D

Dyreza: What this banking Trojan steals and how to respond

What it is Dyreza, also known as Dyre, is a Windows banking Trojan first widely reported in 2014. It was designed to steal online-banking credentials and other sensitive information by interfering with browser sessions. Campaigns...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Dyreza, also known as Dyre, is a Windows banking Trojan first widely reported in 2014. It was designed to steal online-banking credentials and other sensitive information by interfering with browser sessions. Campaigns targeted consumers and organizations, and infected systems could also be enrolled in infrastructure used by the operators.

How it works

Dyreza commonly arrived through phishing messages carrying malicious documents or links. After execution, it established persistence, connected to command servers, and monitored browser traffic. Web-inject or redirection techniques could present altered pages and capture credentials even when the legitimate banking site used HTTPS.

Key points

- A correct padlock icon does not protect data after malware has compromised the local browser or operating system.
- Unexpected transaction prompts, changed banking pages, and suspicious email attachments are important warning signs.
- Credentials used after infection should be considered exposed even if no fraudulent payment is visible yet.

What to do

- Stop online banking on the affected computer and contact the bank through a known number.
- Disconnect and clean or rebuild the device before entering replacement credentials.
- Reset passwords and revoke sessions from a clean device, then review recent transactions.
- Use attachment filtering, user training, and application controls to reduce malicious document execution.

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