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

Gridinsoft Help Center

What it is

CTB Locker is crypto-ransomware first seen in 2014. Once it lands, it encrypts your files and drops a note demanding payment to unlock them. It often hits Windows PCs through convincing lures and fake updates.

How it spreads

- Phishing emails with booby-trapped attachments or links
- Deceptive downloads (e.g., fake "Flash/codec" updates)
- Bundled installers from sketchy sites

What you may notice

- Files won’t open and may get new extensions
- Ransom notes appear on the desktop and in many folders
- CPU/disk spikes; security tools crash or get disabled

If it hits - act fast:

- Isolate the machine (turn off Wi-Fi/unplug network; disconnect external drives).
- Keep ransom notes/logs-they help recovery and investigation.
- Check offline backups; rebuild the system clean and restore data.
- From a clean device, change passwords and enable MFA.
- Block related domains/IPs and review how it got in.

Prevent it

- Patch Windows and apps; remove/lock down unused remote access.
- Use reputable EDR/anti-malware and email/web filtering.
- Keep offline, tested backups and practice restores.
- Train users to spot phishing and fake update prompts.
- Least-privilege accounts; MFA everywhere.