BabLock Ransomware: Signs, removal steps, and prevention tips

Gridinsoft Help Center

What it is (in plain words): BabLock is ransomware that breaks into Windows and Linux systems, scrambles (encrypts) your files, and demands payment to unlock them. It typically goes after small and mid-size businesses where one infected PC can quickly disrupt the whole office.

How it spreads:

- Phishing emails and booby-trapped attachments
- Cracked/unknown software and malicious installers
- Exposed or weakly protected RDP/VPN access
- Unpatched software vulnerabilities and supply-chain downloads

Signs to watch for:

- Files won’t open and new extensions appear
- Ransom notes in many folders
- Sudden CPU/disk spikes; security tools disabled
- Backups or mapped drives also encrypted

If it happens, do this now:

- Isolate affected machines from the network (unplug/disable Wi-Fi).
- Do not delete notes or logs-they help recovery and investigation.
- Check offline backups and prepare clean rebuilds.
- Rotate passwords (especially admin/domain) from a clean device.
- Call IT/IR support; consider reporting to local authorities.

Prevent it:

- Keep systems and apps patched; remove unused remote access.
- Enforce MFA on RDP/VPN and limit admin rights.
- Use reputable EDR/anti-malware and email filtering.
- Maintain offline, tested backups (and practice restore drills).
- Train staff to spot phishing.

Learn more: BabLock - behaviors, IOCs, and removal