A

Autorun Worm: USB Symptoms, Safe Removal, and Prevention

Recognize autorun and shortcut-worm symptoms, clean both Windows and affected USB drives safely, recover hidden files, and prevent reinfection.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 31, 2026

READ TIME
4 min

CONTENTS

In this guide

An **autorun worm** is self-replicating malware that spreads through removable media or writable network shares. Older families relied on `autorun.inf` and Windows AutoRun behavior. Modern USB worms often use deceptive `.lnk` shortcuts, scripts, hidden folders, scheduled tasks, and filenames that imitate the user's documents.

01 Is autorun.inf always a virus?

No. `autorun.inf` is a configuration file that has legitimate uses on installation media, and its presence alone does not prove infection. Treat it as suspicious when it launches an unknown executable or script, appears with hidden malware copies or deceptive shortcuts, returns after deletion, or is detected together with other malicious files. Modern Windows restrictions also mean that an ordinary USB drive may not automatically execute the instructions even when the file exists.

02 Common warning signs

- Folders on a USB drive disappear and are replaced by shortcuts with similar names.
- An unexpected `autorun.inf`, script, executable, or hidden system folder appears.
- The same suspicious files return after the USB drive is cleaned.
- Security software reports an Autorun, VBS, shortcut, worm, or removable-media threat.
- Several computers or network shares develop the same files after using one drive.
- Opening a shortcut launches a script interpreter or executable before opening the expected document.

03 AutoRun, AutoPlay, and shortcut worms

AutoRun lets media specify a program or action in an `autorun.inf` file. **AutoPlay** displays choices based on the detected content. Modern Windows versions restrict automatic execution from ordinary USB flash drives, but that does not make unknown removable media safe.

A shortcut worm can hide the real folders and create convincing `.lnk` files. The user starts the malware by opening the shortcut, so no classic AutoRun behavior is required. Other variants use scripts, document macros, or vulnerabilities in software that processes files from the drive.

04 First response

1. Disconnect the affected USB drive and stop sharing it between computers.
2. Disconnect additional writable removable drives and unnecessary network shares.
3. Do not open suspicious shortcuts, scripts, executables, or an unknown `autorun.inf`.
4. Run a full scan of the computer that last wrote the suspicious files.
5. Scan every recently connected drive and other computers that used it.

Cleaning only the USB drive is not sufficient when an infected computer recreates the worm each time the device is connected.

05 Clean Windows and the USB drive safely

1. Update the installed security product and scan the Windows system before reconnecting removable media.
2. Quarantine detected persistence items, scripts, worm copies, and related payloads. Restart if requested and scan again.
3. Disable AutoPlay temporarily while investigating unknown media.
4. Reconnect one affected drive while holding to the security product's recommended safe workflow, then scan the complete drive.
5. Recover documents only after verifying their real file types. Do not copy executables, scripts, or shortcuts merely because they use familiar icons.
6. After cleanup, disconnect and reconnect the drive and repeat the scan to confirm that files do not return.

Do not run an unknown “USB fix” script from a forum. Some scripts recursively change attributes or delete files and can destroy evidence or legitimate data.

06 Recover files that were hidden

Many shortcut worms hide original folders rather than encrypting them. In File Explorer, enable the display of hidden items for inspection, but do not execute unknown files. Confirm that documents open from a clean copy and that their extensions match their actual type.

If the drive contains irreplaceable data, create an image or read-only copy before making changes. Formatting the drive can remove its current contents, but it will not clean the infected computer or restore files that were deleted or overwritten.

07 When several computers may be affected

- Temporarily restrict write access to shared folders.
- Search endpoint and file-server logs for the same filenames, hashes, script commands, and creation times.
- Scan mapped drives and systems that accessed the removable media.
- Reset credentials if the worm delivered an infostealer, keylogger, or remote-access payload.
- Preserve a sample and relevant logs for an authorized incident-response team.

08 Prevent reinfection

- Keep AutoPlay disabled or limited when it is not required.
- Scan removable media before opening its contents.
- Show complete filename extensions and be cautious with shortcut icons.
- Limit write permission on shared storage and block unnecessary script execution.
- Keep Windows, document readers, and security software updated.
- Maintain offline or otherwise protected backups of important files.

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