Virut - what it is, why file infections spread fast, and the safest way to recover

Gridinsoft Help Center

What it is

Virut is a Windows file-infecting virus that also turns your PC into part of a botnet. It slips its code into many EXE or SCR files and then connects to attacker-controlled IRC servers to get commands. It changes its look each time (polymorphic), which makes detection and cleaning harder. Basics and examples: https://gridinsoft.com/threats/virut

Why it matters

One Virut hit can corrupt tons of programs, crash Windows, and pull in more malware. For big outbreaks, a full reinstall is often the safest fix.

How it works

- Infect: runs once, then patches other EXE/SCR files it finds.
- Spread: jumps via shared folders and USB drives.
- Control: phones home to IRC to download and run more payloads.
- Persist: any leftover copy can re-infect cleaned files.

Red flags

- Many normal apps suddenly won’t start or get flagged as infected.
- New infections show up after every reboot or scan.
- Unknown processes sending steady traffic to odd servers.
- More crashes than usual, BSODs, or broken executables across folders.

Do it right

- Isolate now: disconnect from the internet and stop using USB drives.
- Back up personal files only (documents, photos). Do not back up EXE or DLL files.
- If infections are widespread, reinstall Windows or restore from a clean image.
- Change passwords from a known-clean device and check accounts for strange logins.
- After rebuild, update Windows and apps, install reputable anti-malware, and scan any backups before restoring.