Cerber Ransomware: What it is, how it spreads, and how to recover safely

Gridinsoft Help Center

What it is

Cerber is ransomware run like a business ("RaaS"). The operators rent the malware to affiliates, who break in, encrypt files, and demand payment-then share the profits with Cerber’s creators.

How it spreads

- Phishing emails with booby-trapped attachments or links
- Malicious or hacked websites (drive-by downloads)
- Exploited remote access (weak RDP/VPN) and unpatched software

What you may notice

- Files won’t open and get new extensions
- Ransom notes dropped across folders
- Security tools disabled; sudden CPU/disk spikes

If it hits (act fast)

- Isolate affected machines (unplug/disable Wi-Fi).
- Do not delete ransom notes/logs; they help recovery.
- Check offline backups; rebuild clean systems if possible.
- Rotate admin/domain passwords from a clean device.
- Engage IR/IT support; consider reporting to authorities.

Prevent it

- Patch OS/apps; lock down or remove unused remote access.
- Enforce MFA everywhere, least-privilege for admins.
- Use reputable EDR/anti-malware and email filtering.
- Keep offline, tested backups; practice restore drills.
- Train staff to spot phishing and fake updates.