P

W32/Parite (Pinfi) Virus: File Infection, Removal, and Recovery

W32/Parite, also called Pinfi or Packed.Parite, is a polymorphic Windows file-infector that modifies executable files and writable network shares. Learn how to contain and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 4, 2026

READ TIME
4 min

CONTENTS

In this guide

W32/Parite is a family of polymorphic Windows file-infecting viruses. It is also known by aliases such as **W32/Pinfi**, Win32.Parite, PE_PARITE, and Packed.Parite. Once active, it modifies executable files on local disks and writable network shares, allowing those infected programs to spread the virus when they run.

Why cleanup is difficult: many detections can be legitimate applications that Parite modified, not many separately downloaded malware files. Deleting every detected executable can break Windows and installed software, while restoring programs too early can let the active virus infect them again.

01 How W32/Parite infects files

Microsoft describes Parite as a packed, encrypted, polymorphic file infector targeting `.exe` and `.scr` executable files. An active component repeatedly selects another eligible file, appends viral code, and changes its entry point so the added code runs first. The original program can still appear to work, which makes infection less obvious.

1. An infected executable runs and activates the virus.
2. The virus places code in memory and can inject into a normal Windows process.
3. It searches local storage and writable network shares for executable targets.
4. Each infected file becomes another carrier when someone or the system launches it.
5. Clean executables restored while the virus is active may be infected again.

Parite is described as polymorphic because it changes or re-encrypts portions of its code while spreading. This variation can complicate simple hash-based detection, though modern security tools also inspect structure and behavior.

02 Common aliases and what they mean

Name	Context
Win32/Parite or W32/Parite	Common family name for the Windows file infector
W32/Pinfi	Alias used by some security vendors
Packed.Parite	Highlights the packed or obfuscated form of an infected sample
PE_PARITE	Refers to infection of Windows Portable Executable files

The exact suffix may identify a variant or detection method, but the response should account for a resident file-infector across the whole environment.

03 Signs of a Parite infection

- detections appear across many unrelated applications;
- clean executables become detected again after they are copied back;
- detections occur on a writable shared folder or removable drive;
- application files change size or hash without a vendor update;
- security software reports Parite, Pinfi, or similar aliases in multiple locations.

These clues are not unique to Parite. Confirm with the full security report and avoid manually executing suspected files to “test” them.

04 How to remove W32/Parite safely

1. **Stop the spread.** Disconnect the affected computer from writable network shares and remove external media. Temporarily revoke write access to contaminated shares.
2. **Preserve personal data.** Back up documents, photos, and other non-executable data to controlled storage. Do not copy programs, scripts, screensavers, or unknown installers into the clean backup set.
3. **Scan outside the normal infected session.** Use a trusted offline or boot-time scanner so the resident component is not actively reinfecting files.
4. **Follow the security vendor's Parite procedure.** File disinfectors may repair some host files, but not every modified executable can be trusted or restored reliably.
5. **Replace software from clean sources.** Reinstall Windows components and applications from official media or verified packages instead of copying binaries from another potentially affected host.
6. **Scan every reachable location.** Include writable shares, removable drives, deployment folders, and backups containing executable files.

7. **Verify before reconnecting.** Restart, rescan, and monitor file hashes or modification activity. Reconnect shares only after all participating systems are clean.

05 When a clean reinstall is safer

Reimage the device when system files are widely infected, disinfection repeatedly fails, the original clean binaries are unavailable, or the integrity of the operating system cannot be demonstrated. On business networks, rebuild from a known-good image and reset compromised software-distribution shares before bringing endpoints back.

Do not format or erase the only disk before preserving irreplaceable non-executable data and evidence. The goal is to replace programs while retaining safe user content, not to destroy everything indiscriminately.

06 Frequently asked questions

Can Parite infect documents and photos?

Parite primarily targets executable file types such as EXE and SCR. Documents or photos may still reside on an affected disk, but they are not the same kind of executable carrier. Scan all restored data because other malware may be present.

Why does W32/Parite return after removal?

An infected executable, another active endpoint, a writable share, removable media, or an unclean software package can reintroduce it. Cleanup must cover every carrier and stop the in-memory infection before files are restored.

Should every detected EXE be deleted?

No. Some can be replaced or disinfected, and deleting system executables can make Windows unbootable. Use a vendor-supported cleanup process or rebuild from trusted media.

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