N

Neshta (Neshuta): How this file-infecting virus spreads

What it is Neshta, sometimes called Neshuta, is a Windows file-infecting virus. It appends malicious code to executable files and changes how they start, allowing the virus to run whenever an infected program is launched. One infected...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Neshta, sometimes called Neshuta, is a Windows file-infecting virus. It appends malicious code to executable files and changes how they start, allowing the virus to run whenever an infected program is launched. One infected host can contaminate many local programs and files on writable shared locations.

How it works

The virus establishes a way to launch its code and then searches for suitable executable files. Infected files retain the virus and can spread it when copied to another computer. Damage may include corrupted applications, unstable systems, disabled security tools, and secondary malware depending on the variant and infection source.

Key points

- File infectors are harder to clean than a standalone Trojan because many legitimate programs may contain modified code.
- Restoring one executable can fail if another infected file immediately reinfects it.
- Backups made after the infection began may contain contaminated executable files.

What to do

- Disconnect writable shares and removable media before starting cleanup.
- Use trusted boot or offline scanning and replace system and application files from clean installation media.
- Scan backups and shared storage before reconnecting them to rebuilt systems.
- Reinstall the operating system when file integrity cannot be restored with confidence.

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