Crysis (Dharma) Ransomware: What it is, how it spreads via RDP, and how to recover safely

Gridinsoft Help Center

What it is

How it gets in

- Open or poorly protected RDP (guessable passwords, no MFA)
- Stolen credentials bought on underground markets
- Unpatched servers and reused admin passwords

What you may notice

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

If it hits (act fast)

- Isolate affected machines (unplug/disable Wi-Fi; disconnect mapped drives).
- Preserve ransom notes and logs-don’t wipe evidence.
- Check offline backups; rebuild on clean images and restore data.
- Rotate admin/domain passwords from a clean device; close RDP to the internet.
- Engage IR/IT teams; consider reporting to authorities.

Prevent it

- Remove or lock down RDP (VPN + MFA, allowlisted IPs, non-default ports).
- Patch OS/apps; disable unused remote access.
- Enforce MFA and least privilege for admins.
- Use reputable EDR/anti-malware and email/web filtering.
- Keep offline, tested backups and practice restores.