

S

Salinity: How this polymorphic file-infecting virus spreads

What it is Salinity is a family of polymorphic Windows file-infecting viruses. It modifies executable files so its code runs with the host program and can spread through local storage, network shares, and removable media. Some variants...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

Salinity is a family of polymorphic Windows file-infecting viruses. It modifies executable files so its code runs with the host program and can spread through local storage, network shares, and removable media. Some variants also add backdoor or botnet functions and interfere with security software.

How it works

When an infected file starts, Salinity becomes active and searches for more executable files to modify. Polymorphic changes make infected copies look different at the byte level. Network-enabled variants contact peers or command infrastructure, download additional code, and may block access to security websites or terminate protective processes.

Key points

- Hundreds of alerts can represent legitimate applications infected by one active virus, not hundreds of separate downloads.
- Cleaning while the virus remains active in memory can result in immediate reinfection.
- Damaged executables may not be reliably repairable and should be replaced from a trusted source.

What to do

- Disconnect shared and removable storage and use an offline or trusted boot scan.
- Replace infected system and application files from clean installation media.
- Scan backups and connected devices before restoring or reconnecting them.
- Reinstall the operating system when complete disinfection and file integrity cannot be confirmed.

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](https://support.gridinsoft.com)