

Date of Publication
August 24, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors
17 to 23 AUGUST 2026

Table Of Contents

<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	18
<u>Adversaries in Action</u>	25
<u>Recommendations</u>	29
<u>Threat Advisories</u>	30
<u>Appendix</u>	31
<u>What Next?</u>	35

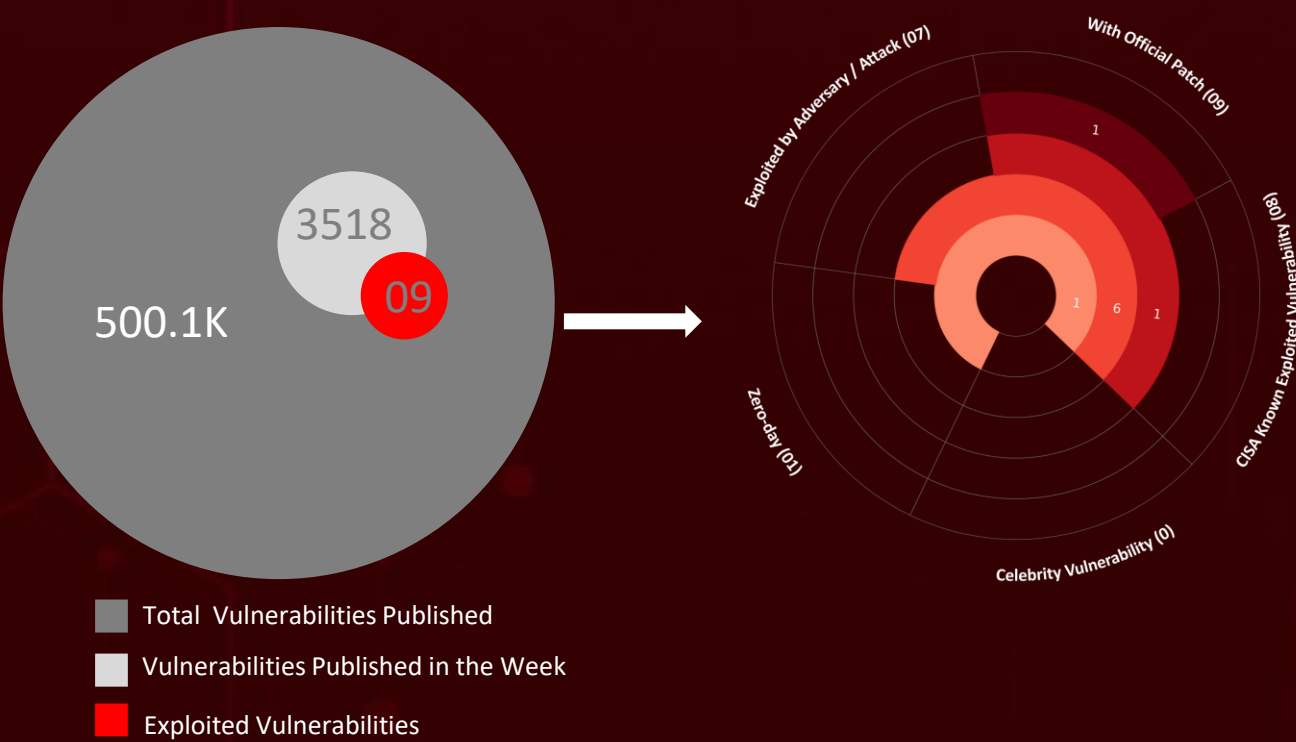
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **twelve** major attacks were detected, **nine** vulnerabilities were actively exploited, and **four** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

On the vulnerability front, three critical flaws dominated the week. Apple addressed **CVE-2026-65400**, a serious authentication bypass in macOS Screen Sharing affecting Sonoma, Sequoia, and Tahoe, though attackers moved quickly, exploiting internet-exposed Screen Sharing ports (TCP 5900) to seize root access and deploy Monero miners even after the patch was released. Separately, MLflow, the popular open-source platform, was found vulnerable to **CVE-2026-64849**, a critical SSRF flaw residing in an unauthenticated webhook-testing endpoint. Meanwhile, VMware vCenter's Syslog server was exposed by **CVE-2026-59310**, a directory traversal bug letting unauthenticated attackers write malicious files and achieve instant root-level code execution.

Threat actor activity was equally alarming. **StopAndProtect**, a sprawling cybercrime operation, has compromised nearly 2,000 poorly secured WordPress sites, repurposing them as a distributed network for malware delivery, command-and-control, and stolen-data storage, luring victims through fake ClickFix CAPTCHA prompts. Meanwhile, **Medusa**, a ransomware-as-a-service group, continues its double-extortion campaigns, having compromised over 500 critical-infrastructure victims across healthcare, education, legal, and manufacturing sectors by August 2026.

Rounding out the week's findings, **Jewelbug**, a China-based hacker-for-hire group, was found running dual operations through a single control panel, XG-Web: state-sponsored espionage against government and military, alongside a parallel cryptocurrency fraud scheme. Collectively, these incidents reflect an intensifying trend toward hybrid cyber operations that blend technical exploitation with social engineering, underscoring the urgent need for prompt patching, vigilant monitoring, and layered security defenses.



High Level Statistics

12

Attacks
Executed

9

Vulnerabilities
Exploited

4

Adversaries in
Action

- [CoolClient](#)
- [PlugX](#)
- [Monero](#)
- [Antino](#)
- [ClientKing](#)
- [XG-Web](#)
- [SilentDataCollector](#)
- [NetworkShareScanner](#)
- [SilentEncryptor](#)
- [Medusa](#)
- [Babuk-derived](#)
- [ESXi ransomware](#)
- [Grandoreiro](#)

- [CVE-2026-12569](#)
- [CVE-2026-65400](#)
- [CVE-2026-64849](#)
- [CVE-2024-1709](#)
- [CVE-2023-48788](#)
- [CVE-2025-10035](#)
- [CVE-2026-1731](#)
- [CVE-2026-59310](#)
- [CVE-2026-59309](#)

- [HoneyMyte](#)
- [Jewelbug](#)
- [Storm-1175](#)
- [Lazarus](#)



Insights

Jewelbug blends state-aligned espionage with for-profit crypto fraud under one roof.

One open port, TCP 5900, was all it took; **CVE-2026-65400** handed attackers root on Macs and a side income mining **Monero**.

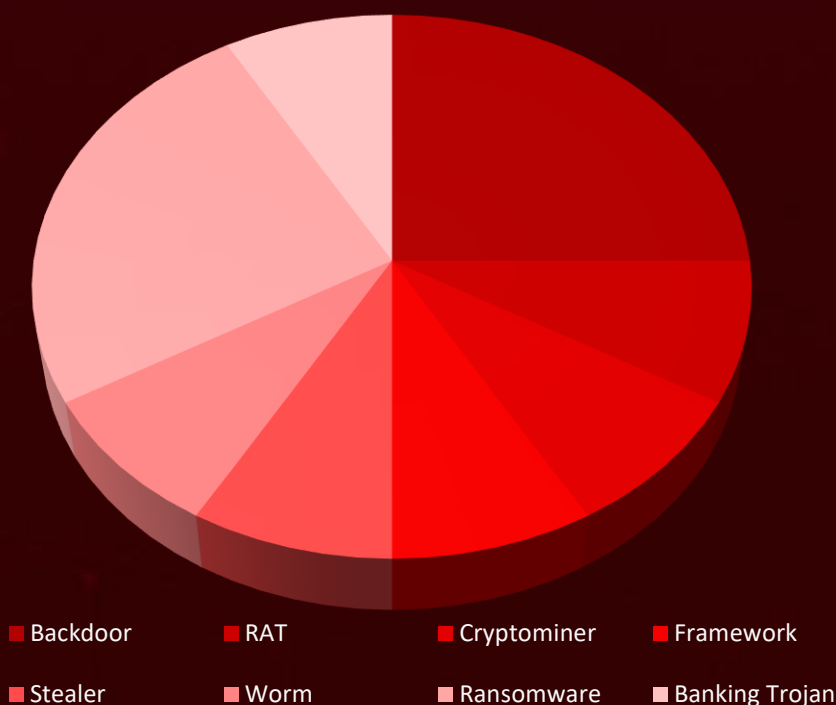
ClOp-linked actors turn exposed **PTC Windchill** and **FlexPLM** into a straight line from disclosure to extortion.

Neglect has a cost: **StopAndProtect** hijacks almost 2,000 unmaintained WordPress sites into a sprawling network for malware delivery and stolen data.

Medusa's leak site went quiet, but the threat didn't. **Storm-1175** simply rebranded its speed and exploit arsenal into StormEncryptor.

No credentials, no waiting; **CVE-2026-59310** hit vCenter's syslog server and, five days later, had already reached 361 IPs in 47 countries.

Threat Distribution



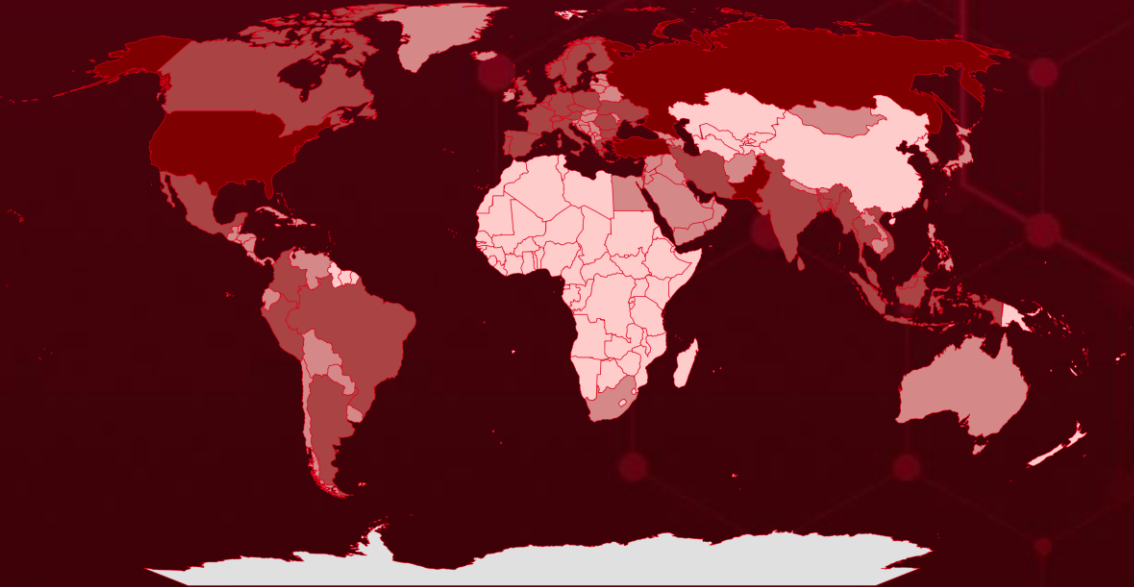


Targeted Countries

Most



Least

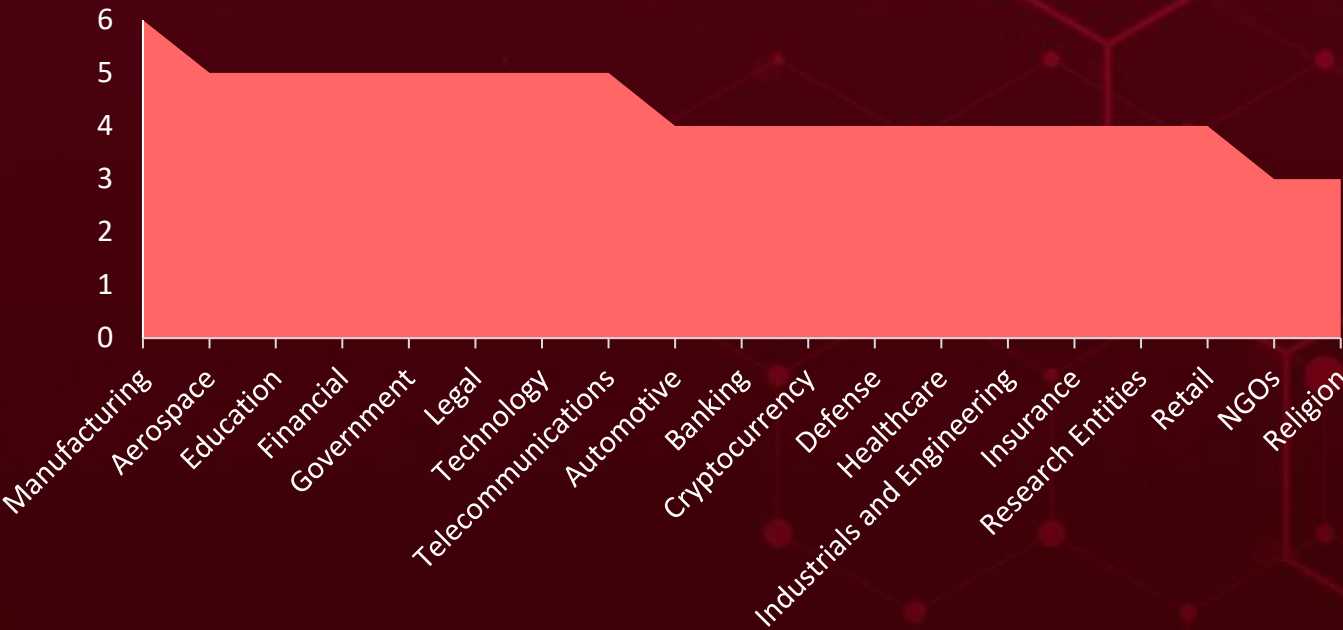


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
Turkey	Germany	Greenland	Bahamas
Russia	Poland	Cambodia	Bosnia and Herzegovina
Pakistan	Greece	Guadeloupe	Ecuador
United States	Romania	Australia	Jamaica
Sweden	India	Guatemala	El Salvador
Peru	Singapore	Saint Maarten	Japan
Myanmar	Indonesia	Haiti	Bahrain
Brazil	Sri Lanka	South Korea	Jordan
Austria	Iran	Honduras	North Macedonia
Bulgaria	Switzerland	Timor-Leste	Venezuela
Bangladesh	Israel	Hong Kong	Oman
Canada	Thailand	Uruguay	Yemen
Norway	United Kingdom	Hungary	Palestine
Colombia	Ukraine	Aruba	Laos
Portugal	Malaysia	Iceland	Paraguay
Cyprus	Mexico	Chile	Latvia
Spain	Italy	Belize	Philippines
Czech Republic	Vietnam	Puerto Rico	Afghanistan
Taiwan	Albania	Bermuda	Costa Rica
Denmark	Panama	Cuba	Liechtenstein
Belgium	Estonia	Bhutan	Qatar
Finland	Belarus	Saudi Arabia	
Netherlands	Republic of Ireland	Iraq	
France	Anguilla	Slovenia	
Argentina	Dominican Republic		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1071 Application Layer Protocol	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1071.001 Web Protocols	T1082 System Information Discovery
T1036 Masquerading	T1105 Ingress Tool Transfer	T1027 Obfuscated Files or Information	T1505 Server Software Component	T1083 File and Directory Discovery
T1070 Indicator Removal	T1056 Input Capture	T1564 Hide Artifacts	T1505.003 Web Shell	T1021 Remote Services
T1572 Protocol Tunneling	T1588 Obtain Capabilities	T1113 Screen Capture	T1486 Data Encrypted for Impact	T1219 Remote Access Software

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CoolClient	CoolClient is a backdoor family attributed to the HoneyMyte APT group, and it has kept evolving over time. A 2025 variant added clipboard theft and HTTP traffic interception for harvesting credentials. The newest version can deploy a signed kernel-mode driver as a Windows service and talk to it through IOCTL requests. That driver boosts the malware's stealth by hiding the CoolClient process and shielding its files and registry entries from inspection or modification. The overall design resembles the kernel-mode enhancements previously seen in ToneShell, but the CoolClient driver adds dedicated IOCTL handlers that let the user-mode backdoor communicate directly with the driver.	Through PlugX infection	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
HoneyMyte			-
IOC TYPE	VALUE		
SHA256	ee72ae4cc869affddab11647e95bab9c5691c9fc76dcb4b31650ff504da29156		

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
PlugX	PlugX is a remote access trojan (RAT) that has been around since 2008, used as a backdoor to take full control of a victim's machine. Once a device is infected, the attacker can remotely run a wide range of commands, pulling machine information, capturing the screen, sending keyboard and mouse events, keylogging, rebooting the system, managing processes (creating, killing, and listing them), managing services (create, start, stop, and so on), editing Windows registry entries, opening a shell, and more. It also records its own activity in a text log file.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Keylogging, screen capture, system compromise	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
HoneyMyte			-
IOC TYPE	VALUE		
SHA256	d247570da6646a9d66d094090d71a59e6b06e0c31c7346d3d4fbadddef90a887, 25c2e47b5663f4b414c02671bfe849bca588d8992cd643af8a411557fa5e3f1e		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Monero</u>	Monero, a privacy- focused cryptocurrency, has become a magnet for cryptominers, both legitimate and malicious. The lure lies in its unique mining algorithm, RandomX, designed to be resistant to specialized hardware (ASICs) and favor consumer-grade CPUs and GPUs.	Exploiting Vulnerability	CVE-2026-65400
TYPE		IMPACT	AFFECTED PLATFORM
Cryptominer		Data Theft	Apple macOS Sonoma, macOS Sequoia, macOS Tahoe
ASSOCIATED ACTOR			PATCH LINKS
-			https://support.apple.com/en-us/148170 , https://support.apple.com/en-us/148171 , https://support.apple.com/en-us/148172
IOC TYPE	VALUE		
SHA256	657fe4474fd1788c2910fb3fc4e2e8ed85ea4598638c4b38811bbbf4090a3999, 4f4e99c6e30bc5ce997aa398ab131ecc3e969eb78211de93d32174575e4d998e		

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
Antino	Antino is the group's Windows backdoor. It is the payload dropped by a wave of malicious HTML Application (HTA) downloaders that use current geopolitical events as lures, the activity that prompted this investigation. Antino is also delivered as a fake Adobe Flash or Adobe installer, using file names such as flashcenter_pp_ax_install_en.exe and Adobeinstall.exe, downloaded from domains the group controls.	Trojanized Installers	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Persistent foothold, Credential theft	Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-
IOC TYPE	VALUE		
SHA256	09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff, c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ClientKing	ClientKing is a Rust-based backdoor/implant, bundled with a kernel-mode rootkit and a credential-stealing authentication module. Unlike the browser tooling, ClientKing targets servers and network devices. It supports five command-and-control (C&C) transports, one of which is a custom DNS tunnel. It gives the operator a full interactive shell, SOCKS pivoting, and the ability to load kernel modules straight from memory.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Persistent foothold, Credential theft	Linux, x86-64 servers, ARM64 devices
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XG-Web</u>	XG-Web is the single control panel behind Jewelbug's espionage and cryptocurrency-fraud operations. It is built as a React front end over a Node.js backend, with a MySQL database that doubles as the rendezvous point for victim implants. Its developers describe it in their own documentation as a "penetration-testing platform," but internal function names include browser hijacking, data theft, and a man-in-the-middle attack. The framework turns a victim's browser into a full remote-control channel and reaches from there into the host and the internal network behind it.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Framework		Data exfiltration, Command execution	Windows, Google Chrome, Mozilla Firefox
ASSOCIATED ACTOR			PATCH LINK
Jewelbug			-

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
SilentDataCollector	SilentDataCollector is a stealer that builds a list of every file across all drives, fixed, removable, and network, then encrypts that list and sends it to the base command-and-control (C&C) server. The operator can steer file collection by uploading a command file to the C&C, which the stealer reads before compressing, encrypting, and exfiltrating the requested files back to the same server.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Steal Data	Windows, WordPress
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	23cbabfe3ca3a7f1eb365f772d6a4ed8095cb8f7755622cc82e804478259dc70		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
NetworkShareScanner	NetworkShareScanner acts as an SMB/USB worm, enumerating network shares and plugged-in USB devices to spread beyond the machine it first infected.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Worm		System disruption	Windows, WordPress
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	8d1e23630a6695fa9c793d73832f59436c98bba30ed81c16d01b549bd17feab4, 10babb15e08f9fbd72cce11713a273b971c910dd5bdb989a3f6ff4d9c8e372c0		

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
SilentEncryptor	SilentEncryptor is the ransomware component. It downloads a command file from the base C&C that tells it whether to encrypt every infected computer or only those with specific hostnames, and it also carries the ransom message shown to the victim. Its key derivation function combines a per-file password with the machine name to produce a 32-byte key, and since both the per-file password and machine name are embedded in the encrypted file's renamed filename, decryption of the files is possible.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Encrypt Data, Data theft	Windows, WordPress
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	b79b9b027f76579555069a7506d946648a8cb3126c0dda837dc9fee0e5c79489, 65550f6d0ffec8421f703cdc7273d9c0563b3d480fe6702bad294a18afe72143		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Medusa</u>	Medusa is a RaaS operation (since June 2021) running double/triple-extortion against critical infrastructure, distinct from MedusaLocker. Core operation dormant since mid-Feb 2026; lead affiliate has pivoted to StormEncryptor.	Exploiting Vulnerability	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Encryption, data theft/extortion	ScreenConnect, FortiClient EMS, GoAnywhere MFT, BeyondTrust RS/PRA
ASSOCIATED ACTOR			PATCH LINKS
Storm-1175, Lazarus			https://www.screencconnect.com/download , https://fortiguard.fortinet.com/psirt/FG-IR-24-007 , https://www.fortra.com/security/advisories/product-security/fi-2025-012 , https://www.beyondtrust.com/trust-center/security-advisories/bt26-02
IOC TYPE	VALUE		
SHA256	0cefeb6210b7103fd32b996beff518c9b6e1691a97bb1cda7f5fb57905c4be96, 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Babuk-derived ESXi ransomware</u>	This is a Babuk-derived ESXi encryptor deployed as the final stage of a global campaign against internet-facing VMware vCenter. After gaining root on the vCenter Server Appliance, the actor harvested vmdir machine credentials, created SSO administrator accounts, and pushed the encryptor to a datastore shared by all ESXi hosts.	Exploiting Vulnerability	CVE-2026-59310
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data encryption, Service disruption, Log destruction	VMware vCenter Server, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure
ASSOCIATED ACTOR			PATCH LINK
-			https://support.broadcom.com/web/ecx/suport-content-notification/-/external/content/SecurityAdvisories/0/38017

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
Grandoreiro	Grandoreiro is a Brazilian-origin banking trojan written in Delphi, active across Latin America since at least 2016 against financial institutions and their customers. In this May 2026 campaign the operators abuse Duplicate Files Finder for DLL sideloading, so malicious code executes inside a trusted, signed application. The loader is lightweight in function but heavily defended: it hides the host application's GUI window, then runs extensive anti-analysis checks before ever contacting its C2 system uptime below three minutes, desktop shortcuts for a specific seven-application set, VMware and VirtualBox drivers, BIOS registry keywords, 49 blacklisted analyst and EDR process names, blacklisted usernames and hostnames, and analyst tool directories.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Banking Trojan		Banking fraud, System profiling, Payload delivery	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1b2fe30c5bf57f9623efb34688580fe5bbb2c55351c5a07a6c4313bb6faa29f1, 1fe5a72aefc38afeeee72d8a939f9db50800a447b7313f4d8c504771bb7fa2de		

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 PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-12569</u>		PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030	ClOp
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ptc:windchill_pdmlink:*:*:*:*:*:* *; cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*	-
PTC Windchill and FlexPLM Improper Input Validation Vulnerability		ASSOCIATED TTPs	PATCH LINKS
	CWE-502, CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.ptc.com/en/support/article/CS473270 , https://support.ptc.com/appserver/common/login/ssl/login.jsp?dest=%2Fappserver%2Fcss%2Fview%2Fsolution.jsp%3Fn%3DCS473270&msg=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-65400</u>		Apple macOS Sonoma (Before 14.8.9), macOS Sequoia (Before 15.7.9), macOS Tahoe (Before 26.6.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:apple:macos:*:*:*:*:*:*	Monero Miner
Apple macOS Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1496: Resource Hijacking	https://support.apple.com/en-us/148170 , https://support.apple.com/en-us/148171 , https://support.apple.com/en-us/148172

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-64849</u>		MLflow (Before 3.15.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:mlflow:mlflow:*:*:*:*:*	-
MLflow Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://github.com/mlflow/mlflow/releases/#release-v3.15.1 , https://github.com/mlflow/mlflow/releases/tag/v3.15.0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-1709</u>		ConnectWise ScreenConnect	Storm-1175
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:connectwise:screenco nnect:*:*:*:*:*:*	Medusa
ConnectWise ScreenConnect Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1072: Software Deployment Tools	https://www.screencnect.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-48788</u>		Fortinet FortiClient EMS	Storm-1175
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:forticlient_ent erprise_management_server:*:* .*.*.*.*.*.*	Medusa
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1505.003: Web Shell, T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-10035</u>		Fortra GoAnywhere MFT	Storm-1175
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*	Medusa
Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77, CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.fortra.com/security/advisories/product-security/fi-2025-012

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-1731</u>		BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	Storm-1175
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*	Medusa
BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Web Shell	https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-59310</u>		VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*	Babuk-derived ESXi ransomware
Broadcom VMware vCenter Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1053: Scheduled Task/Job, T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-59309</u>		VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Broadcom VMware vCenter Authentication Bypass Vulnerability		cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-303	T1595: Active Scanning, T1136: Create Account, T1036: Masquerading	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>HoneyMyte (aka Mustang Panda, Bronze President, TEMP.Hex, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)</u>	China	Government	Myanmar, Mongolia, Pakistan, Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	CoolClient, PlugX	Microsoft Windows
TTPs			
TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0009: Collection, TA0007: Discovery, TA0011: Command and Control, T1569: System Services, T1569.002: Service Execution, T1106: Native API, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1543: Create or Modify System Process, T1543.003: Windows Service, T1548: Abuse Elevation Control Mechanism, T1548.002: Bypass User Account Control, T1134: Access Token Manipulation, T1134.004: Parent PID Spoofing, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1014: Rootkit, T1055: Process Injection, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1553: Subvert Trust Controls, T1553.002: Code Signing, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1112: Modify Registry, T1564: Hide Artifacts, T1070: Indicator Removal, T1070.004: File Deletion, T1056: Input Capture, T1056.001: Keylogging, T1115: Clipboard Data, T1005: Data from Local System, T1057: Process Discovery, T1082: System Information Discovery, T1071: Application Layer Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Jewelbug (Earth Alux, REF7707, CL-STA-0049, Ink Dragon)</u>	China	Government, Military, Defense, Law Enforcement, Telecommunications, Aerospace, Industrial Manufacturing, Web Hosting Services, Cryptocurrency	Middle East, Southeast Asia, South Asia, Taiwan, United States
	MOTIVE		
	Espionage and Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Antino, ClientKing, XG-Web	Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers

TTPs

TA0043: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1587: Develop Capabilities; T1608: Stage Capabilities; T1189: Drive-by Compromise; T1566: Phishing; T1078: Valid Accounts; T1204: User Execution; T1059: Command and Scripting Interpreter; T1176: Software Extensions; T1556: Modify Authentication Process; T1547: Boot or Logon Autostart Execution; T1112: Modify Registry; T1014: Rootkit; T1027: Obfuscated Files or Information; T1036: Masquerading; T1218: System Binary Proxy Execution; T1539: Steal Web Session Cookie; T1056: Input Capture; T1185: Browser Session Hijacking; T1217: Browser Information Discovery; T1082: System Information Discovery; T1550: Use Alternate Authentication Material; T1114: Email Collection; T1113: Screen Capture; T1115: Clipboard Data; T1557: Adversary-in-the-Middle; T1074: Data Staged; T1102: Web Service; T1071: Application Layer Protocol; T1572: Protocol Tunneling; T1090: Proxy; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1583.001: Domains; T1583.006: Web Services; T1584.004: Server; T1587.001: Malware; T1608.001: Upload Malware; T1608.004: Drive-by Target; T1608.006: SEO Poisoning; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204.001: Malicious Link; T1059.007: JavaScript; T1059.003: Windows Command Shell; T1176.001: Browser Extensions; T1556.003: Pluggable Authentication Modules; T1547.006: Kernel Modules and Extensions; T1027.013: Encrypted/Encoded File; T1036.005: Match Legitimate Resource Name or Location; T1218.005: Mshta; T1056.003: Web Portal Capture; T1550.004: Web Session Cookie; T1114.002: Remote Email Collection; T1074.002: Remote Data Staging; T1102.001: Dead Drop Resolver; T1102.002: Bidirectional Communication; T1071.001: Web Protocols; T1071.004: DNS; T1090.001: Internal Proxy

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-1175	-	Healthcare, education, professional services, finance, legal, insurance, technology, manufacturing	Global
	MOTIVE		
	Espionage and Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2024-1709 CVE-2023-48788 CVE-2025-10035 CVE-2026-1731	Medusa ransomware	Windows and Linux
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0010: Exfiltration, TA0011: Command and Control, TA0040: Impact, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1569: System Services, T1072: Software Deployment Tools, T1505: Server Software Component, T1484: Domain or Tenant Policy Modification, T1562: Impair Defenses, T1036: Masquerading, T1003: OS Credential Dumping, T1555: Credentials from Password Stores, T1046: Network Service Discovery, T1018: Remote System Discovery, T1021: Remote Services, T1570: Lateral Tool Transfer, T1105: Ingress Tool Transfer, T1572: Protocol Tunneling, T1219: Remote Access Software, T1567: Exfiltration Over Web Service, T1486: Data Encrypted for Impact, T1490: Inhibit System Recovery, T1489: Service Stop, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1569.002: Service Execution, T1505.003: Web Shell, T1484.001: Group Policy Modification, T1562.001: Disable or Modify Tools, T1003.001: LSASS Memory, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1567.002: Exfiltration to Cloud Storage			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, TraderTraitor, Gleaming Pisces, Slow Pisces, G0032)</u>	MOTIVE	Healthcare, education, professional services, finance, legal, insurance, technology, manufacturing	Global
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Medusa ransomware	Windows and Linux

TTPs
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011:Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1584: Compromise Infrastructure, T1584.004: Server, T1608: Stage Capabilities, T1608.001: Upload Malware, T1608.006: SEO Poisoning, T1586: Compromise Accounts, T1586.002: Email Accounts, T1566: Phishing, T1566.003: Spearphishing via Service, T1566.001: Spearphishing Attachment, T1190: Exploit Public-Facing Application, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1505: Server Software Component, T1505.003: Web Shell, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1014: Rootkit, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1055: Process Injection, T1055.001: Dynamic-link Library Injection, T1684: Social Engineering, T1684.001: Impersonation, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, T1070: Indicator Removal, T1070.004: File Deletion, T1078: Valid Accounts, T1057: Process Discovery, T1082: System Information Discovery, T1113: Screen Capture, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1102: Web Service, T1041: Exfiltration Over C2 Channel

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **HoneyMyte, Jewelbug, Storm-1175, Lazarus**, and malware **CoolClient, PlugX, Monero, Antino, ClientKing, XG-Web, SilentDataCollector, NetworkShareScanner, SilentEncryptor, Medusa, Babuk-derived ESXi ransomware**, and **Grandoreiro**.

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

- Run a Scan to discover the assets impacted by the **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **HoneyMyte, Jewelbug, Lazarus**, and malware **CoolClient, Antino Backdoor, NetworkShareScanner, SilentEncryptor, Grandoreiro** in Breach and Attack Simulation(BAS).

Threat Advisories

[CI0p-Linked Actors Exploit PTC Windchill and FlexPLM in Data Theft Campaign](#)

[HoneyMyte Arms CoolClient with a Signed Kernel-Mode Rootkit](#)

[macOS Screen Sharing Authentication Bypass Flaw Exploited](#)

[One Team, Two Payrolls: Jewelbug's Parallel Operations](#)

[MLflow SSRF Flaw \(CVE-2026-64849\) Hands Attackers Your Cloud Credentials](#)

[StopAndProtect: Nearly 2,000 Hacked WordPress Sites Weaponized as Criminal Infrastructure](#)

[Medusa Ransomware: RaaS Escalating Double-Extortion Attacks on Critical Infra](#)

[Suspected China-Nexus APT Weaponizes CVE-2026-59310](#)

[Grandoreiro Outlives Its Own Takedown](#)

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
CoolClient	SHA256	ee72ae4cc869affddab11647e95bab9c5691c9fc76dcb4b31650ff504da29156
PlugX	SHA256	d247570da6646a9d66d094090d71a59e6b06e0c31c7346d3d4fbadddef90a887, 25c2e47b5663f4b414c02671bfe849bca588d8992cd643af8a411557fa5e3f1e, f2f0d2062eb1a181e1669456f077ef4e913750cb5b2a97c3c7668afedca a6961, 91753cefea41f924951a6d441179a0f97b902ae30b7b1fd04b601d266d ba435e, d9529976ce67da55a0f1a561ff4fb7e6535bfc7b607c838182752fd6e673 2794, 64b9f35206cb8ad0b79a07dad35acf024d2d429855352674f3fecc0798b 96cfd, 1f8a2658aeabcfecce2fe37978ccbcddfee8045e23ed5f069b4c1743acad 4ccd, ce44171fbacb22d86c61f4c4c47ffb0fca380c96dd1894522ee465e39d72 dcec, dc4558efd0113791cbccc363a89a71b3170b71b82065b464a91832488e 792ee3

Attack Name	TYPE	VALUE
<u>Monero</u>	SHA256	657fe4474fd1788c2910fb3fc4e2e8ed85ea4598638c4b38811bbbf4090a3999, 4f4e99c6e30bc5ce997aa398ab131ecc3e969eb78211de93d32174575e4d998e, 459655bcc84a8239a65300ea61fd44a16f4a7df3cbf011a675646560c2cc0d5d, c20e89caf440d8b3b9b1da8c9467ab6aaea9a17a79a2169f89f07b1a603cb422, 66871e7a931ce86c90fc19cacb47a91fd fba9d3d214369657497ced2a77f2f4f, c05a6df ee8a914f64c75dfb4fa2bae9e8aa8214b5921faa1b3c275c7a3b79be6, 8bf1ae207338b8cd2f3ec202cef0285d09041f94ebdd5ae6c2edfe8ad59f06b1, 60033b1bda21c6d2a70d7e3829d76a44fdc45087ba27b0e6fe01b54f0c968180
<u>Antino</u>	SHA256	09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff, c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc, 153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0dc22d3bb5c94e, 297413a3e49e7353bf484a3eb15ec647de729211059df8fc68678d2378b6f561, 30f5122cc199b9c2e524503b343a9ee13a6f9773dcbcb1df82c8b25ad20bca61d, 430f12970f8d58f12edccee9019a1aa90fa232c961449bdcc69c8d348a52cf55, 5ccdf53881f6c758af8d94fe67066af209b4bc0a3cb80b6a4c724fad86eb97ef, 5edb8d1023b8babf302871b68fa2b26d5ca57633f64951922998e8f1d6c8f7ac, 6d5fe6b6a34eeb470798b970b70f41a07ccf59b22f49ad9b3dfff7aa3256f3c2, 97c3a6be1711c5340d8806e4a54f7297f3f763d0aa4240b667f1e4e1f98f2aad, ac3d453d3c9b0310ebb8a67cef35e2ac954d4acdf70cf497fe43a02c7a510813, e782a6d4919f194d41e524ebd6df5894197043cf772fcf60455127b246f302c0, ea893abf20b00d9bfc042a88fbf7b4bd42e68ce07c116d3e3b002e5b4a853877, ed96e7f1085a50251eb8967ac53777272a617831084f0edad8a769c583a18869

Attack Name	TYPE	VALUE
<u>SilentDataCollector</u>	SHA256	23cbabfe3ca3a7f1eb365f772d6a4ed8095cb8f7755622cc82e804478259dc70
<u>NetworkShareScanner</u>	SHA256	8d1e23630a6695fa9c793d73832f59436c98bba30ed81c16d01b549bd17feab4, 10babb15e08f9bd72cce11713a273b971c910dd5bdb989a3f6ff4d9c8e372c0, f042240c3de00c46dee625916bf246b7e87481e4081a6a97208b091409766e41
<u>SilentEncryptor</u>	SHA256	b79b9b027f76579555069a7506d946648a8cb3126c0dda837dc9fee0e5c79489, 65550f6d0ffec8421f703cdc7273d9c0563b3d480fe6702bad294a18afe72143, 0080d0dd72eda4850a02e51c0e5c6f768423dfe970cafae2ab52ceee75972b40
<u>Medusa</u>	Email	key[.]medusa[.]serviceteam[.]protonmail[.]com, medusa[.]support[.]onionmail[.]org, mds[.]svt[.]breach[.]protonmail[.]com, mds[.]svt[.]mir2[.]protonmail[.]com, MedusaSupport[.]cock[.]li
	SHA256	0cefeb6210b7103fd32b996beff518c9b6e1691a97bb1cda7f5fb57905c4be96, 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c, e57ba1a4e323094ca9d747bfb3304bd12f3ea3be5e2ee785a3e656c3ab1e8086, 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19, 56b08aa03bd8c0ea094cfef03d5954ffd857bac42df929dc835eea62f32b09e0, a5a3c3c4fbf5c7db808176db3242c2106995c85f8ba987472ea0e92e59503b55, d3abd4bae082d4c9918447fe82c521567cc7f9b0e5f2d55999a6e5c40fa7fd54, 7ffce7f6d7262f214d78e6b7fd8d07119835cba4b04ce334260665d7c8fb369a, b29defbbc4ebaa243c1712ccc4943374f1b6fb864c39ed9f70fceb17eee098db, 04b13b6cd5e5291b1cde78975a140feea7fd3bc3777c53caa1ab33426c83bfcc

Attack Name	TYPE	VALUE
<u>Grandoreir</u> <u>o</u>	SHA256	1b2fe30c5bf57f9623efb34688580fe5bbb2c55351c5a07a6c4313bb6faa29f1, 1fe5a72aefc38afeeee72d8a939f9db50800a447b7313f4d8c504771bb7fa2de, 2820a2e36f1cb537a7853fde2313a5158d1e3696ff81c3066ec8fe274358c22d, 368246eb503585f26e0151431909792b8d9be0edc229bb207be882bfb374c005, 37492ecd9deb8591ea7e179ebb8e13c6b486cdacae18a6a482d9dd18f08453a3, 47d5a73b220813299f753ef0a96582a8d08b853391864128a1f15271dbb42e65, 609755a8c73e53f332428786c366323b3979850aaa0e075d946e6c05aa62f867, 65db035f79db85ad66fb3e0365e478f95f8f648545b18360d850a7ed179c9dab, 684f5eb157ef2ba3ea17335d6c8c9c801f93e6eb3aa08ecbfaf5806a4b5e3b80, a91c7cb932301454df4b0feed58082cae7f2d0e4078d7e6df3f53d806ed04f1d, 90254c3baec79cf9b448836293d3864ee273c30de374933296c6e8e3bcaefdbd, ad5762fa98da2aff24d9d6b55be5dae21d07c54679ead67252a19c2521162a87, c019cfa9b50a69ff07e98bd78b3a6fc489110e5db1c0d79ada716605a2320951, ca33f5608b72ecca64a002074a4103c7cb83de902ecf5c69949eeeb7eef03b5a, cc238813ab277cbb4324d37875c37985ca5baeaf8c412b4c85aa8ec5faec7096, e0491eddb45425a674e479b2590517ffef2f108add431761bb89791fc208b6e9, e99416ff71e4574de4fceeabdc34f3b9a6e0610f36b77b735b231bd39edb7a0a1

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 demo of HivePro.

REPORT GENERATED ON

August 24, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com