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

Gridinsoft Help Center

What it is

Clop is big-game ransomware: attackers break into a network, encrypt files, and demand payment to unlock them-often with data theft first to pressure victims (double extortion). It mostly targets Windows environments and larger organizations.

How it spreads

- Phishing emails and booby-trapped attachments
- Exploited remote access (weak RDP/VPN) and unpatched apps
- Stolen admin credentials; lateral movement across the domain

What you may notice

- Files won’t open and gain new extensions
- Ransom notes sprinkled across folders
- Security tools disabled; sudden CPU/disk spikes on servers

If it hits (act fast)

- Isolate affected systems from the network.
- Preserve notes and logs-don’t wipe evidence.
- Check offline backups and rebuild on clean images.
- Rotate domain/admin credentials from a clean device.
- Engage IR/IT teams; consider reporting to authorities.

Prevent it

- Patch internet-facing services; close or secure unused remote access.
- Enforce MFA everywhere; least privilege for admins.
- Use reputable EDR/anti-malware and email filtering.
- Keep offline, tested backups and practice restore drills.
- Train staff to spot phishing and fake updates.