M

MedusaLocker Ransomware: Identification, Response, and Recovery

MedusaLocker is a Windows ransomware family distinct from the newer Medusa RaaS operation. Learn how to identify it, contain the intrusion, preserve evidence, and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What is MedusaLocker ransomware?
02 MedusaLocker vs. Medusa ransomware
03 How MedusaLocker affects a network
04 How to identify a suspected MedusaLocker incident
05 Immediate response
06 Containment is not recovery
07 Recovery options
08 Should you pay the ransom?
09 How to reduce MedusaLocker risk
10 Frequently asked questions
11 References

01 What is MedusaLocker ransomware?

MedusaLocker is a Windows ransomware family observed since 2019 that encrypts local and network-accessible files and leaves a ransom note demanding payment. Variants have used different encrypted-file extensions and note names, so an extension alone is not enough to identify the family.

MedusaLocker should not be confused with the separate **Medusa ransomware-as-a-service operation** first identified in 2021 or with Android malware that also uses the Medusa name. These threats have different operators, timelines, behaviors, and indicators. Current FBI and CISA advisories about the Medusa RaaS operation do not automatically describe MedusaLocker.

02 MedusaLocker vs. Medusa ransomware

Name	Commonly reported timeline	Important distinction
MedusaLocker	Observed since 2019	Older Windows ransomware family with multiple variants, notes, and extensions
Medusa RaaS	Identified in 2021	Separate operation covered by a 2025 joint FBI/CISA advisory; known for encryption and data-extortion activity
Medusa Android malware	Separate mobile threat	Banking or device-abuse malware; not the Windows ransomware described here

If an alert or incident report says only "Medusa," confirm the ransom-note text, filenames, hashes, process activity, and source that assigned the name before using family-specific instructions.

03 How MedusaLocker affects a network

Observed MedusaLocker variants prepare Windows systems for encryption, enumerate drives and shares, and attempt to reduce recovery options. Published research has described behavior such as:

- Encrypting files on local disks, mapped drives, and accessible network shares.
- Attempting to remap network drives so additional data becomes reachable.
- Stopping selected services or processes that keep important files open.
- Deleting Windows Volume Shadow Copies and interfering with ordinary recovery.
- Leaving ransom instructions in affected directories.
- Using different extensions and note formats across variants.

Ransomware execution is often the final visible stage of a broader intrusion. The attacker may already have used stolen credentials, remote access, scripts, administration tools, or lateral movement. Investigate the access that preceded encryption instead of treating every encrypted device as an isolated event.

04 How to identify a suspected MedusaLocker incident

- Multiple files become unreadable and receive the same unfamiliar extension.
- A ransom note appears repeatedly in encrypted directories.
- Security or backup-related services stop unexpectedly.
- Shadow-copy deletion, backup changes, or suspicious system utilities appear shortly before encryption.
- One account or host accesses and changes many files across network shares.
- Endpoint alerts show the encryptor, a loader, remote administration, or suspicious child processes.
- Authentication and network logs show unusual remote access or lateral movement before impact.

Do not rename encrypted files, run the ransom note's tools, or test random decryptors on the only copy. Preserve representative encrypted files, the original note, and relevant metadata for identification.

05 Immediate response

1. **Isolate affected systems and network segments.** Disconnect network paths, VPN access, and shared storage as needed to stop continuing encryption. Avoid destroying volatile evidence without the incident lead's approval.
2. **Protect backups.** Make backup infrastructure unreachable from compromised accounts and systems. Preserve known-good offline or immutable copies.
3. **Disable compromised access.** Revoke exposed sessions, remote-access accounts, API tokens, and administrative credentials. Make emergency changes from a clean system.
4. **Preserve evidence.** Collect the ransom note, encrypted-file samples, memory or disk images when appropriate, endpoint alerts, identity logs, firewall and VPN records, and the incident timeline.
5. **Scope the intrusion.** Find the first affected account and host, other systems contacted, tools deployed, persistence, data accessed, and whether encryption is still running.
6. **Engage the response team.** Involve security, IT, leadership, legal or privacy counsel, insurers, communications, and law enforcement according to the organization's plan.

06 Containment is not recovery

Stopping the encryptor does not remove the attacker's foothold. Before bringing systems back:

- Identify and close the original entry point.
- Remove persistence, unauthorized accounts, remote-management tools, scripts, and later payloads.
- Patch exploited services and restrict exposed remote access.

- Determine whether credentials, session tokens, certificates, or service-account secrets were accessible.
- Search peer systems for the same behavior and indicators.
- Assess possible data access or exfiltration separately from file encryption.

07 Recovery options

1. **Rebuild affected systems from known-good media or images.** A clean rebuild is preferable when privileged access or scope is uncertain.
2. **Restore verified data from an offline or immutable backup** created before the compromise. Scan and test the data before reconnecting production access.
3. **Rotate credentials and secrets** after the environment is clean, including service accounts and privileged identities.
4. **Validate business applications** for integrity, permissions, and data consistency.
5. **Monitor for renewed access** using endpoint, identity, DNS, network, cloud, and backup telemetry.
6. **Document lessons and owners** for each corrective action.

Is there a MedusaLocker decryptor?

Availability depends on the exact variant, encryption implementation, and current trusted recovery research. Do not assume that a tool for "Medusa" supports MedusaLocker or your extension. Work from copies, verify the tool's publisher and family match, and preserve the originals. A legitimate decryptor restores files; it does not remove persistence or secure stolen credentials.

08 Should you pay the ransom?

Payment does not guarantee a working key, complete recovery, deletion of stolen data, or freedom from another demand. It may also involve legal or sanctions risk. An organization should make any decision with incident responders, leadership, legal counsel, insurers, and relevant

authorities, based on verified facts and applicable law.

09 How to reduce MedusaLocker risk

- Keep internet-facing operating systems, VPNs, appliances, and applications patched and supported.
- Place remote administration behind controlled access, use MFA, and restrict source networks.
- Use separate privileged accounts and prevent ordinary or compromised accounts from managing backups.
- Segment workstations, servers, sensitive applications, and backup infrastructure.
- Monitor mass file changes, shadow-copy deletion, unusual service stops, and remote execution.
- Use application control and endpoint detection on servers and workstations.
- Maintain offline or immutable backups and rehearse full restoration.
- Retain identity, endpoint, VPN, network, and backup logs long enough to reconstruct initial access.

10 Frequently asked questions

Does a .medusa extension prove MedusaLocker?

No. Extensions can overlap, change between variants, or be imitated. Use the note, sample hash, encryption behavior, process evidence, and reputable analysis together.

Can antivirus restore encrypted files?

Security software may stop or remove a detected payload, but it generally cannot reverse properly implemented encryption. Restore from verified backups or use a trusted variant-specific decryptor when one is available.

Should an infected computer be powered off?

Isolation is the immediate priority. Whether to shut down depends on active encryption, safety, and the need to preserve volatile evidence. Follow the incident-response lead's direction.

11 References

- Cisco Talos: Threat Spotlight - MedusaLocker
- Microsoft Security Intelligence: MedusaLocker
- FBI/CISA: separate Medusa ransomware advisory

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com