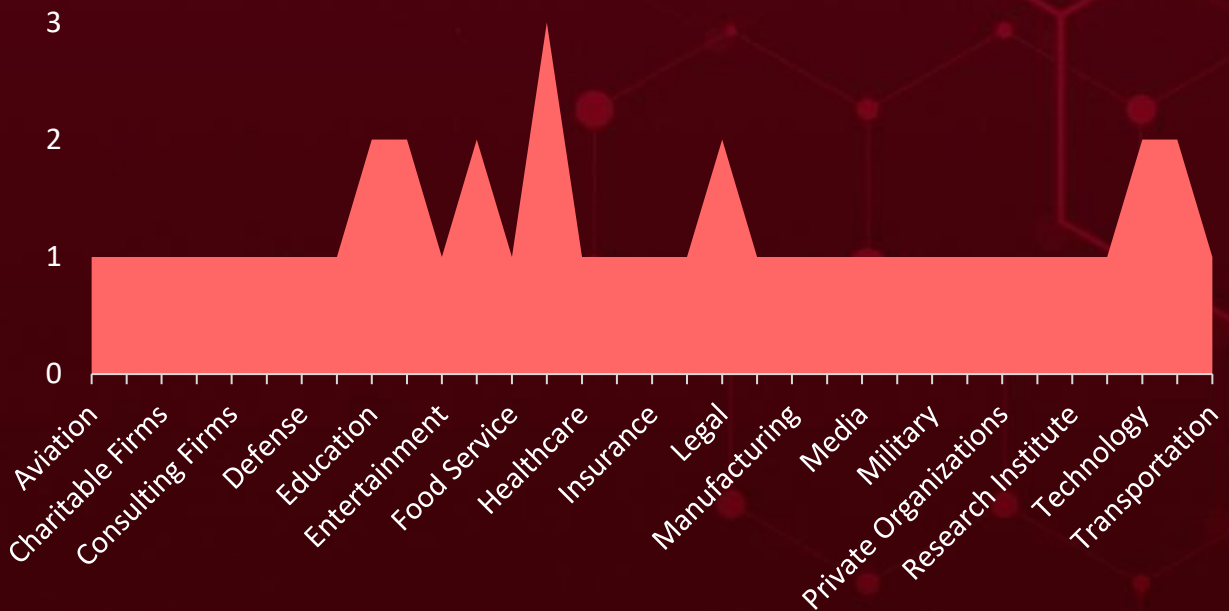
Countries
United States
Indonesia
Turkey
Australia
United Kingdom
Canada
Russia
Germany
India
Japan
Nepal
South Africa
Poland
Colombia
Argentina
Djibouti
Pakistan
Egypt
Rwanda
France
Spain
Algeria

Countries
United Arab Emirates
Austria
Netherlands
Bangladesh
Philippines
Italy
Cambodia
Brazil
Saudi Arabia
Bulgaria
South Korea
Maldives
Sri Lanka
Mexico
Uganda
Mozambique
China
Myanmar
Afghanistan
Vietnam
Switzerland
Cabo Verde

Countries
Armenia
Cyprus
Sierra Leone
Czech Republic (Czechia)
Costa Rica
Denmark
Norway
Bahrain
Saint Lucia
Dominica
South Sudan
Dominican Republic
Tonga
DR Congo
Albania
Ecuador
Niger
Antigua and Barbuda
Panama
El Salvador
Romania
Equatorial Guinea

Countries
Central African Republic
Eritrea
Solomon Islands
Estonia
State of Palestine
Eswatini
Tanzania
Ethiopia
Turkmenistan
Fiji
Uzbekistan
Finland
Namibia
Barbados
New Zealand
Gabon
North Korea
Gambia
Burundi
Georgia
Paraguay
Belarus

🏭 Targeted Industries

Chart axis labels (x-axis): Aviation, Charitable Firms, Consulting Firms, Defense, Education, Entertainment, Food Service, Healthcare, Insurance, Legal, Manufacturing, Media, Military, Private Organizations, Research Institute, Technology, Transportation

Y-axis: 0, 1, 2, 3

⚛ TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1027** Obfuscated Files or Information	**T1190** Exploit Public-Facing Application
T1083 File and Directory Discovery	**T1082** System Information Discovery	**T1070** Indicator Removal	**T1566** Phishing	**T1105** Ingress Tool Transfer
T1053 Scheduled Task/Job	**T1057** Process Discovery	**T1059.001** PowerShell	**T1055** Process Injection	**T1543** Create or Modify System Process
T1133 External Remote Services	**T1068** Exploitation for Privilege Escalation	**T1047** Windows Management Instrumentation	**T1059.003** Windows Command Shell	**T1204** User Execution

⚔ Attacks Executed

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

IOC TYPE	VALUE
SHA256	eda7cc5e1781c681afe99bf513fcaf5ae86afbf1d84dfd23aa563b1a043cbba8, 13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13, 464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SilentCryptoMiner	SilentCryptoMiner is a covert cryptocurrency miner based on XMRig, capable of mining multiple cryptocurrencies like ETH, ETC, XMR, and RTM using various algorithms. It employs process hollowing to inject its miner code into dwm.exe for stealth and halts mining when specific processes defined in its configuration are active to evade detection. The malware is remotely controlled via a web panel and incorporates anti-analysis techniques, scanning for virtualized environments and enforcing an executable size between 680 MB and 800 MB. Its configuration is Base64-encoded and AES-CBC encrypted, adding an extra layer of obfuscation.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
CryptoMiner		Mine cryptocurrencies	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	44B212683CDEF95C55DD2E645B414B5179B589C64F1DBD6F5B4252BD4CA59790

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StealerBot	StealerBot is a private post-exploitation toolkit, designed for espionage and stealthy data theft. Developed in .NET, it operates as a modular implant, avoiding traditional file-based execution by loading its components directly into memory via ModuleInstaller, a backdoor loader named by the attackers. StealerBot features multiple modules for deploying additional malware, capturing screenshots, logging keystrokes, stealing browser passwords and files, phishing Windows credentials, and escalating privileges by bypassing UAC, making it a versatile tool for persistent access and data exfiltration.	Exploiting Vulnerability	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Toolkit			
ASSOCIATED ACTOR			Microsoft Office
			PATCH LINK
SideWinder		System Compromise, Data Theft	https://msrc.micr osoft.com/update -guide/en-US/advisory/CVE-2017-11882
IOC TYPE	**VALUE**		
MD5	3a036a1846bfeceb615101b10c7c910e, 47f51c7f31ab4a0d91a0f4c07b2f99d7, f3058ac120a2ae7807f36899e27784ea		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PureCrypter RAT	PureCrypter is a .NET-based malware loader deeply integrated into the cybercriminal ecosystem, providing advanced evasion techniques and persistent access. Obfuscated using SmartAssembly, it employs compression, encryption, and obfuscation to bypass antivirus detection. Its key capabilities persistence, code injection, and defense mechanisms are configurable via Google's Protocol Buffer message format.	Exploiting Vulnerability	CVE-2024-43451
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT			
ASSOCIATED ACTOR			Microsoft Windows
			PATCH LINK
Blind Eagle		System Compromise	https://msrc.micr osoft.com/update -guide/vulnerabilit y/CVE-2024-43451
IOC TYPE	**VALUE**		
SHA256	3acd90196dcf53dd6e265dc9c89b3cb0c47648a3b7ac8f226c6b4b98f39f2fc8		

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

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

IOC TYPE	VALUE
SHA256	35612c79bde985c957ba521bbc7aa8541c31fb235ca7a91d0ee225f988921eb4, 613fb5ffbce15d7c71a019dd0f80256b2d05772e4f62c2fbf7c74164f1227755

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

IOC TYPE	VALUE
SHA256	d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb

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

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

IOC TYPE	VALUE
SHA256	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404, f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513, 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2

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

🐛 Vulnerabilities Exploited

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

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

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

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

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

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

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

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

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-26633	❌	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✅	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	
Microsoft Management Console Security Feature Bypass Vulnerability	✅		-
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-707	T1553: Subvert Trust Controls; T1204:User Execution; T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709	❌	ConnectWise ScreenConnect	-
	ZERO-DAY		
	❌	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSO MWARE**
NAME	**CISA KEV**	cpe:2.3:a:connectwise:scr eenconnect:*:*:*:*:*:*:*:*	Medusa Ransomware
ConnectWise ScreenConnect Authentication Bypass Vulnerability	✅		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-288	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://www.scree nconnect.com/do wnload

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

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

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

Adversaries in Action

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

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)	Colombia	Government, Judicial Institutions, Private Organizations, Financial, Critical Infrastructure	Colombia
	MOTIVE		
	Information theft and espionage, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSO MWARE**	**AFFECTED PRODUCTS**
	CVE-2024-43451	PureCrypter RAT, Remcos RAT	Microsoft Windows

TTPs
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1587: Develop Capabilities; T1587.004: Exploits; T1588: Obtain Capabilities; T1588.001: Malware; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1546: Event Triggered Execution; T1055: Process Injection; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1140: Deobfuscate/Decode Files or Information; T1573: Encrypted Channel; T1550.002: Pass the Hash

NAME	ORIGIN		TARGETED INDUSTRIES	TARGETED COUNTRIES
	-		All	Worldwide
	MOTIVE			
	Information theft and espionage			
Mora_001	**TARGETED CVEs**	**ASSOCIATED ATTACKS/RANSOMWARE**		**AFFECTED PRODUCTS**
	CVE-2025-24472 CVE-2024-55591	SuperBlack		FortiOS, FortiProxy
TTPs				

TA0004: Privilege Escalation; TA0042: Resource Development; TA0040: Impac; TA0002: Exécution; TA0008: Lateral Movement; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0011: Command and Control; TA0003: Persistences; TA0007: Discovery; T1047: Windows Management Instrumentation; T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpréter; T1210: Exploitation of Remote Services; T1133: External Remote Services; T1556: Modify Authentication Process; T1136.001: Local Account; T1136: Create Account; T1602:Data from Configuration Repository; T1588: Obtain Capabilities; T1588.005: Exploits; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1068: Exploitation for Privilege Escalation; T1098: Account Manipulation; T1486: Data Encrypted for Impact; T1489: Service Stop; T1020: Automated Exfiltration; T1556.001: Domain Controller Authentication

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seventeen exploited vulnerabilities** and block the indicators related to the threat actor **SideWinder, Blind Eagle, Mora_001** and malware **PolarEdge Botnet, SilentCryptoMiner, StealerBot, PureCrypter RAT, Remcos RAT, Medusa Ransomware, SuperBlack.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **seventeen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **SideWinder, Blind Eagle, Mora_001** and malware **PolarEdge Botnet, SilentCryptoMiner, StealerBot, Remcos RAT, Medusa Ransomware** and **SuperBlack** in Breach and Attack Simulation(BAS).

Threat Advisories

Hackers Weaponize CVE-2024-4577 to Deploy Cobalt Strike and Compromise Systems

PolarEdge Botnet Turns Edge Devices Into Cyber Weapons

SilentCryptoMiner Spreading via YouTube Blackmail Scams

SideWinder's Growing Focus on Maritime and Nuclear Entities

Apple Addresses WebKit Zero-Day Exploited in Sophisticated Attacks

Blind Eagle's Cyber Reign: Striking Before You Can Blink

Microsoft's March 2025 Patch Tuesday Fixes Active Zero-Day Exploits

FreeType Under Attack: Critical Font Parsing Flaw Exposes Millions

Medusa Ransomware: A High-Stakes Game of Digital Hostage

New SuperBlack Ransomware Strikes via Fortinet Authentication Bypass

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 threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

⚔ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
PolarEdge Botnet	SHA256	eda7cc5e1781c681afe99bf513fcaf5ae86afbf1d84dfd23aa563b1a043cbba8, 13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13, 464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd, 932b2545bd6e3ad74b82ca2199944edecf9c92ad3f75fce0d07e04ab084824d5, 121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef
	Domains	longlog[.]cc,landim[.]cc, hitchil[.]cc,Logchim[.]cc, ssofhoseuegsgrfnu[.]ru, aipricadd[.]top, firebasesafer[.]top, largeroofs[.]top, siotherlentsearsitech[.]shop, asustordownload[.]com, gardensc[.]cc, headached[.]cc, durianlink[.]cc, nternetd[.]cc,suiteiol[.]cc, centrequ[.]cc, icecreand[.]cc
	IPv4	119[.]8[.]186[.]227, 159[.]138[.]119[.]99, 43[.]129[.]205[.]244, 122[.]8[.]183[.]181, 195[.]123[.]212[.]54

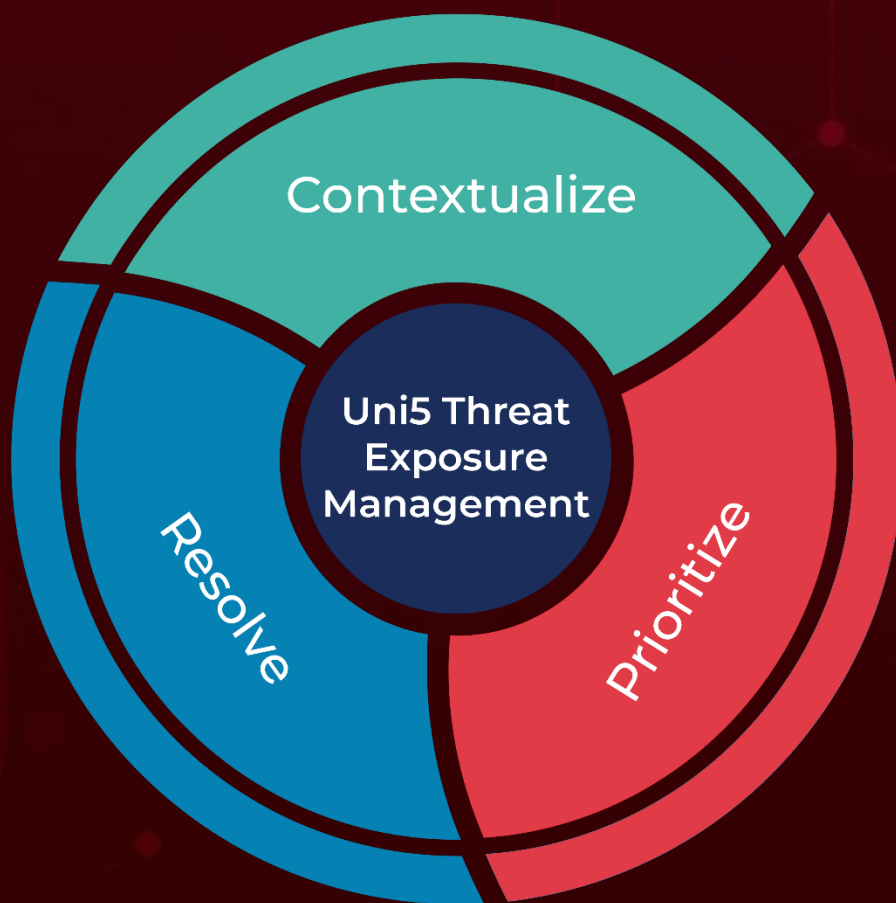| Attack Name	TYPE	VALUE
SilentCryptoMiner	MD5	a2a9eeb3113a3e6958836e8226a8f78f, 5c5c617b53f388176173768ae19952e8, ac5cb1c0be04e68c7aee9a4348b37195
	SHA256	44B212683CDEF95C55DD2E645B414B5179B589C64F1DBD6F5B4252BD4CA59790, 9D93E3AB8D0D9BD84F9F0F9FA2F997DF187CCCE49F9A2BDE7B49AD17E3A3CE08, F5232578BF310696F4E1D89F2A51369EFC32819DAF83A3BE38C3C11962F3A8BE,
StealerBot	MD5	3a036a1846bfeceb615101b10c7c910e, 47f51c7f31ab4a0d91a0f4c07b2f99d7, f3058ac120a2ae7807f36899e27784ea, 0fbb71525d65f0196a9bfbffea285b18, 1ed7ad166567c46f71dc703e55d31c7a, 2f0e150e3d6dbb1624c727d1a641e754, bf16760ee49742225fdb2a73c1bd83c7, b3650a88a50108873fc45ad3c249671a, 4c40fcb2a12f171533fc070464db96d1, eef9c0a9e364b4516a83a92592ffc831
	SHA256	5740947bb9267e1be8281edc31b3fb2d57a71d2c96a47eeeaa6482c0927aa6a4
PureCrypter RAT	SHA256	3acd90196dcf53dd6e265dc9c89b3cb0c47648a3b7ac8f226c6b4b98f39f2fc8
Remcos RAT	SHA256	35612c79bde985c957ba521bbc7aa8541c31fb235ca7a91d0ee225f988921eb4, 613fb5ffbce15d7c71a019dd0f80256b2d05772e4f62c2fbf7c74164f1227755, f28ffdb035e739806d6c9bfc9ef2cd86f7fac2656018c8d0f2706647bcf5332f, 5433726d3912a95552d16b72366eae777f5f34587e1bdaa0c518c5fcbc3d8506
Medusa Ransomware	SHA256	d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, 5f9d864d11c79b34c4502edba7d0e007197d0df086a6fb9d6bfda84a1771ff0f
SuperBlack	SHA256	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404, f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513, 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2, 782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045, d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88

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.

Contextualize

Resolve

Uni5 Threat Exposure Management

Prioritize

More at www.hivepro.com