Rootkit - what it is, how it hides, and how to detect and remove it

Gridinsoft Help Center

What it is

A rootkit is malware built to hide itself (and other malware) while giving an attacker high-level control of a system. It can live in user space, the kernel, the boot process (bootkit), or even device firmware. Once installed, it can mask files, processes, drivers, and network connections, intercept security tools, and let other threats run with elevated privileges. Background and removal basics: https://gridinsoft.com/rootkit

Why it matters

Rootkits make infections hard to see and hard to remove. They can disable defenses, steal data quietly, and reinstall payloads after you think you've cleaned the machine.

How it works - quick tour

- Entry: phishing, drive-by exploits, or malicious drivers/installers.
- Hook: intercepts system calls or drivers to hide activity.
- Persist: lodges in startup, the bootloader, or firmware to survive reboots.
- Assist: loads additional malware with SYSTEM/admin rights on demand.

Red flags

- Security tools won't start, crash, or disagree on what's running.
- Unknown drivers/services with random names; blocked attempts to view them.
- Network activity without matching processes; odd DNS/TLS errors.
- Secure Boot or driver signing suddenly disabled; unexplained BSODs.

Prevent it

- Keep OS, drivers, and firmware updated; enable Secure Boot and driver signing.
- Use least-privilege accounts and block unsigned drivers.
- Run reputable anti-malware/EDR with kernel-tamper detection.
- If suspected, isolate the device, collect logs, and reinstall from known-good media; for boot/firmware compromise, reflash firmware and rotate credentials.