



Shylock: How this banking Trojan intercepted financial sessions

What it is Shylock was a Windows banking Trojan designed to steal online-banking credentials and support fraudulent transactions. Named after a character in Shakespeare's The Merchant of Venice, it used browser interception and modular...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

Shylock was a Windows banking Trojan designed to steal online-banking credentials and support fraudulent transactions. Named after a character in Shakespeare's The Merchant of Venice, it used browser interception and modular functions to collect sensitive data from infected users, especially in selected countries and financial institutions.

How it works

The malware spread through compromised websites, exploit kits, and malicious downloads. After installation, it injected into browser activity, captured form data and credentials, and could alter what the user saw during a banking session. Command infrastructure delivered configuration and

modules tailored to particular targets.

Key points

- Browser-session manipulation can occur after a user reaches the real HTTPS site, so the padlock alone is not enough.
- Banking Trojans may remain quiet until a targeted financial site is opened.
- Shylock is mainly a historical family, but web-inject and credential-theft techniques continue in newer malware.

What to do

- Stop financial activity on the affected device and contact the bank through a verified channel.
- Clean or rebuild the system before changing credentials from a known-safe device.
- Review transactions, account recovery methods, and active sessions for unauthorized changes.
- Patch browsers and plugins and block untrusted downloads and script 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](https://support.gridinsoft.com)