Medusa Ransomware Activity Continues to Increase

By About the Author

Archived: 2026-04-05 13:36:26 UTC

Medusa ransomware attacks jumped by 42% between 2023 and 2024. This increase in activity continues to escalate, with almost twice as many Medusa attacks observed in January and February 2025 as in the first two months of 2024.

The Medusa ransomware is reportedly operated as a ransomware-as-a-service (RaaS) by a group Symantec's Threat Hunter Team tracks as Spearwing. Like the majority of ransomware operators, Spearwing and its affiliates carry out double extortion attacks, stealing victims' data before encrypting networks in order to increase the pressure on victims to pay a ransom. If victims refuse to pay, the group threatens to publish the stolen data on their data leaks site.

Spearwing has amassed hundreds of victims since it first became active in early 2023. The group has listed almost 400 victims on its data leaks site in that time, and the true number of victims is likely to be much higher. Ransoms demanded by attackers using the Medusa ransomware have ranged from $100,000 up to $15 million.

As we discussed in our recent Threat Hunter whitepaper on the topic of ransomware, the decline of well-known names like Noberus and LockBit following law enforcement action in 2023 and 2024 left a gap for the rise of new names on the ransomware landscape. Among those names are RansomHub and the longer established Qilin. With its continuing increase in activity, it seems that Medusa could also be taking advantage of this gap in the ransomware scene.

This is a different ransomware to the older MedusaLocker ransomware and Spearwing is not believed to have any link to that ransomware.

Medusa in Operation

It is believed that Spearwing and its affiliates mostly gain access to victim networks by exploiting unpatched vulnerabilities in public-facing applications, particularly Microsoft Exchange Servers. It has also been reported that the group has gained access to some victims by hijacking legitimate accounts, possibly utilizing initial access brokers for infiltration. In several of the Medusa attacks observed by Symantec it wasn't possible to definitively determine how the attackers had gained initial access to victims' networks, meaning an infection vector other than exploits could have been used.

A variety of living-off-the-land and dual-use tools have been used in attack chains where the Medusa ransomware has been deployed.

Once they have gained access to a victim network, attackers using Medusa typically use remote management and monitoring (RMM) software such as SimpleHelp or AnyDesk for further access and to download drivers. Mesh

Agent is another remote access tool that has been seen in several Medusa ransomware attacks. Mesh Agent has been appearing more frequently in ransomware attack chains in recent times.

Attackers using Medusa often use the Bring Your Own Vulnerable Driver (BYOVD) technique in attacks, where attackers will deploy a signed vulnerable driver to the target network, which they then exploit to disable security software and evade detection. BYOVD is a technique that has been increasingly used in ransomware attack chains over the last two years. In almost all Medusa attacks, KillAV and associated vulnerable drivers are used in this part of the attack chain to download drivers and disable security software.

The use of the legitimate RMM software PDQ Deploy is another hallmark of Medusa ransomware attacks. It is typically used by the attackers to drop other tools and files and to move laterally across the victim network.

Symantec researchers observed the same file path being used with PDQ Deploy to deploy Medusa in almost two-thirds of the Medusa ransomware attacks we investigated in the last year (*see Box 1*).

Other tools used by Spearwing and its affiliates include Navicat, a tool used to access and run database queries, which is likely used by the attackers to search for and copy relevant data for exfiltration. RoboCopy is another tool that has been used by Medusa attackers in a similar fashion, while attackers using Medusa have also been seen using Rclone for data exfiltration. Attackers have also commonly used network scanners like NetScan as part of their attack chain, while they have also used various tools for credential dumping and to delete shadow copies from victim machines.

The tactics, techniques, and procedures (TTPs) used by attackers deploying Medusa have remained consistent since it became active in 2023, with PDQ Deploy, the use of remote access clients, and the BYOVD technique to disable security software being particular hallmarks of Medusa ransomware attack chains. The consistency of the TTPs used in Medusa attacks does raise the question as to whether Spearwing is truly operating as a RaaS. The consistency of the tactics may indicate a few things:

1. The group is carrying out attacks itself as well as developing the ransomware.
2. The group works with just one or a very small number of affiliates.
3. Spearwing provides affiliates with not just the ransomware, but also a playbook as to how the attacks should be carried out and the attack chain to use.

It is difficult to say which one of the above might apply to Spearwing's activity, but it seems that the group doesn't necessarily operate as a "typical" RaaS that works with a lot of affiliates who may use varying TTPs.

See below for brief descriptions of some of the tools most used in Medusa attacks:

- **AnyDesk:** A legitimate remote desktop application. It and similar tools are often used by attackers to obtain remote access to computers on a network.
- **KillAVDriver:** A driver file used to help terminate security processes.
- **KillAV:** Used to deploy a kernel driver for terminating security processes.
- **Mesh Agent:** Publicly available software that allows remote device access and management.
- **Navicat:** Legitimate graphical database management and development software.
- **NetScan:** SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for the discovery of host names and network services.

- **PDQ Deploy:** A legitimate software tool that allows users to manage patching on multiple software packages in addition to deploying custom scripts.
- **PDQ Inventory:** A legitimate software tool that allows users to inventory software on network machines.
- **SimpleHelp:** Remote desktop software that provides remote access and control of a device.
- **Rclone:** Open-source tool that can legitimately be used to manage content in the cloud, but has been seen being abused by ransomware actors to exfiltrate data from victim machines.
- **Robocopy:** A command-line file transfer utility for Microsoft Windows.

The .medusa extension is added to encrypted files and a ransom note named *!READ_ME_MEDUSA!!!.txt* is dropped on encrypted machines. Medusa can also delete itself from victim machines once the ransom is executed, which makes it more difficult for those investigating these ransomware attacks. The ransom demanded by the group varies depending on the victims. Victims are given 10 days to pay and are charged $10,000 per day if they want to extend this deadline. The attackers provide screenshots of stolen data to prove that they have compromised victims' networks. If victims fail to pay, Spearwing will publish the stolen data on its leaks site.

While there is no link between Medusa and MedusaLocker, in a relatively early Medusa attack, in June 2023, attackers deploying Medusa used drivers that were related to ones previously used in a BlackCat (aka Noberus) attack described by Trend Micro. It wasn’t clear if those drivers were publicly available, or if these two instances pointed to a sharing of tools or affiliates by Medusa and BlackCat. No further evidence has appeared to suggest links between the two groups, though it is possible that they may have affiliates or members in common.

Like most targeted ransomware groups, Spearwing tends to attack large organizations across a range of sectors. Ransomware groups tend to be driven purely by profit, and not by any ideological or moral considerations. Medusa has been publicly documented as demanding ransoms from healthcare providers and non-profits, as well as targeting financial and government organizations.

Case Study: Medusa Attack

In an attack investigated by Symantec’s Threat Hunter team in January 2025, Medusa was used to target a healthcare organization in the U.S., where it infected several hundred machines.

The initial access vector used in this attack is not known. The first attacker activity occurred on this network four days before the ransomware was deployed. Once the attacker was on the victim network they staged multiple tools for persistence, lateral movement, and to impair defenses. Most of the tools were staged under the *CSIDL_PROFILE\documents folder*.

Some of the early attacker activity on this network included:

Executing VSS admin to create shadow copies:

- *vssadmin create shadow /for=C:*

Accessing ntds.dit for credential dumping.

Installing SimpleHelp and Mesh Agent onto victim machines:

- *CSIDL_PROFILE\documents\mesh.exe -fullinstall*
- *CSIDL_PROFILE\documents\SN.exe*

Dropping AVKiller and a driver under the documents folder on a machine. The attackers used the known POORTRY driver, as well as one unknown driver, for the purposes of killing security software during this attack:

- *CSIDL_PROFILE\documents\2Gk8.exe*
- *CSIDL_PROFILE\documents\smuot.sys*

On the day of the ransomware attack, Rclone was deployed on the victim network for data exfiltration. The attackers used a renamed version of Rclone - *lsp.exe*. Rclone was found under:

- *CSIDL_SYSTEM_DRIVE\temp*

On the day the ransomware was deployed, the attacker switched to another machine and started staging tools. The attacker used PsExec to execute commands on this machine remotely.

It executed the following commands on this machine:

- *quser*
- *net user*
- *CSIDL_SYSTEM\net1 user <? |comma| ?> default [REDACTED] /domain*

The attacker then dropped and installed SimpleHelp:

- *csidl_profile\documents\mx.exe*

They then attempted to create a shadow copy of the C drive but used an incorrect command. This is notable as it points to hands-on-keyboard activity, rather than this being an automated attack:

- *vssadmin create dhadow /for=C:*

The attacker then corrected the command and executed again:

- *vssadmin create shadow /for=C:*

The attacker then dumped the ntds.dit file, before deleting the shadow copy:

- *vssadmin delete shadows /shadow=*

They then dropped and installed AnyDesk, and used this to download PDQ Deploy and PDQ Inventory onto the machine:

- *CSIDL_PROFILE\documents\anydesk.exe*

The attacker then opened an RDP session to another machine, and this is the last activity that occurred on this machine.

On the other machine, the attacker dropped PDQ Deploy, PDQ Inventory, and SimpleHelp under the same directory, before PDQ Deploy and PDQ Inventory were installed under the programs directory and SimpleHelp under the common appdata directory. The attacker used PDQ Inventory to get an inventory of the endpoints on the network. PDQ Deploy then used this information to deploy the AVKiller binary and driver under the Windows directory to all the endpoints and execute it.

The attacker then used PDQ Deploy to transfer the ransomware binary and execute it. The ransomware had the file name *gaze.exe*.

The ransomware didn't encrypt files with the following extensions:

- .dll
- .exe
- .lnk
- .MEDUSA

It also didn't encrypt content in the following folders:

- WindowsOld
- Perflogs
- Msocache
- ProgramFiles
- ProgramFilesX86
- Programdata

The ransomware contained an encoded list of the services and processes it wanted to terminate. It used the key 0x2e to decode the strings and use them with *net stop <service> & taskkill /F /IM <process> /T*.

The ransomware dropped its ransom note—*!READ_ME_MEDUSA!!!.txt*—into every directory it encrypted. The ransomware was then able to delete itself once it was executed.

Medusa has multiple arguments that perform various tasks. The list of accepted arguments for the ransomware used in this attack can be seen in Box 2.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.
