UEFI Rootkit - what it is, why it’s dangerous, and how to spot and recover from it

Gridinsoft Help Center

What it is

A UEFI rootkit is malware that hides inside a computer’s firmware - the low-level code that starts your PC before Windows loads. Because it lives in the UEFI (which replaces old BIOS), it can run first at every boot, stay hidden from normal scans, and even survive wiping or reinstalling Windows.

Why it matters

If attackers own the firmware, they can control what loads next, hide other malware, and bring it back after you think you cleaned the PC. It’s one of the hardest infections to spot and remove.

How it works

- Break in: attacker gets admin rights through a bug, phishing, or a bad driver/loader.
- Plant: malicious code is written to the UEFI firmware or its boot files.
- Boot first: on power-up, the rootkit runs before Windows and hides itself.
- Assist: it launches or reinstalls other malware with high privileges.

Red flags

- Malware keeps returning after a full Windows reinstall.
- Secure Boot gets disabled without you doing it.
- Unknown or unsigned drivers appear; security tools crash or won’t start.
- Odd boot errors or firmware updates that fail repeatedly.

Do it right

- Keep firmware (UEFI), drivers, and Windows fully updated; enable Secure Boot and TPM.
- Only install drivers/software from trusted sources; avoid unsigned drivers.
- Use reputable security tools with boot-level integrity checks.
- If you strongly suspect a UEFI compromise: back up files, update/reflash the firmware from the motherboard or device maker, then do a clean Windows install and change passwords from a clean device.