Cactus Ransomware: Signs, removal steps, and prevention tips

Gridinsoft Help Center

Cactus sneaks into company networks through weak or outdated VPN setups, then locks (encrypts) files and demands money to unlock them. It’s a break-in via remote access, followed by a warehouse of locked boxes.

How it gets in:

- Vulnerable or misconfigured VPNs/remote access
- Stolen or weak admin passwords
- Unpatched servers and apps

What you might notice:

- Files won’t open; new extensions appear
- Ransom notes in many folders
- Security tools disabled; servers slow or unresponsive

If it hits, do this now:

- Isolate affected machines from the network
- Keep ransom notes/logs (don’t wipe evidence)
- Check offline backups and plan clean rebuilds
- Rotate admin/domain passwords from a clean device
- Contact IT/IR support; consider reporting to authorities

How to prevent it:

- Patch VPNs, firewalls, and servers quickly
- Enforce MFA on all remote access; limit admin rights
- Use reputable EDR/anti-malware and email filtering
- Keep offline, tested backups; run restore drills
- Close unused remote-access paths

Learn more: Cactus - behaviors, IOCs, and removal