Hive Pro

Threat Level

Red

CISA: AA25-071A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

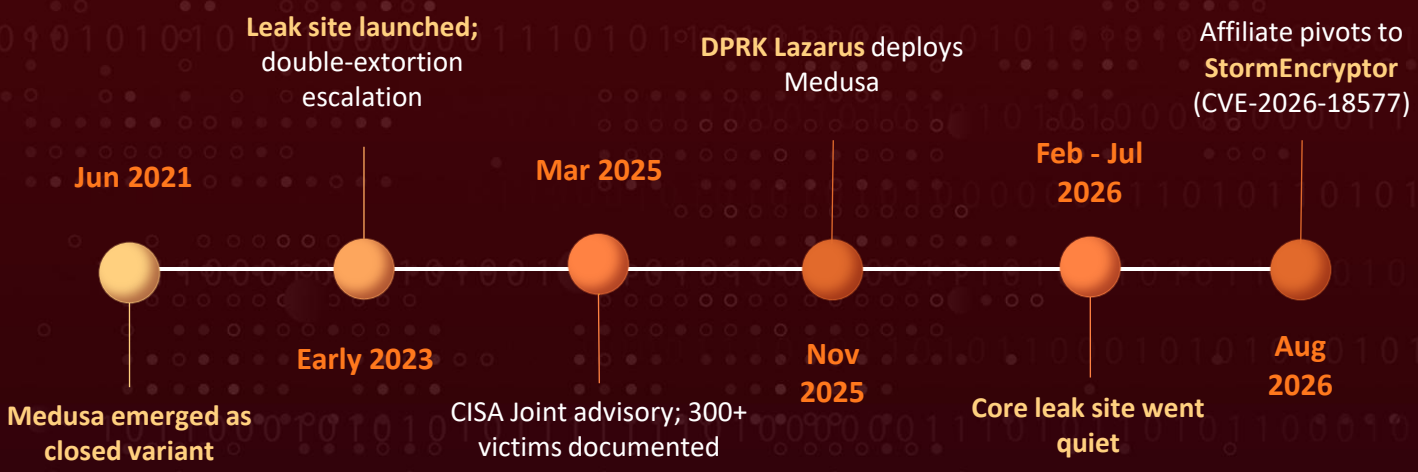
Medusa Ransomware: RaaS Escalating Double-Extortion Attacks on Critical Infra

Date of Publication	Admiralty Code	TA Number
August 20, 2026	A1	TA2026240

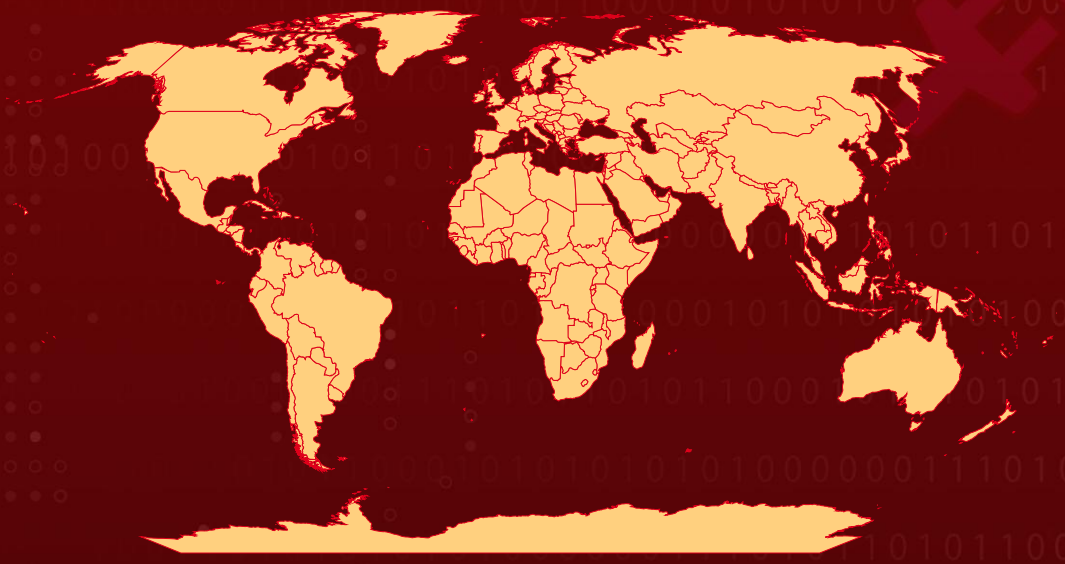
Summary

First Seen: June 2021
Targeted Regions: Global (Primarily United States critical infrastructure)
Targeted Platforms: Windows and Linux
Targeted Industries: Healthcare, education, professional services, finance, legal, insurance, technology, manufacturing
Threat Actor: Storm-1175 (Medusa affiliate), 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)
Malware: Medusa ransomware
Attack: Medusa is a ransomware-as-a-service operation first identified in June 2021, distinct from the MedusaLocker and Medusa mobile malware families, that runs double-extortion attacks, encrypting and stealing data before threatening to leak it, and was linked to over 500 critical-infrastructure victims across healthcare, education, legal, and manufacturing by August 2026. Its operators pair centrally controlled negotiation with an affiliate model, and the affiliate Storm-1175 stands out for weaponizing 16-plus internet-facing vulnerabilities since 2023, and moving from initial access to deployment in as little as 24 hours. The core leak site has been quiet since mid-February 2026, and that same affiliate has since shifted toward a new strain, StormEncryptor. Overall, Medusa exemplifies the convergence of criminal RaaS with fast, state-adjacent exploit capability.

Ransomware Timeline



Attack Regions



Targeted Non-Targeted

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS	✗	✓	✓
CVE-2025-10035	Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	✗	✓	✓

Attack Details

#1 Medusa emerged in June 2021 as a ransomware-as-a-service (RaaS) operation, distinct from the similarly named MedusaLocker and the Medusa mobile malware. It began as a closed variant, with a single group controlling development and operations, before adopting an affiliate model, though core functions such as ransom negotiation stayed centrally controlled by the developers.

#2 The operation runs on double extortion: data is encrypted and simultaneously stolen, with threats to publish it on a dark-web leak site. Victims are typically given 48 hours to respond and can pay to add time to the countdown. Investigators also documented a triple-extortion twist, in which a victim who had already paid was approached again by a separate actor demanding further payment for a working decryptor. By early 2025, Medusa had grown into a serious critical-infrastructure threat. As of August 2026 it was linked to more than 500 victims across sectors including healthcare, education, legal, insurance, technology, and manufacturing.

#3 Its most notable recent chapter involves an affiliate tracked as Storm-1175. Assessed as financially motivated and China-linked, though whether that reflects direct state support, exploit-broker procurement, or informal ties to a national vulnerability-research ecosystem remains an open question, it stands apart by weaponizing internet-facing vulnerabilities at extreme speed. Since 2023 it has exploited more than 16 flaws across managed file transfer, mail, remote-access, and gateway products, including at least one as zero-day (CVE-2025-10035). In the fastest cases it moves from initial access to ransomware deployment within 24 hours, though most intrusions run five to six days.

#4 Technically, operators blend living-off-the-land techniques with legitimate remote-monitoring software and tunneling utilities to move quietly, harvest credentials, and exfiltrate data to attacker-controlled cloud storage before deployment. The payload appends a .medusa extension, and the encryptor is designed to disable security tools and delete backups to frustrate recovery.

#5 Medusa now exemplifies the convergence of criminal RaaS with state-adjacent exploit capability, its affiliate roster spanning both criminal and state-aligned actors. The core leak site has been quiet since mid-February 2026. Most recently the same affiliate was seen shifting away from Medusa toward a new strain, StormEncryptor, distinguished by a .encrypted extension and a different ransom-note name, after likely exploiting a remote-management authentication-bypass flaw (CVE-2026-18577). The pattern is a reminder that the platform and its operators keep evolving.

Recommendations

Patch Medusa's Exploited Web-Facing Products: Treat as an emergency any exposure in the products tied to Medusa initial access, Fortra GoAnywhere MFT (CVE-2025-10035), Fortinet FortiClient EMS (CVE-2023-48788), ConnectWise ScreenConnect (CVE-2024-1709), and BeyondTrust Remote Support/Privileged Remote Access (CVE-2026-1731), all four of which are listed in the Known Exploited Vulnerabilities catalog. Prioritize these for immediate patching, and continue to monitor the Known Exploited Vulnerabilities catalog for any newly added Medusa-associated vulnerabilities.

Isolate and Shield Internet-Facing Systems: Place managed file transfer, email, and remote-access appliances behind a VPN, web application firewall, reverse proxy, or DMZ; where a system cannot be patched immediately, restrict access or take it offline until it can be remediated.

Block and Hunt for the Known Indicators: Ingest the Medusa/Storm-1175 hashes, IP addresses, ransom-note filenames, and negotiation email addresses in this advisory into EDR, SIEM, and firewall tooling, treating the shared Rclone hash (9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c) as lower-fidelity given its documented reuse across multiple threat actors since 2024.

Enforce MFA and Least Privilege: Require multifactor authentication on webmail, VPNs, RMM consoles, and all privileged accounts, and constrain local-administrator rights to blunt LSASS dumping and registry-based credential caching, both of which require elevated privileges.

Enable Tamper Protection and Antivirus Hardening: Turn on tenant-wide tamper protection and the DisableLocalAdminMerge setting to prevent attackers from disabling Microsoft Defender or adding exclusions, and enable attack-surface-reduction rules covering LSASS credential theft, obfuscated scripts, web shell creation, and process creation from PsExec/WMI.

Maintain Offline, Immutable Backups: Follow the 3-2-1 backup rule with at least one offline or immutable copy stored off-site under separate credentials, and routinely test restoration to ensure recovery without paying a ransom.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1569: System Services	T1569.002: Service Execution
	T1047: Windows Management Instrumentation	
	T1072: Software Deployment Tools	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Persistence	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
Privilege Escalation	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1070: Indicator Removal	T1070.003: Clear Command History
	T1006: Direct Volume Access	

Tactic	Technique	Sub-technique
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1112: Modify Registry	
	T1036: Masquerading	
	T1564: Hide Artifacts	T1564.012: File/Path Exclusions
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.003: NTDS
		T1003.002: Security Account Manager
	T1555: Credentials from Password Stores	
	T1558: Steal or Forge Kerberos Tickets	
Discovery	T1046: Network Service Discovery	
	T1083: File and Directory Discovery	
	T1135: Network Share Discovery	
	T1033: System Owner/User Discovery	
	T1049: System Network Connections Discovery	
	T1082: System Information Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1482: Domain Trust Discovery	
	T1018: Remote System Discovery	

Tactic	Technique	Sub-technique
Lateral Movement	T1021.001: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
Command and Control	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
	T1219: Remote Access Software	
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1529: System Shutdown/Reboot	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0cefeb6210b7103fd32b996beff518c9b6e1691a97bb1cda7f5fb57905c4be96, 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c, e57ba1a4e323094ca9d747bfb3304bd12f3ea3be5e2ee785a3e656c3ab1e8086, 5ba7de7d5115789b952d9b1c6cff440c9128f438de933ff9044a68fff8496d19, 56b08aa03bd8c0ea094cfeb03d5954ffd857bac42df929dc835eea62f32b09e0, a5a3c3c4fbf5c7db808176db3242c2106995c85f8ba987472ea0e92e59503b55, d3abd4bae082d4c9918447fe82c521567cc7f9b0e5f2d55999a6e5c40fa7fd54, 7ffce7f6d7262f214d78e6b7fd8d07119835cba4b04ce334260665d7c8fb369a, b29defbbc4ebaa243c1712ccc4943374f1b6fb864c39ed9f70fceb17eee098db, 04b13b6cd5e5291b1cde78975a140feea7fd3bc3777c53caa1ab33426c83bfcc
SHA1	ac0dce3b0f5b8d187a2e3f29efc358538fd4aa45, ad5d8dca6ad20b3b9d3b3bd5b2bbb795205f1109, 75482072f71b5457351fe3fddcd1379608767c00, 1c6913248131b5784b923eff1e76a443f738affc, 2df705c9be0465f1c73a9f5d35147723deb16b5e
MD5	44370f5c977e415981febf7dbb87a85c, 80d852cd199ac923205b61658a9ec5bc, d796259c44be852327623fd2e40c47f2, 4d0b6e3c9c33550a005e41663a1977cb, eb05429d25fc57b476428cdb0a134b2f, 2c7f328feeb94608aaaf99ec70cb0323, 8f11d9067da087cb4185fa804caac2df
IPv4	185[.]135[.]86[.]149, 134[.]195[.]91[.]224, 85[.]155[.]186[.]121, 143[.]244[.]47[.]89, 167[.]88[.]166[.]173, 143[.]110[.]243[.]154, 37[.]221[.]66[.]239, 83[.]138[.]53[.]139, 94[.]156[.]67[.]145,

TYPE	VALUE
IPv4	45[.]61[.]150[.]94, 185[.]135[.]86[.]185, 185[.]238[.]231[.]4, 185[.]238[.]231[.]16, 185[.]238[.]231[.]77, 185[.]238[.]231[.]85, 185[.]238[.]231[.]98, 23[.]234[.]89[.]195, 23[.]234[.]93[.]112, 23[.]234[.]106[.]242, 146[.]70[.]172[.]247, 37[.]19[.]21[.]180, 155[.]2[.]215[.]69, 155[.]2[.]215[.]71
Emails	key[.]medusa[.]serviceteam[@]protonmail[.]com, medusa[.]support[@]onionmail[.]org, mds[.]svt[.]breach[@]protonmail[.]com, mds[.]svt[.]mir2[@]protonmail[.]com, MedusaSupport[@]cock[.]li,
URLs	hxxp[:]//45[.]61[.]150[.]94[:]8000/storm[.]exe, hxxps[:]//3324[.]requestcatcher[.]com/hihi
Domain	erp[.]ranasons[.]com
Filenames	!!!READ_ME_MEDUSA!!!.txt, openrdp.bat, pu.exe, gaze.exe, lsp.exe, main.exe, moon.exe, RunFileCopy.cmd, def.exe, nezha-agent.exe, mimilib.dll, j.exe, Main_new.exe, command.cmd, Ngconf.txt,

Recent Breaches

https://www.sunfiber.com
https://www.walmanoptical.com
https://www.nemr.net
https://www.touchsource.com
https://www.livecasinohotel.com
https://www.ummc.edu
https://www.capemaycountynj.gov
https://www.lccc.edu
https://www.passaiccountynj.gov
https://www.bonanzacasino.com
https://www.umc.edu
https://www.frauenshuh.com
https://www.acmetruck.com
https://www.shaftext.com
https://www.ipgroup.com

Patch Links

CVE-2024-1709: https://www.screenconnect.com/download

CVE-2023-48788: https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE-2025-10035: https://www.fortra.com/security/advisories/product-security/fi-2025-012

CVE-2026-1731: https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

https://labs.cloudsecurityalliance.org/research/csa-research-note-storm1175-medusa-ransomware-zero-day-20260/

https://research.splunk.com/stories/medusa_ransomware/

https://www.microsoft.com/en-us/security/blog/2026/04/06/storm-1175-focuses-gaze-on-vulnerable-web-facing-assets-in-high-tempo-medusa-ransomware-operations/

https://therecord.media/medusa-ransomware-group-zero-days-microsoft

https://www.security.com/threat-intelligence/lazarus-medusa-ransomware

https://www.hivepro.com/threat-advisory/storm-1175-masterstroke-exploits-cve-2025-10035-in-goanywhere-mft

https://www.hivepro.com/threat-advisory/medusa-ransomware-unleashed-a-growing-cybersecurity-menace

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 20, 2026 • 07:30 AM

More at www.hivepro.com