M

Multipartite Virus: How Boot and File Infection Works and How to Remove It

A multipartite virus infects more than one system area, classically boot records and executable files. Learn why partial cleanup fails and how to recover from trusted media.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How a multipartite virus spreads
02 Multipartite virus versus related threats
03 Historical examples
04 Possible signs
05 Safe cleanup
06 When file repair is unsafe
07 Prevention
08 Frequently asked questions
09 References

A **multipartite virus**, also called a multi-part or polypartite virus, is a computer virus that infects more than one part of a system. The classic definition is a virus that infects both executable files and boot records such as a disk's boot sector or Master Boot Record.

Because either infected area can restore the other, cleaning only files or only the boot record can lead to reinfection. The term mainly describes classic PC viruses and should not be used as a synonym for any modern malware with several components.

01 How a multipartite virus spreads

1. An infected executable, removable disk, or bootable medium reaches a computer.
2. Running the infected file or starting the computer from infected media activates the virus.
3. The virus infects a boot record and commonly becomes memory-resident during startup.
4. While active in memory, it infects executable files that are opened, copied, or created.
5. Those infected files or removable disks carry the virus to other systems.

The direction can also start with an infected boot sector. Once the computer boots from it, the memory-resident virus can infect program files. This two-way cycle is why partial cleanup fails.

02 Multipartite virus versus related threats

Threat type	What it infects or changes	Key difference
File-infector virus	Executable or other host files.	Replicates by modifying files but does not necessarily infect boot records.
Boot-sector virus	Boot record, MBR, or volume boot record.	Starts through the boot process but may not infect program files.
Multipartite virus	Both boot records and files, or multiple comparable infection targets.	Each infected area can contribute to continued spread or reinfection.

Threat type	What it infects or changes	Key difference
Bootkit	Startup components used for stealth and persistence.	May not be a self-replicating virus or infect host files.
Modern multi-stage malware	Uses a loader, payloads, persistence, and network components.	Having many modules does not make it a multipartite virus.

03 Historical examples

NIST's malware-handling guidance lists Flip and Invader as multipartite viruses. Other commonly cited examples include Ghostball and OneHalf. These families came from an era when booting from floppy disks and exchanging executable files were major infection paths.

Multipartite infection is less common on current systems because UEFI Secure Boot, signed boot components, modern disk layouts, application controls, and updated endpoint security raise the barrier. Legacy systems, unsupported operating systems, old removable media, and retro-computing environments can still encounter authentic samples.

04 Possible signs

- A specific antivirus alert identifies both infected executables and a boot record.
- Cleaned files become infected again after a restart.
- Executable hashes or sizes change without an authorized update.
- The computer shows boot errors or altered boot records alongside file infections.
- Multiple removable disks become infected after use in the same computer.
- A trusted offline scan reports artifacts that the running operating system did not reveal.

Crashes, slow startup, or file corruption alone are not evidence of a multipartite virus. Hardware failure, disk errors, failed updates, and other malware can cause the same symptoms. Preserve the exact detection name and affected locations.

05 Safe cleanup

1. **Disconnect the computer.** Remove it from networks and stop sharing removable media.
2. **Do not boot other computers from suspect media.** Label and isolate floppy disks, USB drives, external disks, and boot images used with the system.
3. **Preserve evidence and data.** In an organization, involve incident response. Copy essential non-executable documents through a controlled recovery process; avoid carrying programs, scripts, shortcuts, boot images, or unknown archives to clean systems.
4. **Start from trusted external recovery media.** Obtain current vendor media on a clean computer. Scanning only from the infected OS can leave a memory-resident or boot component active.
5. **Scan every affected layer.** Inspect boot records, partitions, system memory where supported, executable files, and removable media.
6. **Prefer a trusted rebuild for confirmed widespread infection.** Repartition or repair the boot chain and reinstall the operating system from known-good media. Do not restore infected executables from backup.
7. **Restore clean data.** Use backups created before the infection, scan them offline, and reinstall applications from original trusted sources.
8. **Verify after restart.** Rescan the boot records and files, then monitor removable media before reconnecting the system.

06 When file repair is unsafe

Some antivirus tools can disinfect a known file infector by removing the virus code. Repair is not guaranteed: the original program may be damaged, the virus may overwrite data, or the exact variant may be unknown. For operating-system and application files, replacement from trusted installation media is generally more reliable. For unique business files, keep forensic copies and use specialist recovery.

07 Prevention

- Keep the OS, firmware, and endpoint security supported and updated.
- Enable Secure Boot where supported and investigate unexpected configuration changes.
- Disable booting from removable media when it is not required and protect firmware settings.
- Use application control and standard-user accounts to limit unapproved executables.
- Scan old or external media before opening files, and never start a computer from unknown media.
- Maintain offline, versioned backups that do not include unverified executable files.

08 Frequently asked questions

Can a multipartite virus survive formatting?

A quick format of one volume may not address every infected disk area or other infected media. A correctly performed repartition and reinstall from trusted media should remove disk-resident infection, but all external media and restored executables must also be checked.

Is a multipartite virus the same as a polymorphic virus?

No. Multipartite describes the locations or methods of infection. Polymorphic describes malware that changes its code representation to make simple signatures less effective. A virus could have both properties.

Does "multiple detections" mean multipartite?

No. The classification requires a virus that infects multiple system areas, classically boot records and files. Several unrelated alerts or several files from one Trojan do not establish that classification.

09 References

- NIST: Guide to Malware Incident Prevention and Handling
- Broadcom: Virus types and multipartite infection
- Bitdefender: Computer virus types

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