S

Shylock Banking Trojan: Man-in-the-Browser Fraud and Account Recovery

Shylock was a Windows banking Trojan that used man-in-the-browser techniques to steal credentials and manipulate financial sessions. Learn its history and the correct account response.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How Shylock banking fraud worked

02 Shylock takedown and continuing relevance

03 Possible signs of a banking Trojan

04 What to do after a Shylock or banking-Trojan alert

05 Why changing only the bank password is insufficient

06 Frequently asked questions

Shylock was a modular Windows banking Trojan first identified around 2011. It targeted online-banking users with man-in-the-browser techniques, credential theft, and fraudulent session manipulation. Its name came from text associated with Shakespeare's *The Merchant of Venice* found in the malware.

Historical status: an international law-enforcement and industry operation disrupted Shylock's command infrastructure in July 2014. A modern “Shylock” alert is therefore likely to involve an old sample, an archived system, or a vendor family label, but any confirmed banking Trojan still requires immediate financial and credential response.

01 How Shylock banking fraud worked

Shylock could inject itself into browser activity and wait until the victim visited a targeted financial site. The user might be on the bank's genuine HTTPS domain while malicious code inside the compromised computer captured form data, altered content, or inserted fraudulent prompts. This is why the browser padlock alone could not protect an infected endpoint.

1. **Initial infection:** malicious links, compromised sites, exploit kits, or deceptive downloads delivered the Trojan.
2. **Persistence and control:** the malware established itself and contacted command-and-control infrastructure.
3. **Target configuration:** operators supplied rules for selected banks, regions, or online services.
4. **Browser interception:** web injects and form grabbing collected credentials or changed the session.
5. **Fraud:** stolen access and manipulated transactions moved funds toward criminal accounts.

Some versions also included modules for additional data theft and remote functions. As with other modular banking Trojans, the visible family name may describe only part of the infection.

02 Shylock takedown and continuing relevance

Europol reports that the 2014 operation seized or redirected servers and domains supporting the Shylock botnet. At least 30,000 Windows computers were believed to have been infected, with strong targeting of UK users as well as victims in other countries.

The infrastructure disruption reduced the historical operation, but the techniques remain relevant. Modern banking malware still uses web injections, session theft, keylogging, overlays, and stolen browser data. The practical lesson is to verify financial activity through a clean channel, not to focus only on whether Shylock itself is still active.

03 Possible signs of a banking Trojan

- unexpected fields, delays, or security prompts appear only during a banking session;
- the bank reports a transfer, payee, device, or login the user does not recognize;
- a security alert identifies Shylock, a banker, web inject, form grabber, or credential stealer;
- the browser process creates unusual child processes or network connections;
- security tools are disabled or updates repeatedly fail;
- the user receives MFA prompts or account-recovery messages they did not initiate.

These symptoms are not proof of Shylock specifically. Preserve the complete detection and financial timeline instead of installing an old family-specific removal tool.

04 What to do after a Shylock or banking-Trojan alert

1. **Stop financial activity on the device.** Disconnect it and do not use it to contact the bank or change passwords.
2. **Call the financial institution through a verified number.** Report the suspected compromised session, review pending transfers and payees, and follow its fraud procedure.
3. **Use a clean device for account recovery.** Reset email and banking credentials, revoke sessions, and update recovery information.

4. **Preserve evidence.** Save alerts, suspicious messages, transaction identifiers, browser and endpoint logs, and the approximate infection time.
5. **Scan or rebuild the endpoint.** Remove persistence and companion payloads. Reimage when integrity or privileged activity cannot be established.
6. **Review all affected accounts.** Check reused passwords, business payment systems, cards, mailbox rules, and stored browser credentials.

05 Why changing only the bank password is insufficient

The Trojan may have captured email access, recovery information, session cookies, and passwords reused elsewhere. An attacker controlling email can reset financial accounts again. Secure the root identity accounts first, revoke sessions, and monitor transactions after restoration.

06 Frequently asked questions

Is Shylock the same as phishing?

No. Phishing can deliver a banking Trojan, but Shylock operated on the infected computer and could interfere with a real banking session.

Does HTTPS stop a man-in-the-browser attack?

HTTPS protects traffic between the browser and the bank. It cannot guarantee the browser process or operating system is clean before data is encrypted or after it is displayed.

Can an old Shylock sample still be dangerous?

Yes. Even if historical command servers are unavailable, executing archived malware is unsafe, and a detection may indicate other components. Quarantine and investigate it.

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