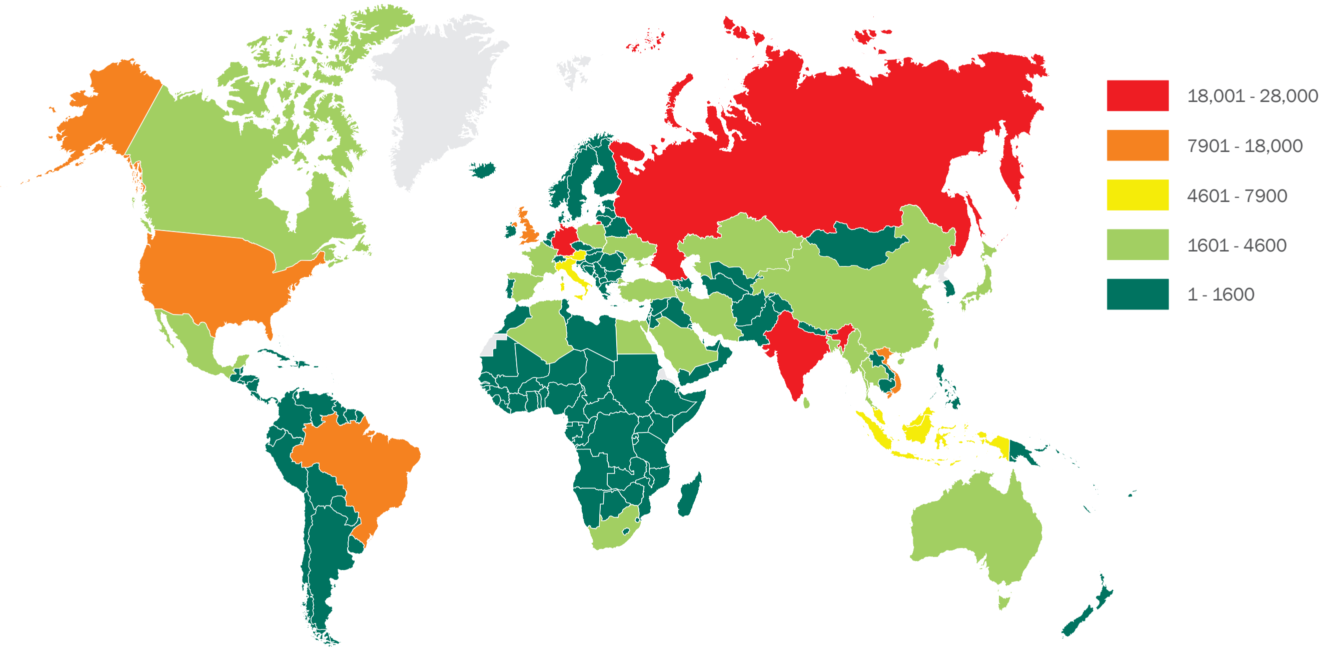
# MONTHLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD:
17.02–17.03.2014

**One of the main events during the reporting period was the discovery of a vulnerability affecting devices running iOS that allows cybercriminals to record and transmit keystrokes or screen touches even if a virtual keyboard is used. Cybercriminals can use the vulnerability to intercept payment data entered by a user when performing a transaction online. Details on this and other detected threats can be found in the section 'Key developments in the online banking sphere' below.**

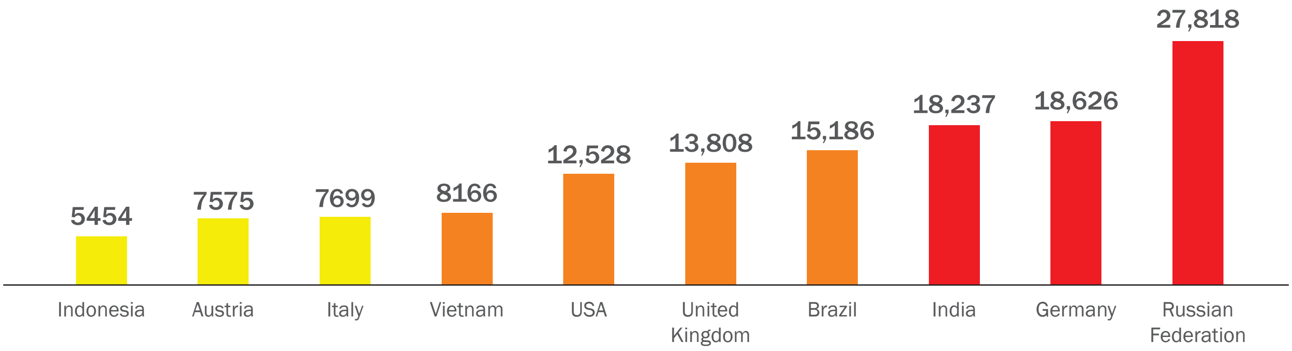
## Overall statistics

During the reporting period, Kaspersky Lab's protection mechanisms blocked 253,000 attempts on user computers to launch malware capable of stealing money via online access to bank accounts. This figure represents a 3.9% increase compared to the previous reporting period (243,368).



Number of users that encountered banking malware

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



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 involving banking malware:**

**1,357,595**

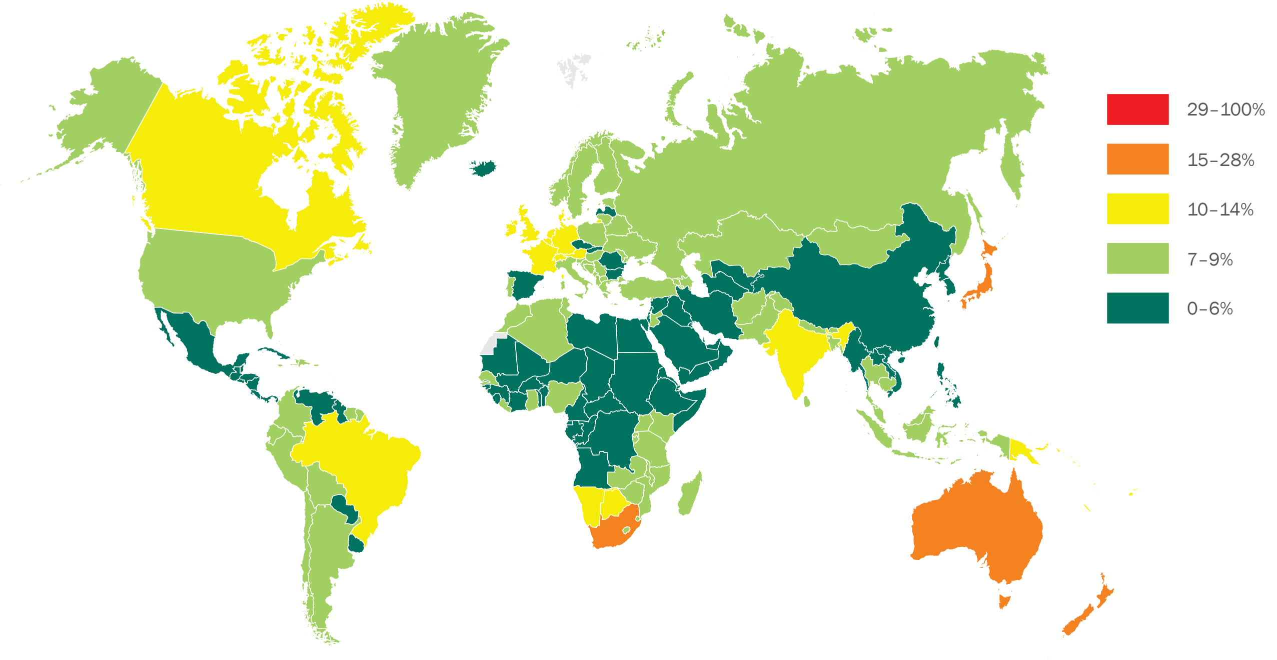
| Verdict | Number of users | Number of notification |
|---|---|---|
| Trojan-Spy.Win32.Zbot | 198,035 | 883,188 |
| Worm.Win32.Cridex | 454 | 123,081 |
| Trojan-Spy.Win32.Spyeyes | 3627 | 57,369 |
| Trojan-Banker.Win32.Agent | 5341 | 19,552 |
| Trojan-Banker.AndroidOS.Faketoken | 12,178 | 19,524 |
| Trojan-Banker.Win32.Banker | 5331 | 16,594 |
| Trojan-Banker.HTML.Agent | 6388 | 12,672 |
| Trojan-Banker.Win32.Banbra | 5318 | 9603 |
| Trojan-Banker.Win32.ChePro | 5924 | 9313 |
| Backdoor.Win32.Shiz | 2803 | 6699 |

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 against online banking clients, and remains a firm favorite among cybercriminals when conducting attacks on users of online banking that involve malware.

As well as web injections (modifications to the HTML pages of banks), four of the 10 entries in the table of malicious programs use technology that records keystrokes. This suggests that this method of stealing transaction data is still effective when attacking online banking users.

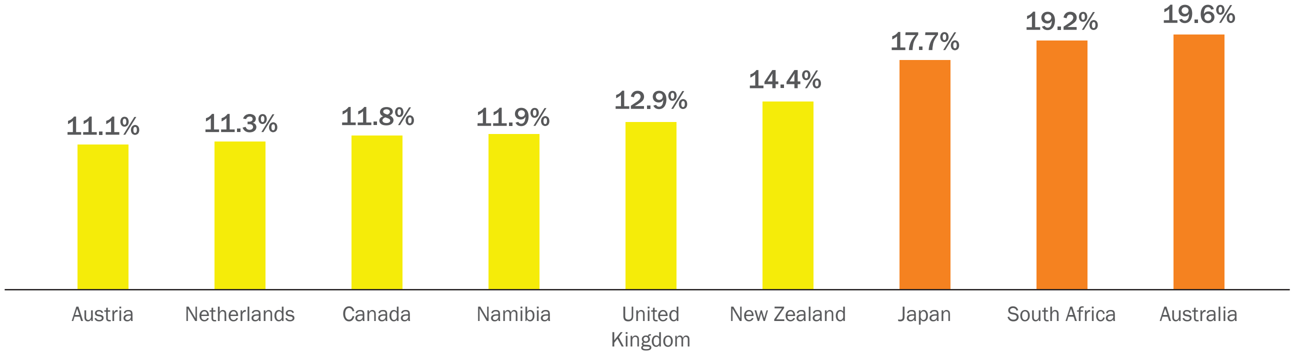
Worm.Win32.Cridex self-proliferates, attacking corporate users of major international banks and e-payment systems. Cybercriminals are especially interested in users' bank card details. This malicious program is distributed via email, instant messaging, removable media, etc.

The proportion of detections (per total 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 where users faced phishing attacks most frequently:



**The overall number of anti-phishing alerts totaled: 5,547,705**

## Key developments in the online banking sphere

- Discovery of a vulnerability in iOS that can be exploited to intercept keystrokes on a virtual keyboard http://www.ibtimes.co.uk/new-apple-ios-7-security-vulnerability-allows-hackers-secretly-monitor-your-iphone-1437992
- Distribution of banking malware via contextual advertising in YouTube clips http://thehackernews.com/2014/02/caphaw-banking-malware-distributed-via_24.html
- Publication of information about vulnerabilities in iOS and Mac OS that allow cybercriminals to intercept data sent via secure connections http://www.reuters.com/article/2014/02/22/apple-encryption-idUSL2N0LR0GW20140222
- Source codes for the Android iBanking Trojan leaked online http://www.computerworld.com/s/article/9246494/Source_code_for_Android_iBanking_bot_surfaces_on_underground_forum
- Discovery of a new modification of the ZeuS banking Trojan that infects mobile devices by masquerading as a security solution that protects against online banking threats http://www.xylibox.com/2014/03/zeus-1134.html
- Discovery of a specialized malicious program for stealing bitcoins after hackers publish an archive of Mt. Gox transaction records http://www.pcworld.com/article/2109000/bitcoinstealing-malware-hidden-in-mt-gox-data-dump-researcher-says.html
- Malware discovered that steals payment details from POS terminals http://www.eweek.com/security/ram-scrapper-pos-malware-plaguing-u.s.-retailers-for-years.html

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.