

SpyEye (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:07:03 UTC

SpyEye is a malware targeting both Microsoft Windows browsers and Apple iOS Safari. Originated in Russia, it was available in dark forums for \$500+ claiming to be the "The Next Zeus Malware". It performed many functionalities typical from bankers trojan such as keyloggers, auto-fill credit card modules, email backups, config files (encrypted), http access, Pop3 grabbers and FTP grabbers. SpyEye allowed hackers to steal money from online bank accounts and initiate transactions even while valid users are logged into their bank account.

► [TLP:WHITE] win_spyeye_auto (20251219 | Detects win.spyeye.)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.spyeye>