S

SpyEye Banking Trojan: History, Behavior, and Response

SpyEye was a criminal banking-Trojan toolkit used to steal financial credentials, manipulate browser sessions, and build botnets. Learn how it worked and how to respond to a detection or suspected account theft.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
4 min

CONTENTS

In this guide

SpyEye was a Windows banking-Trojan toolkit used primarily around 2009–2011 to steal financial and personal information and operate botnets. Criminal customers could purchase and configure the toolkit for their own targets and command-and-control servers. The FBI reported that SpyEye infected more than 1.4 million computers and was

designed to facilitate theft from financial institutions and their customers.

SpyEye is historically significant rather than a label for every modern banking attack. Old samples and detection names can still surface, while newer malware uses similar browser-interception techniques. Confirm the exact file and incident timeline instead of assuming a current global SpyEye campaign.

01 What SpyEye could do

Capabilities varied by version and customer configuration. Public FBI and U.S. Department of Justice accounts documented functions including:

- Capturing credentials and personal data entered into web browsers.
- **Form grabbing**, which collects submitted form values before normal transport protection can help.
- Installing a keylogger to record input.
- Stealing credit-card and online-banking information.
- Manipulating banking activity and enabling fraudulent transactions.
- Receiving commands through operator-controlled infrastructure.
- Using infected computers as a botnet, including optional denial-of-service activity.

A toolkit buyer could choose modules and target institutions, so one sample may not contain every function.

02 How a SpyEye attack worked

1. **Delivery:** exploit kits, malicious downloads, phishing, or another malware component infected a Windows computer.
2. **Persistence:** the Trojan arranged to start again and connected to a customer's command-and-control server.
3. **Browser monitoring:** it watched targeted sites and intercepted information inside the compromised endpoint.

4. **Collection:** credentials, payment data, form content, and other identifying information were sent to the operator.
5. **Fraud:** criminals used the stolen access or browser manipulation to attempt unauthorized transactions.

TLS can protect data between a browser and bank, but it cannot make an already compromised endpoint trustworthy. Malware that reads form data or modifies the browser session acts before encryption or after decryption.

03 Possible signs and evidence

- A security alert naming SpyEye or a related banking-Trojan component.
- Unknown browser injection, keylogging, persistence, or suspicious network detections.
- Unrecognized payees, transfers, account-recovery changes, or device registrations.
- Logins from unfamiliar locations or sessions that remain active after a password change.
- A malicious attachment, exploit-kit redirect, or executable preceding the financial activity.

Financial fraud can also result from phishing, credential reuse, SIM swapping, or account takeover without endpoint malware. Correlate endpoint, identity, email, browser, and bank evidence.

04 What to do after a suspected infection

1. **Stop financial activity on the device** and disconnect it from networks.
2. **Contact affected institutions** using a verified phone number or app on a clean device. Ask about holds, transaction review, payees, and account recovery.
3. **Preserve evidence:** alert details, file hashes, process trees, network destinations, messages, browser history, and transaction times.
4. **Protect accounts from a clean device.** Reset passwords, revoke sessions, review recovery methods, and enable phishing-resistant MFA where available.

5. **Scan and scope.** Look for additional payloads, persistence, stolen browser data, and other endpoints receiving the same delivery.
6. **Rebuild if necessary.** A system used for financial access should be reimaged when infection or administrative compromise cannot be fully bounded.
7. **Continue monitoring** bank, email, identity, and credit activity according to the exposed information and local guidance.

05 Prevention lessons

Keep operating systems, browsers, and document software supported and patched; filter risky email and web content; restrict local administrator access; and monitor unusual browser child processes and credential access. Use unique passwords and MFA, but remember that stolen session tokens and endpoint manipulation can bypass some login protections. Transaction signing or confirmation on an independent trusted channel offers stronger protection for high-risk payments.

06 Frequently asked questions

Is SpyEye the same as Zeus?

They were distinct banking-malware toolkits with overlapping criminal markets and techniques. Later reporting described code and feature convergence, but the names should not be treated as interchangeable for incident identification.

Does changing the bank password remove SpyEye?

No. Change credentials from a clean device, revoke sessions, and clean or rebuild the infected endpoint. Otherwise new credentials can be captured again.

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