Bootkit: What it is, why it’s hard to spot, and how to remove it safely

Gridinsoft Help Center

What it is

A bootkit is stealthy malware that buries itself in the startup area of a PC (MBR/UEFI), so it runs before Windows. That early start lets it hide other malware, survive reboots, and dodge many on-device scans.

What you may notice

- Odd boot behavior: extra delay, crashes, or unexpected reboot loops
- Security tools disabled or detections that keep coming back after cleanup
- BitLocker/Secure Boot warnings, or boot order changing on its own

How it works

- Infects the bootloader or firmware so code runs at power-on
- Hooks low-level disk or OS functions to hide files and traffic
- Can reinstall companion malware even after you think you removed it

If you suspect a bootkit (safe cleanup)

- Disconnect from the network; power down.
- Scan from outside Windows using a trusted bootable rescue media.
- Restore the boot chain: re-enable Secure Boot, repair boot records, or reinstall Windows if required.
- Update firmware/BIOS and drivers; then rescan.
- Change passwords from a clean device; watch accounts for alerts.

Prevent it

- Keep Secure Boot on; prefer UEFI over legacy boot.
- Update firmware/BIOS, OS, and drivers regularly.
- Block booting from untrusted USB/DVD; set a BIOS/UEFI admin password.
- Use reputable real-time protection and avoid cracked installers.