R

Resident Virus: How Memory-Resident Malware Works

A resident virus keeps active code in memory so it can infect files while the system is running. Learn how it differs from non-resident and fileless malware, how to detect it, and how to remove it safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How a resident virus works

02 Resident vs. non-resident vs. fileless malware

03 Possible signs of infection

04 How to remove a resident virus

05 How to reduce the risk

06 Frequently asked questions

A **resident virus**, also called a **memory-resident virus**, is a computer virus that loads part of its code into RAM and remains active while the operating system is running. From memory, it can monitor file or disk operations and infect other files when they are opened, copied, or executed. The original infected program may close, but the resident component

can continue working until the computer is shut down or the malicious code is removed.

01 How a resident virus works

1. **Initial execution:** a person runs an infected executable, boot component, macro, or other host file.
2. **Memory installation:** the virus places a replication component in RAM and may hook an operating-system service or file operation.
3. **Interception:** while programs run, the resident code watches for suitable files, removable media, or system events.
4. **Replication:** it adds viral code to new host files. Those files can restart the cycle on the same or another computer.
5. **Optional persistence:** some viruses alter startup locations or system files so an infected component runs again after reboot.

Residence in RAM and persistence across restarts are different concepts. RAM normally loses its contents when power is removed. A resident virus returns after reboot only if an infected file, boot record, or persistence mechanism loads it again.

02 Resident vs. non-resident vs. fileless malware

Term	Main behavior	Important distinction
Resident virus	Keeps a replication component active in memory	Usually has infected files or another launch point
Non-resident virus	Searches for and infects targets when its host runs, then exits	Does not keep its replication module continuously active
Fileless malware	Uses memory and legitimate tools to reduce files on disk	It may not be a self-replicating virus at all

Calling every threat found in RAM a resident virus is therefore inaccurate. Many Trojans, ransomware samples, and legitimate programs use memory but do not replicate by infecting host files.

03 Possible signs of infection

- Security software repeatedly detects infections in different executable files.
- Files appear clean and then become infected again during the same session.
- Previously working programs change size, fail integrity checks, or stop launching.
- Unexpected processes, startup entries, disk activity, or system instability appear.
- Removable drives or shared folders acquire altered executable files.

These symptoms are not proof of a resident virus. A full scan and analysis of the detection name, affected paths, and process activity are needed to distinguish a virus from damaged software or another malware type.

04 How to remove a resident virus

1. Disconnect the computer from networks and removable drives to limit further spread.
2. Do not keep opening files reported as infected. Save the detection log and affected paths.
3. Update trusted security tools from a clean environment when possible.
4. Boot into Safe Mode or, preferably for a persistent infection, a trusted offline recovery scanner. Scanning while the virus is inactive reduces interference.
5. Run a full scan of fixed and removable drives. Clean or replace every infected host, not only the first detected file.
6. Restore damaged programs and system files from verified installation media or a known-good backup.
7. Scan again after a normal reboot. If system files are widely infected or integrity cannot be established, reimage the device.

05 How to reduce the risk

Keep the operating system and security software updated, use real-time protection, restrict untrusted macros and scripts, show file extensions, and avoid unknown executables or cracked software. Disable unnecessary autorun behavior and scan removable media before opening files. Maintain offline or otherwise protected backups; a backup connected during an infection may also contain infected programs.

06 Frequently asked questions

Does restarting remove a resident virus?

A restart clears ordinary RAM, but it does not repair infected files or startup components. If one of them runs again, the virus can return to memory.

Is a resident virus stored in a RAM chip permanently?

No. The term describes code that remains active in working memory during a session. It does not normally mean the malware permanently lives in the physical RAM hardware.

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