GRIDINSOFT

HELP CENTER

OFFICIAL SUPPORT GUIDE

P

Padodor: What this Windows backdoor can steal and how to respond

What it is Padodor is a Windows backdoor Trojan associated with unauthorized remote access and information theft. Depending on the sample, an attacker may be able to execute commands, transfer files, collect system or user data, and...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Padodor is a Windows backdoor Trojan associated with unauthorized remote access and information theft. Depending on the sample, an attacker may be able to execute commands, transfer files, collect system or user data, and install additional malware. A confirmed infection means the device should not be trusted for sensitive activity.

How it works

The backdoor can be delivered by another loader, a deceptive download, or a malicious attachment. It establishes persistence and communicates with attacker-controlled infrastructure. Historical family names can cover several variants, so exact capabilities and indicators should be confirmed from the detected sample and surrounding system activity.

Key points

- Remote access may expose credentials, documents, and other systems reachable from the infected account.
- The absence of visible windows or performance issues does not mean the backdoor is inactive.
- Deleting the detected file alone does not address persistence, secondary payloads, or stolen secrets.

What to do

- Disconnect the endpoint and retain process, network, account, and persistence evidence.
- Use a trusted scan and rebuild the host if the full infection chain is uncertain.
- Reset credentials and revoke sessions from a clean computer.
- Review neighboring systems and shared accounts for lateral movement or reuse.

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