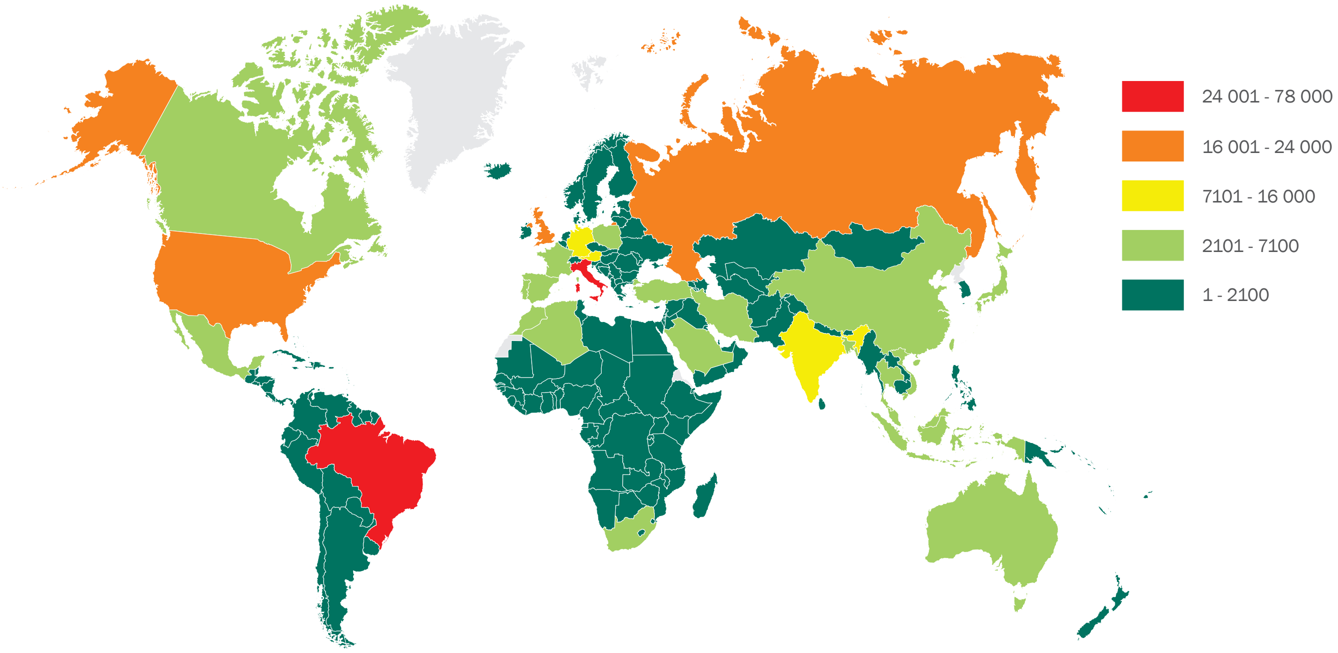
MONTHLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD: 19.04–19.05.2014

One of the main events during the reporting period was the leakage of payment credentials belonging to eBay users. Details of the incident and other detected threats can be found in the section ‘Key events in the online banking sphere’ below.

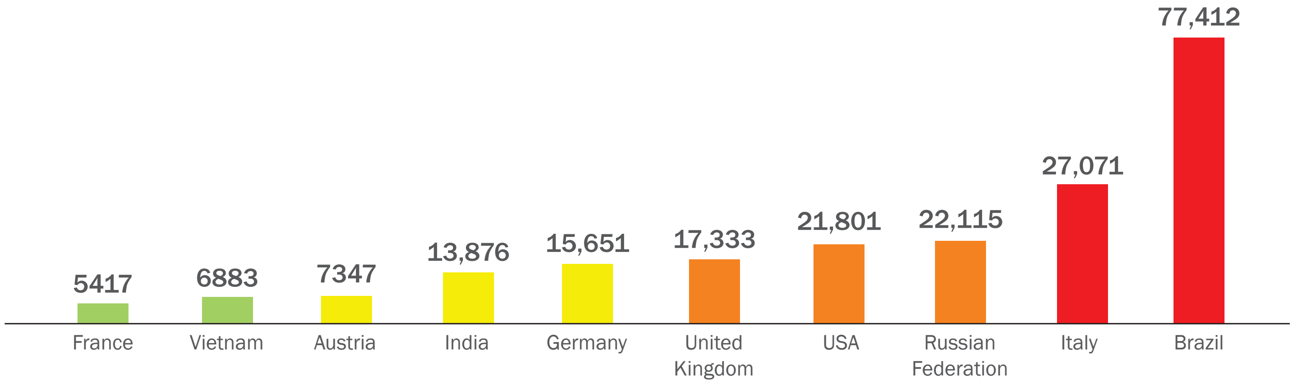
Overall statistics

During the reporting period, Kaspersky Lab solutions blocked 341,216 attempts on user computers to launch malware capable of stealing money from online banking accounts. This figure represents a 36.6% increase compared to the previous reporting period (249,812). This increase in banking malware activity is most likely related to the onset of the vacation season, when customers actively use their payment data to make all types of purchases online.



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):



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:

1 188 711

Verdict*	Number of users	Number of notifications
Trojan-Spy.Win32.Zbot	198 238	820 669
Trojan-Banker.Win32.Lohmys	53 817	165 775
Trojan-Banker.Win32.ChePro	28 536	61 731
Trojan-Spy.Win32.Spyeyes	10 246	33 547
Trojan-Banker.Win32.Banbra	6821	17 541
Trojan-Banker.Win32.Banker	5784	16 202
Backdoor.Win32.Shiz	2343	15 503
Trojan-Banker.Win32.Agent	5861	14 582
Backdoor.Win32.Clampi	2583	7239
Trojan-Spy.Win32.Carberp	1988	6103

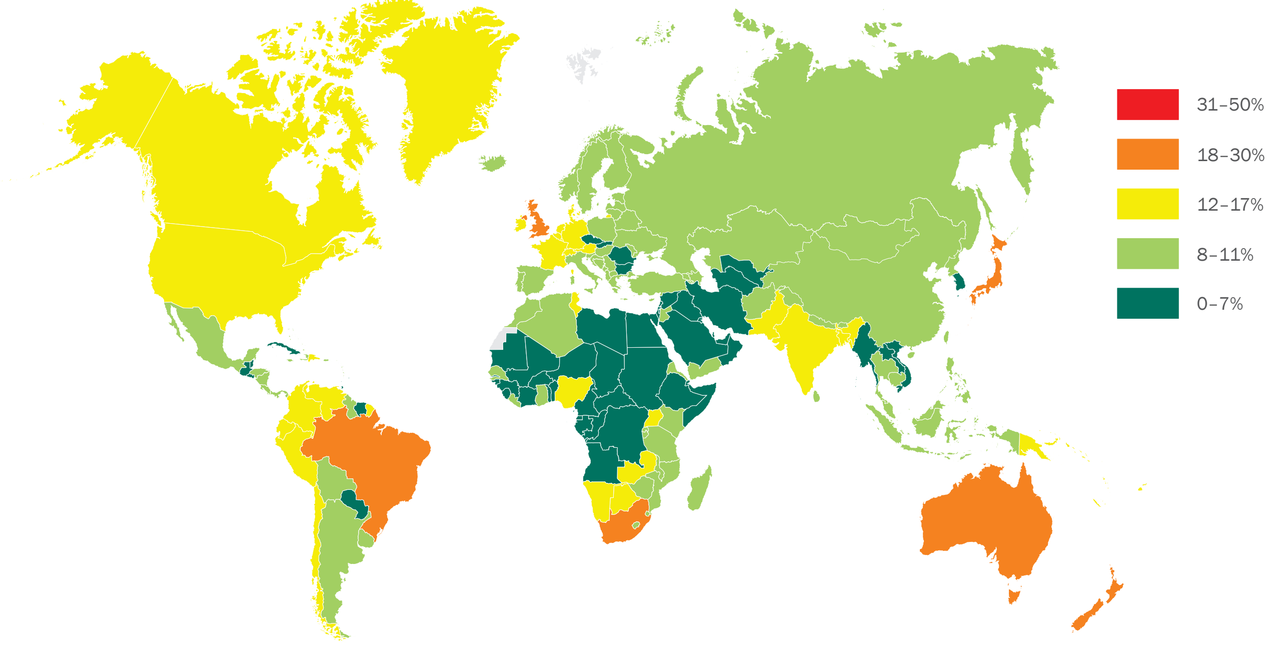
*verdicts are limited exclusively to banking threats (based on an expert assessment of malware functionality; see the verdict list[1] below)

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 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

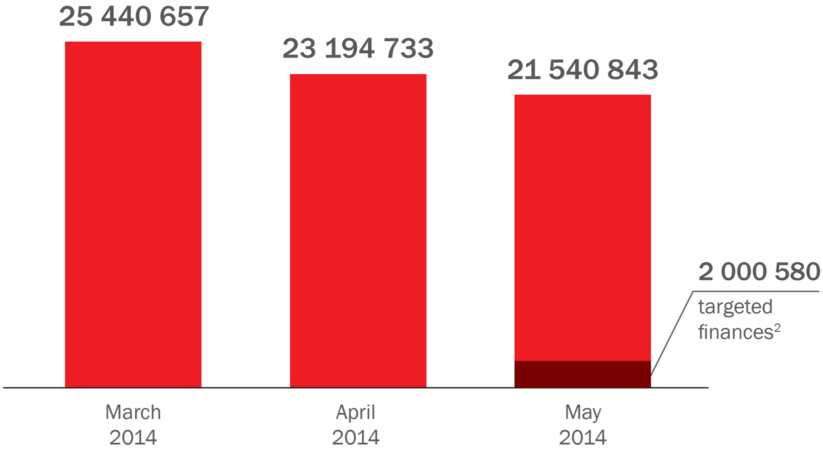
The banking Trojan Trojan-Spy.Win32.Carberp is this month's newcomer to the Top 10. IT is designed to compromise systems of remote banking services and to commit fraud against large banks.



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

The overall number of anti-phishing notifications:

21 540 843



Key developments in the online banking sphere

- Payment details of eBay users leaked: https://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/
- A zero-day vulnerability detected in Internet Explorer: https://technet.microsoft.com/library/security/2963983
- A botnet of 1,500 infected PoS terminals identified: http://intelcrawler.com/news-18
- The Blackshades hacker group detained by authorities: https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals
- A new exploit kit named Infinity uncovered on the black market: http://intelcrawler.com/news-16
- Detection of a new banking Trojan with similar functionalities to those of the banking Trojans Carberp and Zeus, hence its name Zberp: http://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/
- A zero-day vulnerability detected in Adobe Flash Player: http://www.securelist.com/en/blog/8212/New_Flash_Player_0_day_CVE_2014_0515_used_in_watering_hole_attacks

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.