Resident Virus - what it is, how it spreads in memory, and how to detect and prevent it

Gridinsoft Help Center

What it is

A resident virus is malware that loads part of itself into memory (RAM) and stays active after the original infected file has closed. Because its code hooks into system functions, it can silently infect other files as they are opened or copied, intercept disk or file operations, and re-trigger on every boot. This memory-resident behavior lets the virus spread and interfere with normal activity across the whole system.

Why it matters

Once resident, the virus can reinfect cleaned files, corrupt programs, slow the system, and hide from simple on-demand scans. Cleanup is harder because the active memory component can restore deleted parts.

How it works

- Load: an infected file runs once, placing the replication module in RAM.
- Hook: the virus attaches to OS/file-system routines (open, copy, execute).
- Infect: as files are accessed, the virus inserts its code into new hosts.
- Persist: reactivates on startup or when certain processes launch.

Red flags

- Cleaned files become re-infected after reboot.
- AV detections jump across many executables in one session.
- Unusual file sizes or sudden "unknown publisher" warnings on trusted apps.
- System sluggishness plus recurring alerts in Temp/AppData paths.

Prevent it

- Keep OS and security tools updated; enable real-time protection.
- If detected, isolate the machine, boot into Safe Mode or a trusted recovery environment, and run a full scan.
- Replace infected system files from known-good sources or backups; consider reimage if infections are widespread.
- Disable autorun on removable media and avoid running unknown executables.