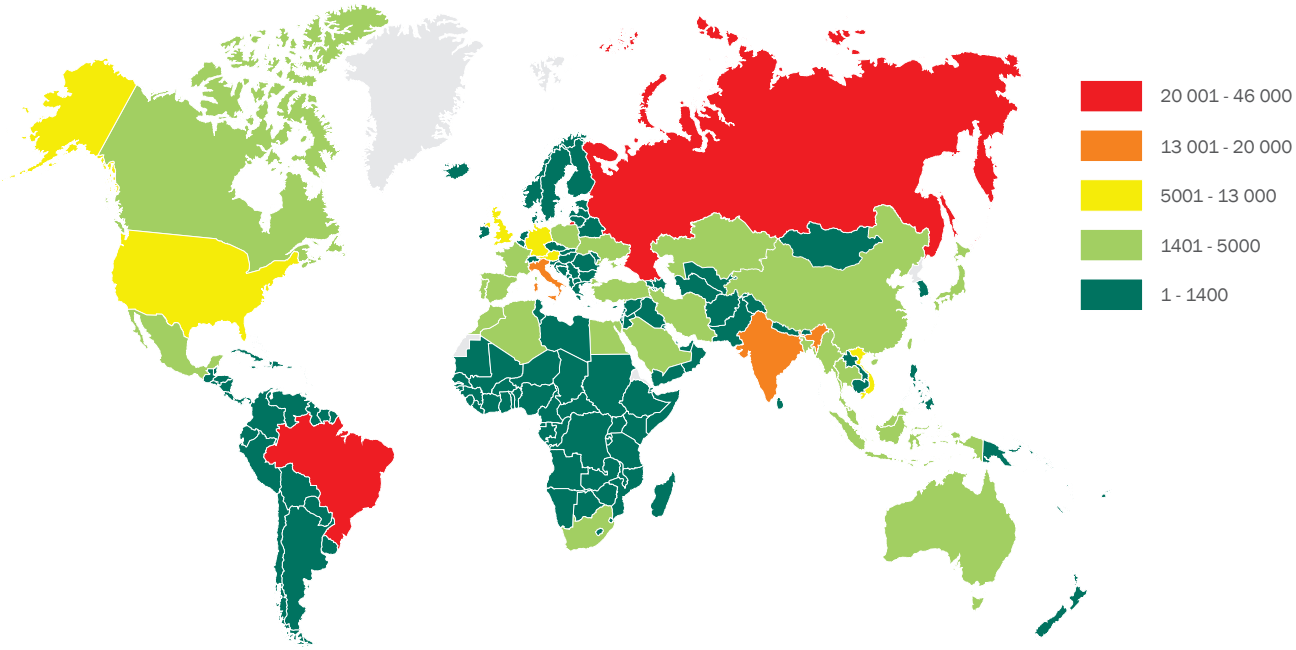
MONTHLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD:
18.03–18.04.2014

One of the main events during the reporting period was the discovery of the Heartbleed bug in the OpenSSL encryption software that allowed unauthorized access to memory on connected clients or servers. Details on this and other detected threats can be found in the section 'Key events in the online banking sphere' below.

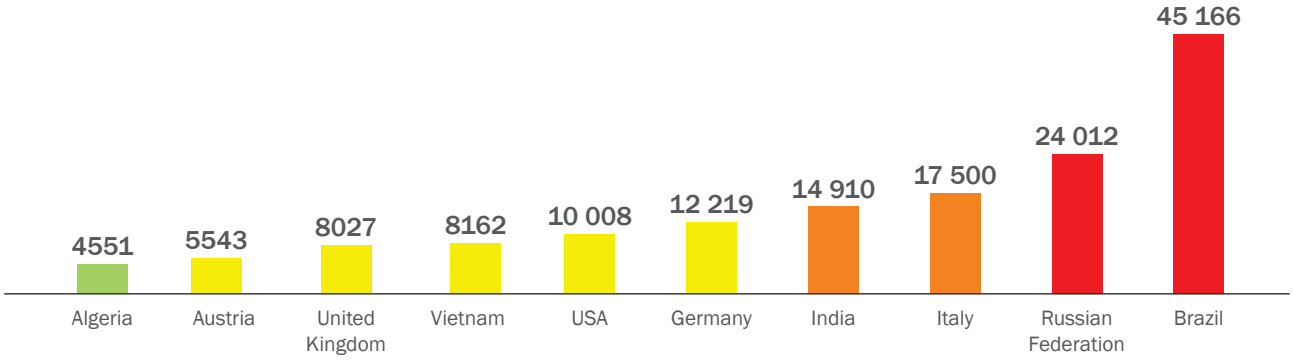
Overall statistics

During the reporting period, Kaspersky Lab solutions blocked 249,812 attempts on user computers to launch malware capable of stealing money from online banking accounts. This figure represents a 1.3% drop compared to the previous reporting period (253,000).



Number of users targeted by banking malware

The number of users attacked using these types of programs during the reporting period is shown in the diagram below (Top 10 rating based on the number of users attacked, in descending order):



KASPERSKY lab

The table below shows the programs most commonly used to attack online banking users, based on the number of infection attempts:

Total notifications of attempted infections by banking malware:

879 739

Verdict*	Number of users	Number of notifications
Trojan-Spy.Win32.Zbot	159688	581841
Trojan-Banker.Win32.Agent	21742	62205
Trojan-Banker.HTML.Agent	13757	35349
Trojan-Banker.Win32.Lohmys	14527	32874
Trojan-Banker.Win32.ChePro	17370	28461
Trojan-Banker.Win32.Banker	9137	27495
Trojan-Banker.AndroidOS.Faketoken	15018	23257
Trojan-Spy.Win32.Spyeyes	5284	20857
Trojan-Banker.Win32.Banbra	7163	14128
Trojan-Banker.HTML.PayPal	2481	6569

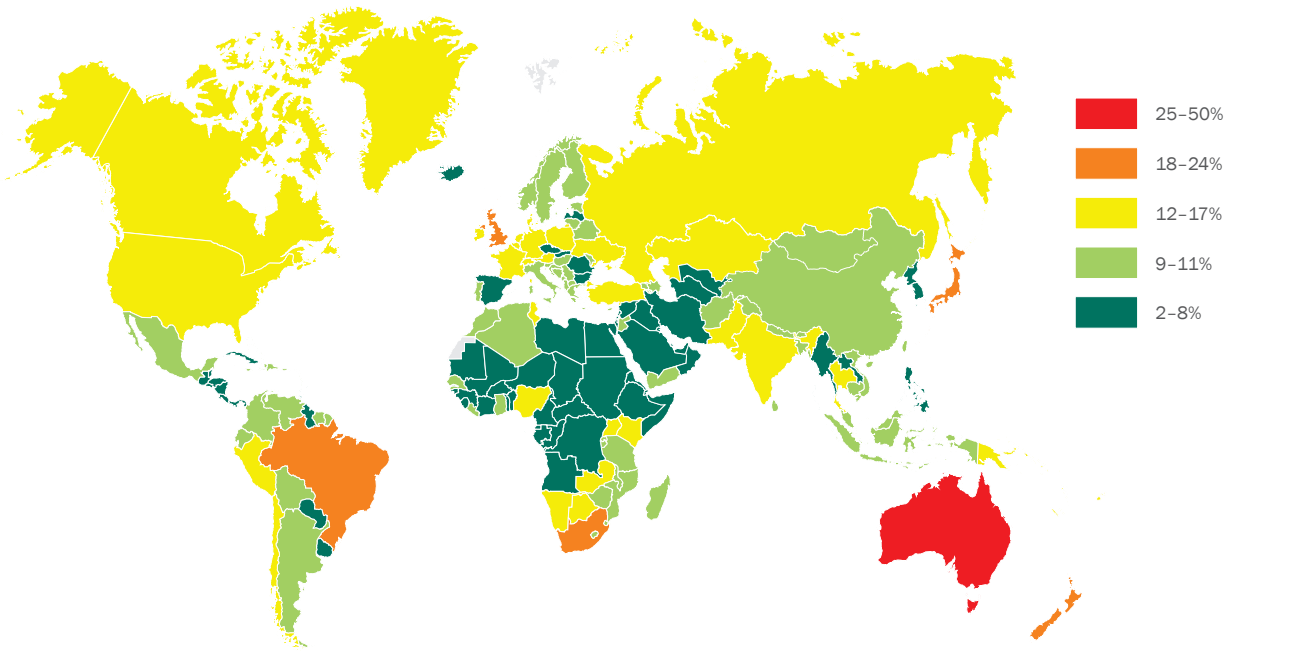
*verdicts are limited exclusively to banking threats (based on an expert assessment of malware functionality)

Zeus (Trojan-Spy.Win32.Zbot) was once again the most widespread banking Trojan. According to Kaspersky Lab's research, the program was involved in 53% of malware attacks on online banking clients.

Trojan-Banker.Win32.ChePro and Trojan-Banker.Win32.Lohmys are representatives of the same family and spread via spam emails bearing the subject line "Internet bank charges". The message contains a Word document with an embedded image that launches malicious code if the recipient clicks on it.

As well as web injections (modification of a bank's HTML pages) four of the 10 entries also make use of keylogging technology, which suggests this method of stealing information is still effective when carrying out attacks on online banking customers.

Worm.Win32.Cridex is a self-propagating program that targets a large number of major international banks and payment systems. The main aim of the attacks is to steal users' bank card details. The program spreads via email, instant messengers, infected removable media, etc.

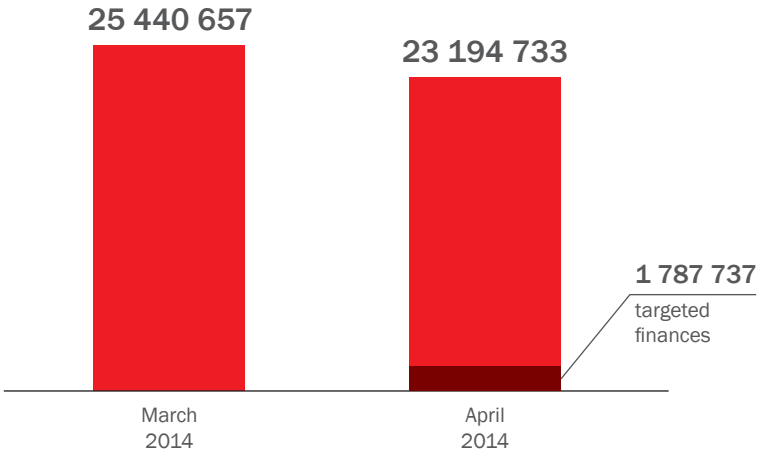


The notifications triggered by Kaspersky Lab's anti-phishing technology as a proportion of all users in a country

KASPERSKY lab

The overall number of anti-phishing notifications:

23 194 733



Key developments in the online banking sphere

- Information appears about a vulnerability in OpenSSL that makes it possible to gain unauthorized access to secret keys, user logins and passwords and other content that is meant to be encrypted https://www.openssl.org/news/secadv_20140407.txt
- New NeoPocket ATM malware detected http://securityblog.s21sec.com/2014/04/neopocket-new-atm-malware.html
- New modification of the Zeus banking Trojan with a signed certificate detected http://www.reuters.com/article/2014/02/22/apple-encryption-idUSL2N0LR0GW20140222
- New type of 'Man-in-the-Middle' attack discovered that changes DNS settings in combination with technology for changing SSL certificates http://blog.phishlabs.com/new-man-in-the-middle-attacks-leveraging-rogue-dns
- Information published about the ZeusVM banking Trojan that spreads using steganography http://www.xylibox.com/2014/04/zeusvm-and-steganography.html
- Data stolen from 3 million Michaels Stores credit and debit cards http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/
- Kaspersky Lab publishes its Financial Cyber Threats report for 2013 http://www.securelist.com/en/analysis/204792330/Financial_cyber_threats_in_2013_Part_1_phishing

The main source of information for this report is Kaspersky Lab's cloud infrastructure — the Kaspersky Security Network, which receives anonymous statistical data from users of Kaspersky Lab software products. Kaspersky Security Network has over 60 million home and corporate users.

KASPERSKY lab