D

Dridex: How this banking Trojan steals data and enables attacks

What it is Dridex is a modular Windows banking Trojan associated with credential theft, fraudulent transactions, and delivery of additional malware. It evolved from earlier banking-malware code and has been distributed in large email...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

Dridex is a modular Windows banking Trojan associated with credential theft, fraudulent transactions, and delivery of additional malware. It evolved from earlier banking-malware code and has been distributed in large email campaigns. A Dridex infection can expose financial accounts as well as business credentials stored or entered on the computer.

How it works

Delivery commonly starts with a malicious Office document, archive, link, or script in an email. Once launched, a loader retrieves the main components and establishes persistence. Modules can capture browser or form data, redirect sessions, record keystrokes, collect system

information, and download other payloads, including ransomware used in later campaigns.

Key points

- A convincing invoice or business document is not safe merely because it uses familiar branding.
- Bank fraud may occur before obvious performance or security symptoms appear on the endpoint.
- Removing the malware does not invalidate credentials or payment details already stolen.

What to do

- Disconnect the device and contact the financial institution through a verified channel when banking data may be exposed.
- Scan or reimage the endpoint, then change passwords from a known-clean system.
- Review mail rules, authentication logs, and recent transactions for secondary abuse.
- Block executable attachments and scripts that are not required by business workflows.