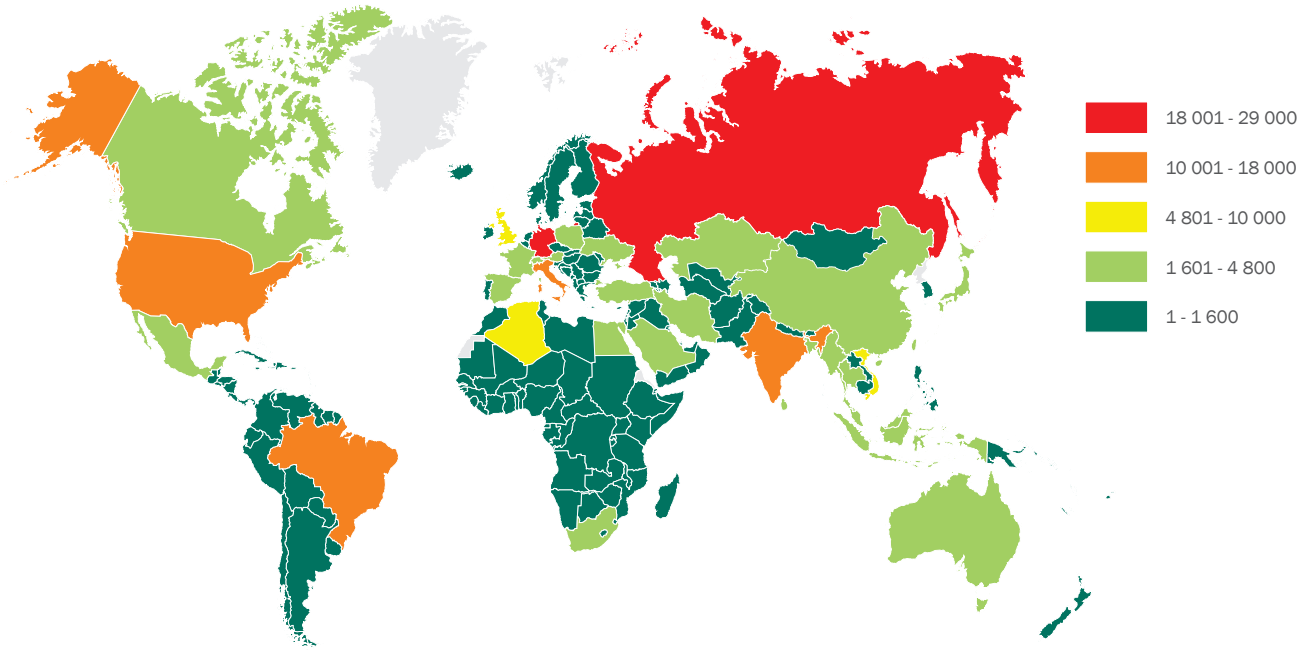
MONTHLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD: 17.01–17.02.2014

One of the main events during the reporting period was the detection of two fundamentally new malicious programs designed to attack users of online banking services and the use of sporting themes when distributing them. Details on this and other detected threats can be found in the section 'Key threats in the online banking sphere' below.

Overall statistics

During the reporting period, Kaspersky Lab's protection mechanisms blocked 243,368 attempts on user computers to launch malware capable of stealing money via online access to bank accounts. This figure represents a 23.6% growth compared to the previous reporting period (196,905).

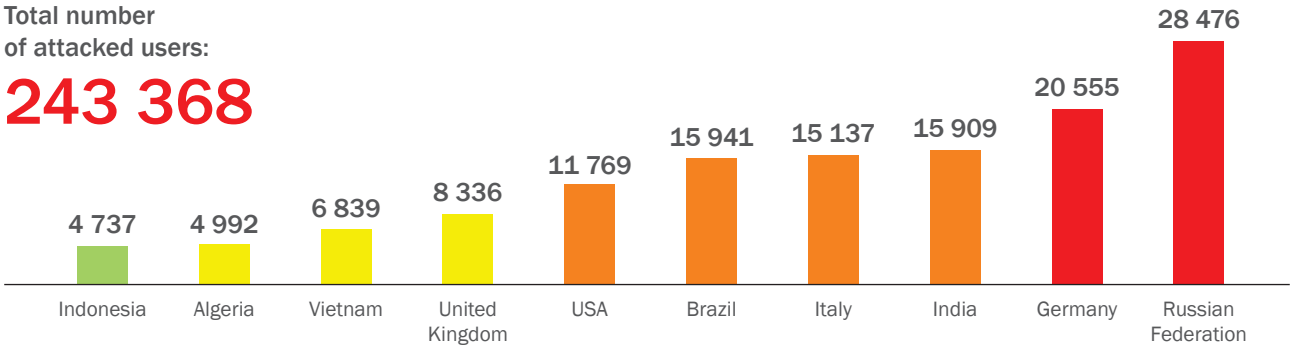


Map showing the number of users that encountered banking malware

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

Total number of attacked users:

243 368



KASPERSKY lab

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

Total notifications about infection attempts:

2 545 415

Verdict	Number of users	Number of notification
Trojan-Spy.Win32.Zbot	187506	1357433
Worm.Win32.Cridex	4028	891564
Trojan-Spy.Win32.Spyeyes	4306	163390
Trojan-Banker.HTML.Agent	11162	23203
Trojan-Banker.Win32.Banker	6261	20455
Trojan-Banker.Win32.Agent	6810	18382
Trojan-Banker.AndroidOS.Faketoken	8354	13088
Trojan-Banker.Win32.ChePro	6436	9973
Trojan-Banker.Win32.Banbra	4491	8293
Backdoor.Win32.Shiz	3527	7926

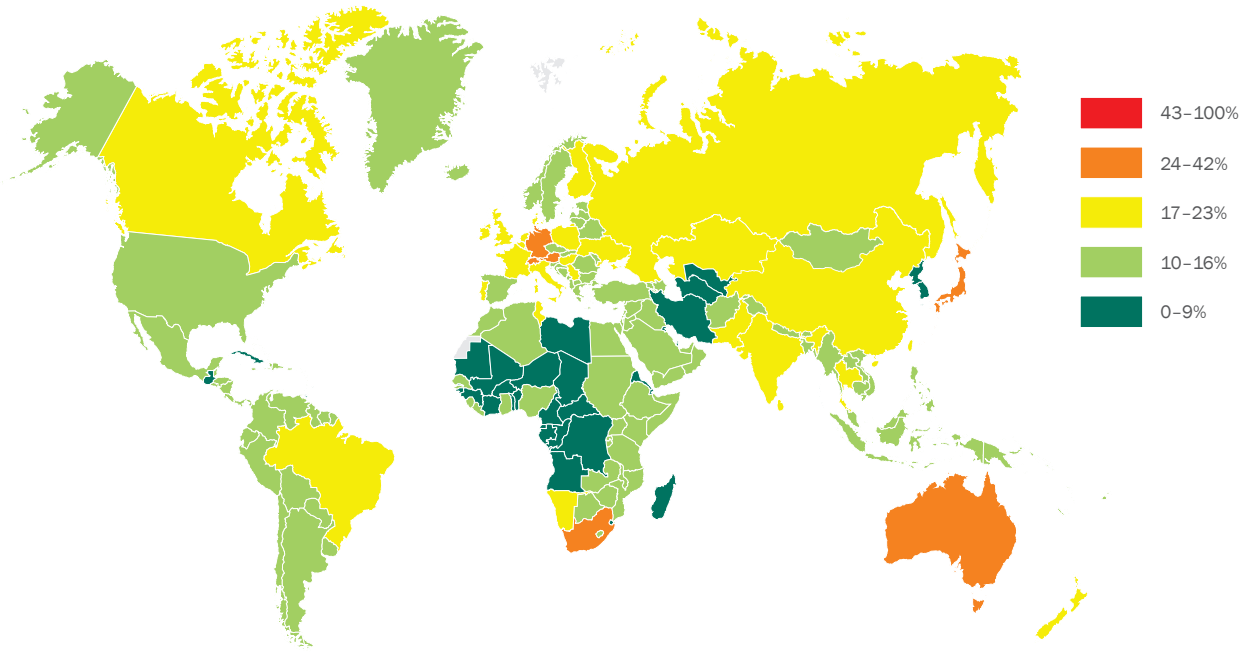
Zeus (Trojan-Spy.Win32.Zbot) remains the most widespread banking Trojan. According to Kaspersky Lab's research, the program is involved in 53% of malware attacks on online banking clients, and remains a firm favorite among cybercriminals.

The first four banking Trojans in the table above log keystrokes, which suggests this method of stealing information is still effective when carrying out attacks on online banking customers.

Trojan.Win32.ChePro spreads via spam messages with the subject "Invoice from Internet Bank". The messages contain a Microsoft Word document with an embedded image that, if clicked, launches a malicious program.

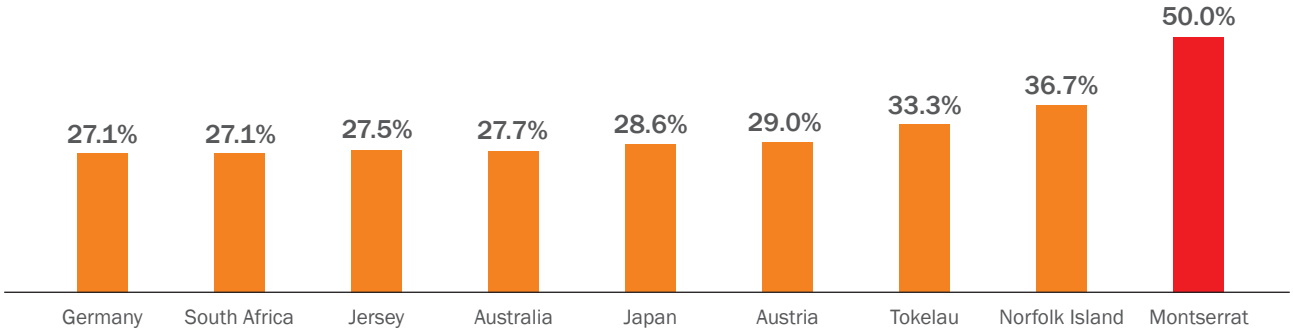
Worm.Win32.Cridex self-proliferates, attacking corporate users of major international banks and e-payment systems. Cybercriminals are especially interested in users' bank card details. This malicious program is distributed via email, instant messaging, removable media, etc.

The proportion of detections (per number of users in a country) triggered by Kaspersky Lab's anti-phishing technology is displayed in the map below.



The proportion of detections (per number of users in a country) triggered by Kaspersky Lab's anti-phishing technology

The countries/regions where users faced phishing attacks most frequently:



Total of anti-phishing alerts: **1 865 570 950**

Key developments in the online banking sphere

- Detection of the new malicious program Trojan-Dropper.Win32.Metel which attacks users of the iBank2 online banking system https://www.net-security.org/malware_news.php?id=2705
- The author of the SpyEye malicious program has been charged http://krebsonsecurity.com/2014/01/feds-to-charge-alleged-spyeye-trojan-author/
- The Zbot mass mailing allegedly spread by international companies http://garwarner.blogspot.com.au/2014/02/gameover-zeus-now-uses-encryption-to.html
- Automatic infection of Android-based devices with a malicious program utilizing USB debugging Mode when connected to infected PCs http://www.pcworld.com/article/2090940/new-windows-malware-tries-to-infect-android-devices-connected-to-pcs.html
- Targeted Olympic-themed SMS spam mailing that contained a link to a malicious program for Android http://www.securelist.com/en/blog/8180/Mobile_scammers_target_sports_fans
- Brazilian cybercriminals started using fraudulent JAVA applications to download banking Trojans http://www.securelist.com/en/blog/208216072/Encrypted_Java_Archive_Trojan_bankers_from_Brazil#page_top
- Mass appearance of fraudulent sites created to steal user payment data by offering fake tickets to the FIFA World Cup http://www.securelist.com/en/blog/208216028/World_Cup_fake_tickets_fake_giveaways_real_attacks#page_top
- Detection of a new malicious program designed to steal money from Latin American banks http://www.securelist.com/en/blog/208214232/From_Latin_America_with_love_Jumcar_strikes_again
- Spam mailing exploiting the release of the popular WhatsApp application to distribute a Trojan program http://www.securelist.com/en/blog/208214225/WhatsApp_for_PC_a_guaranteed_Trojan_banker

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