A

Autorun Worm: How USB-spreading malware works and how to stop it

What it is An autorun worm is self-replicating malware that copies itself to removable media or shared storage and tries to launch when the location is opened. Older variants relied on Windows AutoRun or AutoPlay behavior and an...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

An autorun worm is self-replicating malware that copies itself to removable media or shared storage and tries to launch when the location is opened. Older variants relied on Windows AutoRun or AutoPlay behavior and an autorun.inf file. Newer variants may use deceptive shortcuts or filenames because modern Windows restricts automatic execution.

How it works

After one computer is infected, the worm writes a hidden copy to connected USB drives and may replace visible folders with malicious shortcuts. A user who opens the shortcut starts the worm on another computer. Some variants also spread through writable network shares, steal data, or

download additional malware.

Key points

- Hidden files, unexpected shortcuts, or an autorun.inf file on a USB drive are common warning signs.
- Formatting only the USB drive is not enough if the computer that infected it remains compromised.
- Disabling AutoRun reduces one path, but it does not make unknown removable media safe.

What to do

- Disconnect affected removable drives and scan the host and every recently used drive.
- Show hidden files only for inspection; do not double-click suspicious shortcuts or executables.
- Disable unnecessary AutoPlay, limit write access to shared folders, and keep endpoint protection updated.
- Recover documents from a known-clean backup rather than copying unverified executables back.