Medusa Ransomware (MedusaLocker) - What it is, how it spreads, and how to recover safely

Gridinsoft Help Center

What it is

MedusaLocker is ransomware that encrypts your files and demands a cryptocurrency payment to unlock them. It often arrives through email lures or exposed services, then spreads across the network. Technical details and IOCs are in our Medusa overview for defenders.

How it spreads - quick tour

- Phishing emails with malicious attachments or links
- Weak or exposed RDP/VPN and public-facing apps
- Lateral movement once inside, targeting shared folders and backups

What you may notice

- Files gain a new extension and will not open
- A ransom note appears on the desktop and in folders
- Backups missing, shadow copies deleted, tools crashing

If it hits - first moves

- Isolate affected systems and disconnect external drives.
- Preserve notes and logs; do not delete evidence.
- Rebuild from known-good images and restore offline backups.
- From a clean device, change passwords and enable MFA.
- Identify the entry point and block it (email rule, account, or service).

Prevent it

- Patch internet-facing services fast; remove unused remote access.
- Use EDR/anti-malware plus email, web, and DNS filtering.
- Enforce MFA and least privilege on admin accounts and shares.
- Keep offline, tested backups and run recovery drills.
- Monitor for mass file changes, C2 beacons, and tool executions.