B

Bootkit Malware: How It Persists, How to Detect It, and Recover

A bootkit runs through a compromised startup chain before the operating system fully loads. Learn how it differs from a rootkit, what evidence matters, and how to recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Bootkit versus rootkit
02 How bootkits gain persistence
03 Possible signs and useful evidence
04 What to do after a suspected bootkit detection
05 Recovery: match the fix to the layer
06 After recovery
07 Frequently asked questions
08 References

A **bootkit** is malware that alters or abuses a computer's startup chain so malicious code runs before, or while, the operating system loads. This early position can provide durable persistence and can let the malware interfere with security controls that start later.

A UEFI rootkit concerns persistence at the firmware layer, while Early Launch Anti-Malware (ELAM) is a Windows mechanism for evaluating boot-start drivers. These distinctions help identify the affected layer without treating every startup warning as evidence of the same threat.

Bootkits are uncommon compared with ordinary malware. A bootkit detection deserves careful handling, but repeated crashes or a failed reinstall alone do not prove that one is present.

01 Bootkit versus rootkit

Term	Main idea	Typical location
Rootkit	Hides malicious activity or maintains privileged, stealthy access.	User mode, kernel, hypervisor, firmware, or other layers.
Bootkit	Starts through a modified or malicious boot component before the normal OS startup completes.	MBR/VBR on legacy BIOS systems or files and configuration associated with the EFI System Partition on UEFI systems.
Firmware implant	Persists in device or system firmware itself.	UEFI flash or component firmware; this is not the same as every UEFI bootkit stored on disk.

A bootkit is often discussed as a type of rootkit, but the terms are not interchangeable. The location matters because recovery that cleans Windows files may not repair a compromised boot chain.

02 How bootkits gain persistence

On older BIOS systems, a bootkit can modify the Master Boot Record or Volume Boot Record so attacker code receives control during startup. On UEFI systems, it may add or replace boot files in the EFI System Partition, alter boot entries, enroll an unauthorized key, or exploit a vulnerable trusted boot component.

A bootkit is usually not the initial way into a device. Deployment commonly requires administrator-level control, raw disk access, a separate exploit, or physical access. After installation, it may load a malicious driver, weaken security features, or launch another payload.

03 Possible signs and useful evidence

- Secure Boot unexpectedly disabled, or firmware settings and boot order changed without authorization.
- Unexpected files, hashes, timestamps, boot entries, or keys associated with the EFI System Partition.
- BitLocker recovery prompts or measured-boot/attestation changes that cannot be explained by an approved update.
- A security product reports a specific boot component or behavior, especially when confirmed from a trusted offline environment.
- Malware or a driver returns after apparently successful removal.
- Differences between disk contents observed from the running OS and from trusted external media.

These signals can also have benign causes: firmware updates, disk repair, dual-boot changes, cloned drives, or legitimate bootloader updates. Record exact detection names and affected paths before making a conclusion.

04 What to do after a suspected bootkit detection

1. **Disconnect the device from networks.** This limits follow-on access and protects credentials and other systems.
2. **Preserve evidence.** Record the alert, time, Secure Boot state, BitLocker state, firmware version, boot entries, disk layout, and recent administrative changes. In an organization, involve incident response before wiping the device.

3. **Do not trust the active OS for the only scan.** Use vendor-supported bootable or recovery media obtained on a clean computer. Keep Secure Boot enabled when the recovery workflow supports it.
4. **Scope the intrusion.** A bootkit generally implies an earlier privileged compromise. Investigate accounts, remote access, exploitation, lateral movement, and other payloads.
5. **Choose recovery based on the affected layer.** Repairing ordinary system files is not sufficient if boot components remain modified.

05 Recovery: match the fix to the layer

Finding	Typical recovery direction
Legacy MBR/VBR modification	Rebuild the boot records or repartition and reinstall from known-good media, following the operating system vendor's guidance.
Malicious files or entries in the EFI System Partition	Recreate trusted boot files and configuration or fully repartition/reinstall. Validate Secure Boot settings afterward.
Unauthorized Secure Boot keys or firmware settings	Restore approved keys and firmware settings using the device manufacturer's documented process.
Suspected firmware compromise	Escalate to the hardware vendor or a qualified incident-response team. A normal OS reinstall may not address firmware-resident code.

Do not blindly flash firmware or delete the EFI System Partition. An incorrect image or key change can make the device unbootable or trigger data-encryption recovery. Obtain recovery keys and verified vendor media first.

06 After recovery

- Patch the OS, firmware, boot components, and security products.
- Enable and verify Secure Boot, TPM-backed protections, Trusted/Measured Boot, and disk encryption where supported.

- Reset credentials used on the affected device from a known-clean system; revoke active sessions and rotate privileged secrets.
- Restore data only from backups created before the compromise and scan the restored data.
- Monitor for the original entry vector and for recurrence across other endpoints.

07 Frequently asked questions

Can a bootkit survive reinstalling Windows?

It can if the reinstall leaves the affected boot partition or firmware state intact. A reinstall that correctly removes and recreates all disk partitions may eliminate a disk-resident bootkit, but not necessarily a genuine firmware implant.

Does Secure Boot make bootkits impossible?

No. Secure Boot substantially raises the barrier by verifying trusted boot components, but configuration errors, stolen or abused trust, vulnerable signed components, and implementation flaws can still matter. Keep it enabled and apply vendor revocation and firmware updates.

Should I replace the motherboard?

Not for an unconfirmed alert. First determine whether the finding is in the disk boot chain or actual firmware. Hardware replacement is an exceptional response best decided with the manufacturer or incident responders.

08 References

- MITRE ATT&CK: Bootkit (T1542.003)
- Microsoft: Secure the Windows boot process
- Microsoft: BlackLotus investigation and recovery guidance

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com