S

Sality Malware: File Infection, Warning Signs, and Recovery

Learn how the polymorphic Sality family infects Windows executable files, weakens security, spreads through removable media, and complicates cleanup.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 31, 2026

READ TIME
3 min

CONTENTS

In this guide

Sality is a long-running family of polymorphic Windows file infectors. Variants insert malicious code into executable files, interfere with security software, spread through removable media or shares, and may join peer-to-peer infrastructure to obtain additional components.

Because many files can be altered across a system or network, Sality cleanup is more complex than deleting one detected executable.

01 What does Sality mean?

In cybersecurity, Sality is the family name used for this Windows malware, including detections such as Win32/Sality. It is not a description of one specific file: different variants and security vendors may use additional suffixes. Confirm the complete detection name and affected file before choosing a recovery method.

02 How Sality infects files

File-infecting variants modify eligible Windows executables so the malicious code runs when an infected program starts. Polymorphism changes portions of the malware between infections, making simple hash matching less effective. Damaged or incorrectly cleaned files may no longer work.

03 How it spreads

- Execution of an already infected program.
- Writable network shares containing executable files.
- Removable drives and unsafe autorun-related behavior in older environments.
- Other malware that installs a Sality variant.
- Reintroduction from an unclean backup, software repository, or neighboring device.

04 Additional malicious behavior

Depending on the variant, Sality can terminate security processes, modify system settings, block access to security sites, create persistence, and download more malware. Some variants communicate through a peer-to-peer network, which avoids dependence on one fixed command server.

05 Warning signs

Possible indicators include many unrelated executable files receiving detections, security software closing or failing to update, programs becoming corrupted, unknown network activity, and infections returning after cleanup. These signs are not unique to Sality, so preserve samples and use reliable family identification.

06 Immediate response

1. Disconnect the affected device from networks and removable storage.
2. Stop using shared software repositories until they are checked.
3. Preserve alerts, hashes, logs, and representative samples.
4. Scan neighboring systems and removable media with updated tools.
5. Protect credentials from a known-clean device if theft is possible.

07 Cleaning vs. rebuilding

A vendor-supported disinfecting tool may repair some known variants, but large numbers of modified files create integrity risk. If system files, security components, or trusted software repositories are affected, rebuilding from known-good media is often safer. Restore documents and data, not executable files of uncertain origin.

08 Recovery checklist

Patch the rebuilt system, update security tools, disable unnecessary legacy sharing and autorun behavior, rotate exposed credentials, and scan backups before restoration. Verify business applications from original signed installers. Monitor for renewed detections and peer-to-peer traffic before reconnecting broadly.

09 Preventing reinfection

Use application control, least privilege, supported operating systems, segmented networks, protected software repositories, and removable-media policy. Download programs only from official sources. Do not copy an executable from an infected machine merely because it still launches.

10 Sality vs. a Trojan

Sality is notable for infecting and replicating through executable files. A Trojan disguises itself or relies on users to run it and does not self-replicate by definition. A Sality infection can still download Trojan payloads.

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