F

# Floxif Malware: File Infection, Safe Cleanup, and Recovery

Floxif is a Windows file-infecting virus that modifies executable and DLL files. Widespread infection often makes a clean rebuild safer than selective repair.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

**Floxif** is a Windows file-infecting malware family. Microsoft classifies **Virus:Win32/Floxif** as a virus that infects executable and DLL files and can download or install additional malware. This is different from a trojan that merely arrives as one standalone malicious file.

When an infected program runs, Floxif code can execute with it and spread to other eligible files. Quarantining the first detected installer may therefore be insufficient if the payload already ran.

## What Floxif can affect

- Windows executable files and dynamic-link libraries;
- installed application folders and copied portable programs;
- additional drives or backups containing executable content;

- system integrity through downloaded secondary malware.

Microsoft's Floxif threat description notes that opening an infected executable or DLL launches the malicious payload.

## Interpret the detection before acting

- one file in an unopened archive may mean the infection was blocked before execution;
- detections across unrelated installed programs strongly suggest active file infection;
- detections in File History, backups, or external drives may be inactive but can reinfect a rebuilt system if restored and run;
- a heuristic family label should be confirmed through the security product's details and, when needed, vendor analysis.

## Immediate response

1. **Disconnect the computer and removable drives.** Do not launch or copy applications from the affected system.
2. **Record detections.** Preserve file paths, hashes, scan results, execution history, and the suspected source.
3. **Use an offline or trusted full scan.** This helps find infected files that are locked while Windows is running and identifies secondary payloads.
4. **Assess spread.** Multiple infected system or application files reduce confidence that selective disinfection will produce a trustworthy machine.

## Recovery options

If detection was limited to an unopened file and investigation confirms it never ran, quarantine it and rescan. If applications are infected, uninstall them and reinstall signed copies from their official publishers rather than trusting repaired binaries.

For widespread infection, altered system files, repeated detections, or an uncertain timeline, erase the affected system volume and reinstall Windows from trusted media. Update it before restoring data.

Before rebuilding, check whether the same installer or executable was deployed to other endpoints. Compare hashes and detection timelines, isolate affected hosts, and invalidate software-distribution packages that contain infected binaries. A clean endpoint should not receive files from an unverified peer.

## Preserve personal data without reinfection

- prioritize documents, photos, videos, and other non-executable personal data;
- do not restore EXE, DLL, SCR, MSI, scripts, installers, cracks, macros, or unknown archives from the infected system;
- scan backup media from a clean, updated environment before opening files;
- reinstall applications from publishers instead of restoring program folders.

## After cleanup

Investigate the original installer or download source, update applications, and remove cracks or repacks. If a secondary stealer or backdoor was found, revoke sessions and change exposed credentials from a clean device. Monitor removable drives and backups so they do not reintroduce infected executables.

## Floxif FAQ

**Can antivirus repair every infected file?**

No. Repair may be unavailable or leave a damaged file. Replacement from a trusted original is safer.

**Can photos carry Floxif?**

The family targets executable code, but scan all restored data and beware of disguised extensions or archives.

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**