B

Bifrose: What this backdoor Trojan does and how to respond

What it is Bifrose, also written Bifrost, is a family of Windows backdoor Trojans and remote-access tools. Once installed, it can let an unauthorized operator control the computer, browse or transfer files, capture information, run...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Bifrose, also written Bifrost, is a family of Windows backdoor Trojans and remote-access tools. Once installed, it can let an unauthorized operator control the computer, browse or transfer files, capture information, run commands, and install more malware. Its presence should be treated as a full system compromise.

How it works

Bifrose has historically been delivered through malicious attachments, bundled installers, or another loader. The malware creates persistence and connects to command-and-control infrastructure for instructions. Different variants can hide their process or configuration and may use misleading filenames that resemble legitimate Windows components.

Key points

- Unexpected outbound connections, new startup entries, and security tools being disabled can accompany an infection.
- Removing one visible file does not prove that downloaded payloads or stolen credentials are gone.
- Remote access means documents, browser sessions, and passwords used on the device may be exposed.

What to do

- Disconnect the computer from the network and preserve relevant endpoint and network logs.
- Run a trusted offline or full-system scan and investigate persistence before reconnecting the device.
- Change passwords from a clean system and revoke active sessions for important accounts.
- Reimage the computer when the scope cannot be established 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