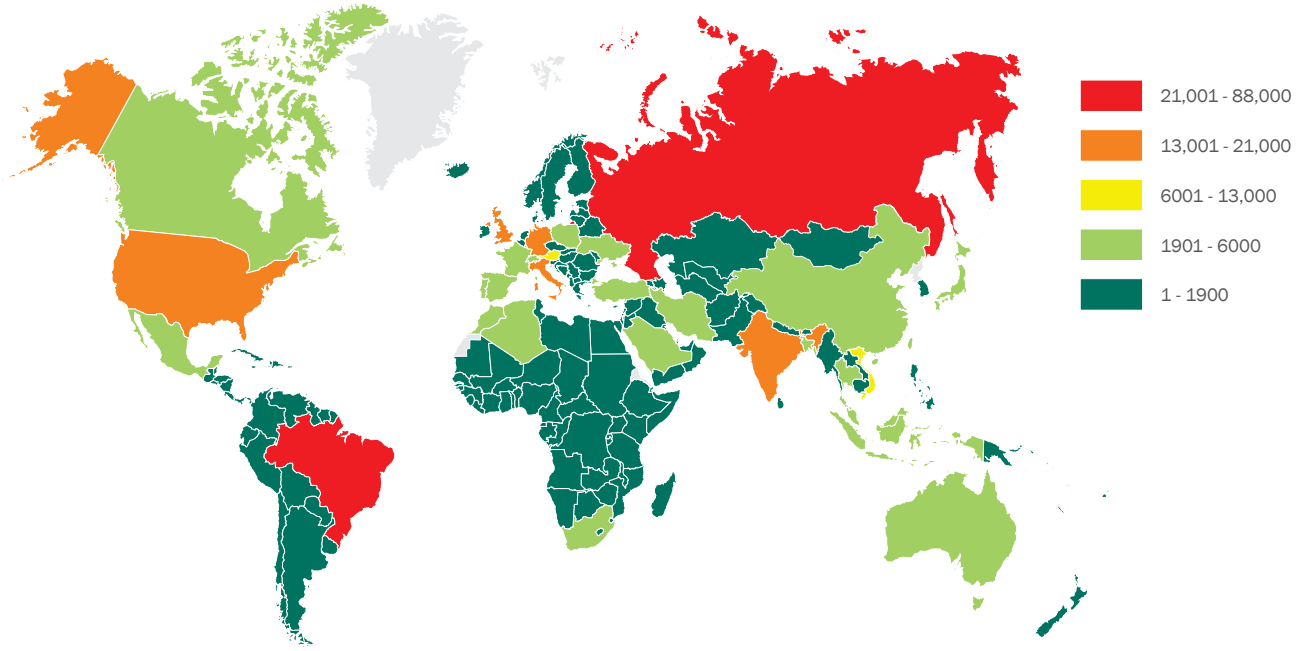
MONTHLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD: 19.05–19.06.2014

One of the main events during the reporting period was the start of a special operation to eliminate the ZeuS Gameover botnet. Details of the incident and other detected threats can be found in the section 'Key events in the online banking sphere' below.

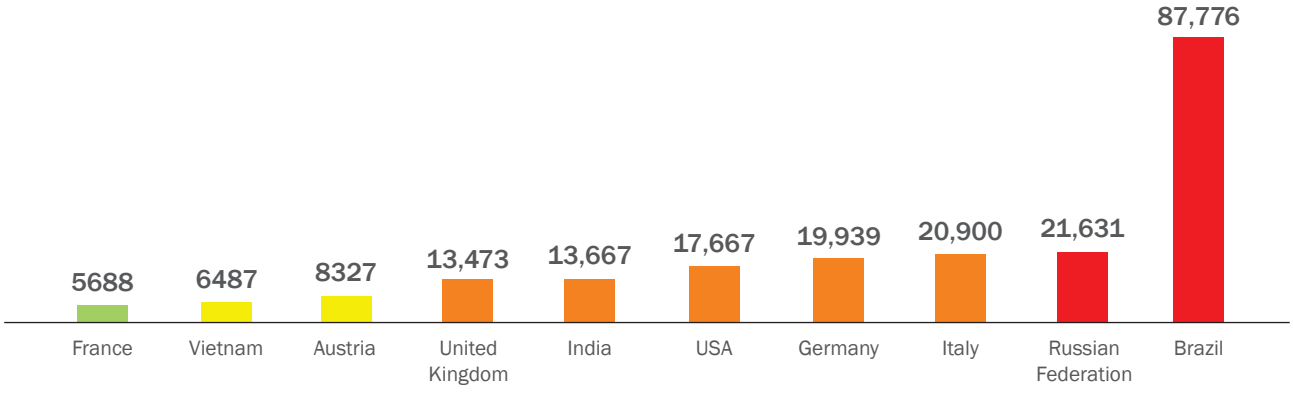
Overall statistics

During the reporting period, Kaspersky Lab solutions blocked 350,936 attempts on user computers to launch malware capable of stealing money from online banking accounts. Last month, we registered a surge of malware activity (by almost 37%). During the reporting period this figure increased only 2,9% (350,936 vs 341,216). This fact is most likely related to the vacation season, when customers make greater use of their payment data to make all types of online purchases.



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

Brazil remains the most frequently attacked country and the issue of protecting users' online banking data has only been exacerbated by the 2014 World Cup currently taking place in the country. Kaspersky Lab experts have examined the safety of Wi-Fi networks and made a list of recommendations for those who want to use their payment information in Brazil: http://www.securelist.com/en/blog/8229/Adware_or_money_loss_instead_of_your_favorite_World_Cup_game

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

Total notifications of attempted infections by banking malware:

1,387,080

Verdict*	Number of users	Number of notifications
Trojan-Spy.Win32.Zbot	202,062	951,306
Trojan-Banker.Win32.Lohmys	46,116	150,707
Trojan-Banker.Win32.ChePro	55,106	150,387
Trojan-Spy.Win32.Spyeyes	10,985	32,882
Trojan-Banker.Win32.Agent	7043	18,494
Trojan-Banker.Win32.Banbra	6683	16,683
Trojan-Banker.Win32.Banker	5136	15,069
Trojan-Banker.Win32.Shiotob	2641	13,835
Backdoor.Win32.Clampi	2017	6022
ackdoor.Win32.Shiz	2016	4596

*verdicts are limited exclusively to banking threats (based on an expert assessment of malware functionality; see the verdict list[1] on page 3)

Zeus (Trojan-Spy.Win32.Zbot) remained 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 email contains a Word document with an embedded image that launches malicious code if the recipient clicks on it.

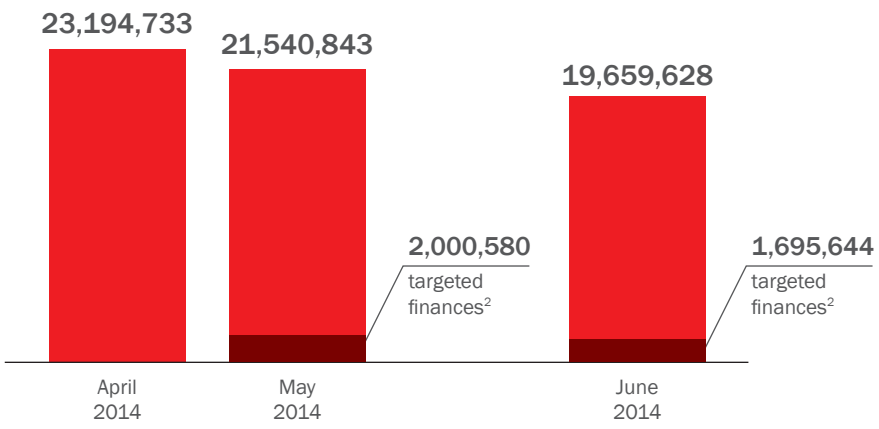
As well as web injections (modification of a bank's HTML pages), four of the 10 entries also make use of keylogging technology, which suggests this method of stealing information is still effective when carrying out attacks on online banking customers

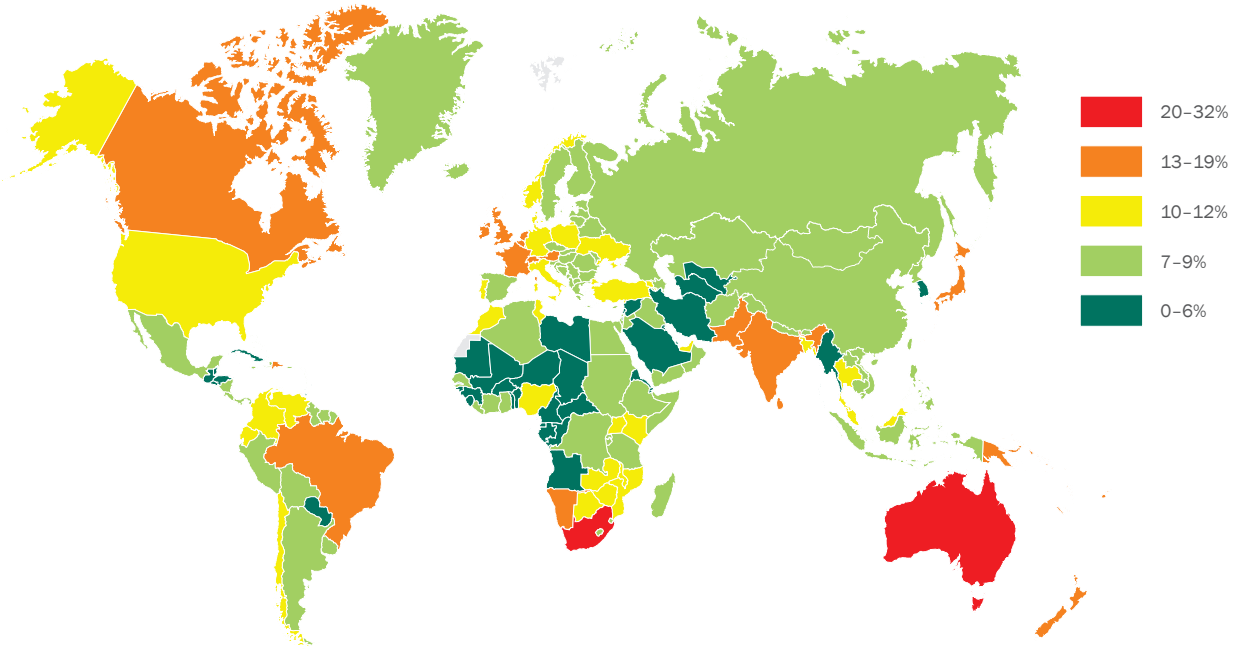
Trojan-Spy.Win32.Carberp dropped out of this month's Top 10. The banking Trojan is designed to compromise systems of remote banking services and to commit fraud against large banks.

Phishing

The overall number of anti-phishing notifications:

19,659,628





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

Key developments in the online banking sphere

- Detection of malicious content spreading in the form of adverts exploiting the popularity of the 2014 World Cup http://www.securelist.com/en/blog/8229/Adware_or_money_loss_instead_of_your_favorite_World_Cup_game
- An operation is launched to eliminate the ZeuS Gameover botnet and to track down and arrest the creator of the banking Trojan http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/
- A data breach at the major restaurant chain P.F. Chang's China Bistro results in customers' payment data being leaked http://www.usatoday.com/story/money/business/2014/06/13/pf-changs-data-breach/10413015/
- Detection of Svpeng, a mobile Trojan that steals users' online banking data and possesses ransomware functionality https://www.securelist.com/en/blog/8227/Latest_version_of_Svpeng_targets_users_in_US
- Detection of the new banking Trojan Pandemiya http://threatpost.com/new-pandemiya-banking-trojan-written-from-scratch
- Experts discover the first malware for Android that communicates with a C&C server hosted in the Tor domain https://www.securelist.com/en/blog/8225/The_first_mobile_encryptor_Trojan
- Detection of an application imitating Google Play that steals online banking passwords http://itsecuritynews.info/2014/06/18/what-are-you-doing-dsencrypt-malware/

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.

1 List of malicious programs considered most dangerous by Kaspersky Lab's experts in terms of their ability to steal banking info:

- Worm.Win32.Cridex
- Backdoor.Win32.Shiz
- Backdoor.Win32.Cevantor
- Backdoor.Win32.Redaptor
- Backdoor.Win32.Sinowal
- Backdoor.Win32.SpyEye
- Backdoor.Win32.Caphaw
- Trojan-Banker
- Trojan-Spy.Win32.Carberp
- Trojan-Spy.Win32.Lurk
- Trojan-Spy.Win32.Spyeyes
- Trojan-Spy.Win32.Zbot
- Trojan-Spy.Win32.Hbot
- Trojan.Win32.ChePro
- Trojan.Win32.Spyeyes
- Backdoor.Win32.Clampi
- Backdoor.Win32.Papras

2 Phishing attempts are classified as 'financial' if they target banks, payment systems and/or e-commerce organizations.

KASPERSKY lab