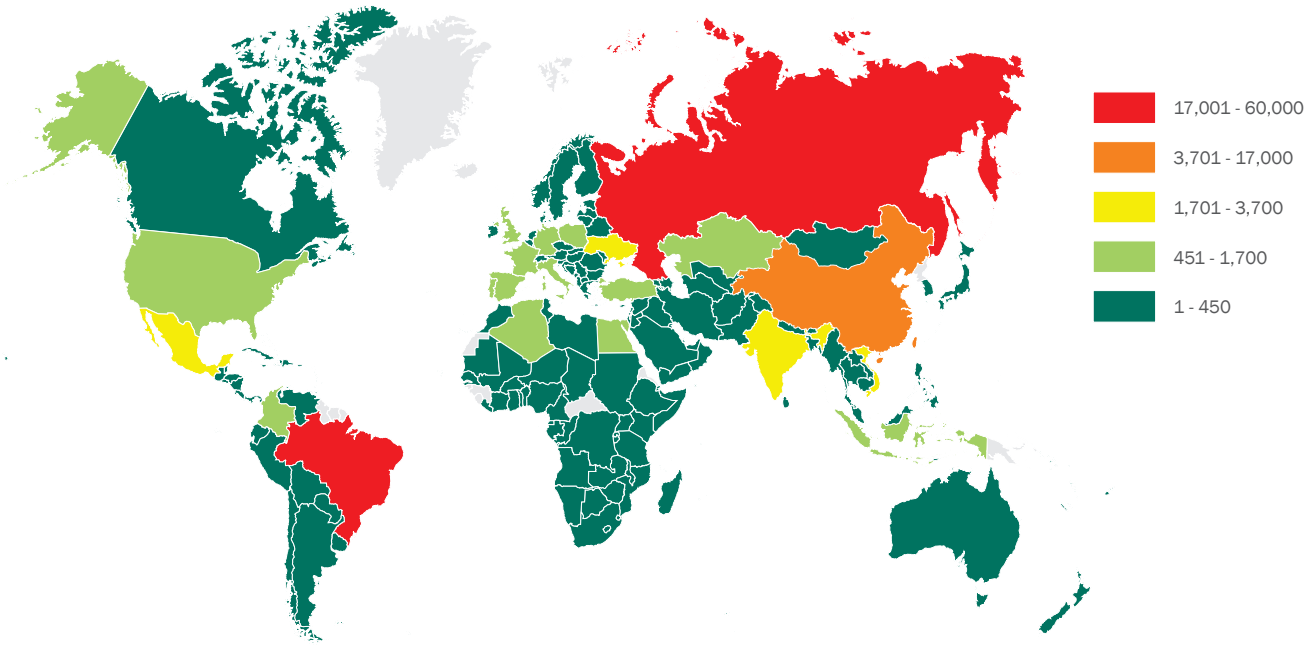
BI-WEEKLY REPORT ON ONLINE THREATS IN THE BANKING SECTOR

REPORTING PERIOD:
11-25 NOVEMBER 2013

One of the biggest events during the reporting period was the detection of two completely new malicious programs targeting online banking users — Neverquest and I2Ninja. Details on these and other detected threats are provided in the Key banking threat-related incidents section.

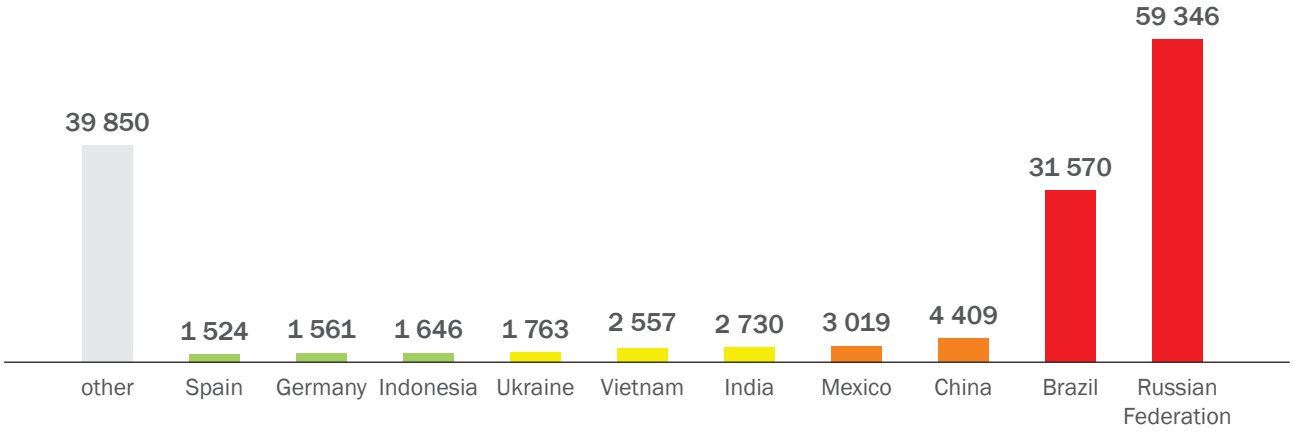
Overall statistics

During the reporting period, Kaspersky Lab's protection mechanisms blocked attempts to launch malware which steals money via access to the online bank accounts of 150,000 users. This means that approximately one in 20 users of online banking are at risk.



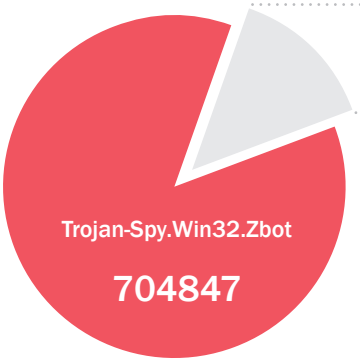
Russia and Brazil are areas of increased banking malware infection risk

The number of users attacked using this type of program during the reporting period is shown in the graph below (Top 10 based on the number of users attacked, in ascending order):



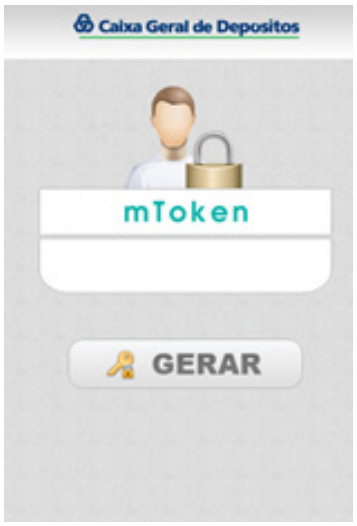
KASPERSKY lab

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



Trojan.Win32.Spyeyes	92264
Trojan-Banker.Win32.Agent	6852
Trojan-Banker.AndroidOS.Faketoken	5624
Trojan-Banker.Win32.Banbra	5325
Trojan-Banker.Win32.Banker	2422
Trojan-Banker.Win32.Qhost	461
Trojan-Banker.JS.Banker	198

Zbot and Spyeyes are currently the most technologically advanced and widespread. To make matters worse, their source code is publicly accessible, which means that any cybercriminal can use it to develop new malware.



Main window of Trojan-Banker.AndroidOS.Faketoken

According to our records, incidents involving attempts to infect Android devices are on the rise. One example is the new malicious program Trojan-Banker.AndroidOS.Faketoken designed to steal transaction authorization numbers sent by the bank in text messages. The application is disguised as an additional piece of banking software needed to receive new authorization numbers.

Trojan-Banker.Win32.Agent, Trojan-Banker.Win32.Banbra and Trojan-Banker.Win32.Banker are designed to log key presses. These malicious programs primarily target Brazilian financial sites.

Another banking Trojan, Trojan-Banker.Win32.Qhost, changes network connection settings on the victim's computer, redirecting requests to spoofed banking system websites in order to conduct a phishing attack.

Trojan-Banker.JS.Banker is a malicious JavaScript module which emulates the contents of a banking site.

Key banking threat-related incidents

- Dutch hackers published a video with step-by-step instructions on how to steal money from online banking users with the help of Trojan.Win32.Spyeyes http://www.liveleak.com/view?i=807_1383224319 (18+)
- The CVE-2013-3906 vulnerability, which was patched by Microsoft on November 5, 2013 (http://blogs.technet.com/b/msrc/archive/2013/11/05/microsoft-releases-security-advisory-2896666-v2.aspx), was exploited to distribute Trojan-Spy.Win32.Zbot before the vulnerability was patched.
- Two completely new samples of banking malware designed to attack online banking users were detected: Neverquest (which is distributed via exploits, spam and social media) and I2Ninja (which implements a P2P algorithm that makes it difficult to take control of infected computers).
- Trojan.Win32.Spyeyes got a new module which prompts the user for bank card data during bank transactions, supporting a large number of banks that were previously unsupported by other modules designed to steal money from bank accounts.

The main source of information for this report is Kaspersky Lab's cloud infrastructure, 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