Medusa Ransomware Group: A Rising Threat in 2025

By Check Point Software

Published: 2025-06-08 · Archived: 2026-04-05 22:36:09 UTC

The 2025 Ransomware Surge: Context for Medusa's Rise

The rise of the Medusa group is set against a historic ransomware surge in Q1 of 2025.

- Data shows 2,289 reported incidents in the first three months of the year,
- More than double the number from the same period last year (1,011)
- Representing a 126% year-over-year increase.

This surge comes despite high-profile law enforcement operations in 2024 disrupting major ransomware players LockBit and ALPHV. This fragmentation has allowed other ransomware variants and newly formed groups to fill the void left in the RaaS marketplace.

When it comes to Medusa ransomware vs cl0p, the latter remains the most active group in the RaaS marketplace. While it may not be the biggest player in the industry, Medusa's activities have caught the attention of US law enforcement.

- In March 2024, the FBI and US Cybersecurity and Infrastructure Security Agency (CISA) posted an advisory warning organizations about the threats posed by the Medusa ransomware group.

The advisory includes a description of the group's:

- Tactics
- Techniques
- Procedures
- Recommendations to minimize the risk

Who Is the Medusa Ransomware Group?

Medusa is a RaaS variant that has grown significantly, claiming hundreds of victims and becoming a top ten ransomware actor since 2023. Originally a closed ransomware variant (all operations handled by the Medusa ransomware group alone), it has since developed an affiliate model that allows others to launch attacks.

But the central Medusa ransomware group still handles ransom negotiations.

The specific location of the Medusa ransomware group is unknown, but evidence suggests it operates out of Russia or one of its allied states. This is due to the group avoiding targeting organizations within Russia and the Commonwealth of Independent States and activity on Russian-language dark web forums like RAMP.

- Medusa is not connected to MedusaLocker or the Medusa mobile malware variant.

- Evidence shows the group operates independently and is not an offshoot of another cybercriminal group.
- The software Medusa uses is unique, with no reports of code similarities to other RaaS variants.

However, there is intelligence linking Medusa to "Frozen Spider," an eCrime group active in broader cybercrime-as-a-service networks. Although details are unclear, Frozen Spider uses Medusa ransomware for big game hunting, targeting larger-scale organizations for higher ransoms.

Medusa Targets

The Medusa ransomware group hits a variety of industries, often targeting critical infrastructure used in **healthcare**, **education**, **technology**, **manufacturing**, **legal**, and **government organizations**.

- Previous high-profile targets include the Minneapolis Public School District and Toyota Financial Services.

They often go after profitable small and medium-sized enterprises (SMEs) in industries that:

- Utilize sensitive data
- Require significant digital infrastructure
- Rely heavily on business continuity

This increases their chances of getting paid, as victims scramble to resume normal operations and protect their data. Medusa victims have been reported in over 45 countries, including the United States, Canada, Australia, Germany, Italy, and the UK.

- Medusa ransomware UK statistics show the group has an outsized presence in the country.
- Ransomware trends from 2025 Q1 found that Medusa accounts for 9% of all reported victims in the UK, compared to just 2% of victims worldwide.

Medusa's Use of Public Channels and Data Leak Sites

Unlike many other ransomware groups, Medusa is known for using public channels with a:

- Public Telegram channel
- Facebook profile
- Twitter/X account
- OSINT (Open Source Intelligence) Without Borders Website

These properties are allegedly run by users under the pseudonyms "Robert Vroofdown" and "Robert Enaber."

Utilizing these public channels, the Medusa ransomware group aims to publicly pressure its victims into paying ransoms while also building its reputation and presence in the RaaS marketplace by demonstrating its capabilities and accomplishments.

The Medusa ransomware group also launched its own data leak site in 2023 known as the Medusa Blog.

The group publishes sensitive information on the site when victims refuse to pay ransoms. This data leak site is on the dark web alongside Medusa's TOR links and forums.

Medusa's Tactics, Techniques, and Procedures (TTPs)

The Medusa ransomware group's primary goal appears to be financial returns.

They utilize a double extortion model where data is encrypted and exfiltrated to achieve this. This enables the group to start ransom negotiations with large demands as they not only disrupt operations but also threaten to publicly release the victim's sensitive data.

To infiltrate corporate systems, Medusa typically pays Initial Access Brokers (IABs) to provide user credentials and other sensitive data that enables access. These brokers utilize credential stuffing, phishing, and other techniques to gather their datasets before advertising them on cybercrime marketplaces.

IABs accelerate Medusa's ransomware attacks, allowing the group to focus on encrypting and exfiltrating datasets and negotiating ransoms rather than gaining initial access to networks. But, the Medusa ransomware group also conducts phishing campaigns and exploits public-facing vulnerabilities to gain access to networks themselves.

Common Medusa ransomware tactics during an attack include:

- Utilizing PowerShell and other tools to evade ransomware detection techniques and increase access.
- Data transfer is also handled using PowerShell scripts.
- Tor provides a secure channel to copy data.
- Encryption processes add a .MEDUSA extension to each of the victim's files.
- Ransom notes are delivered via a !!!READ_ME_MEDUSA!!!.txt that provides instructions, a unique identifier, and warnings of future actions if payment is not made.
- The attack is then announced on the Medusa Blog.

How to Defend Against Medusa Ransomware: 8 Effective Tips

Protecting your business network against Medusa ransomware threats requires a range of security controls and best practices.

Methods promoted in the recent Medusa advisory include:

1. **Developing extensive recovery plans** that include backups of sensitive business data stored in physically separated locations.
2. **Utilizing strong authentication processes** that comply with NIST standards. This includes strong password management processes and multifactor authentication, particularly for your most sensitive systems.
3. **Tracking all of your software** (including operating systems and firmware) and ensuring they remain up to date with patches for the latest vulnerabilities.
4. **Segmenting your network** to prevent the Medusa ransomware tactics of scanning networks for lateral movement and greater access after the initial breach.
5. **Monitoring network activity** and developing methods of identifying abnormal or suspicious behavior. This includes tools for endpoint detection and response.
6. **Ensuring employees remotely accessing your network utilize VPNs** for secure connectivity.

7. **Auditing accounts for access** and applying the principle of least privilege, where users only have access to the data and resources they need based on their role.
8. **Filtering network traffic** and blocking packets from unknown or untrustworthy sources.

Enhance Ransomware Protection with Check Point Solutions

You need a dedicated solution to implement these methods and protect your business against Medusa ransomware in 2025 and beyond. Check Point Endpoint Security from Check Point offers comprehensive Anti-ransomware protection against the most sophisticated attacks. The solution provides:

- Complete endpoint protection
- Automated ransomware attack detection and remediation
- Fast recovery to ensure business continuity

All this comes in a single, cost-effective product that can be tailored to meet your security and compliance needs.

Find out how Check Point Endpoint Security mitigates the risk posed by the top ransomware groups and most advanced threats by booking a demo today.
