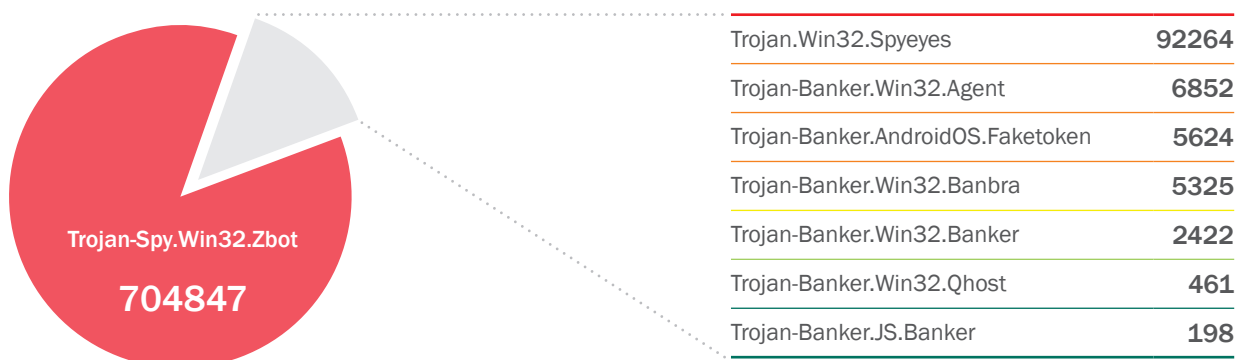
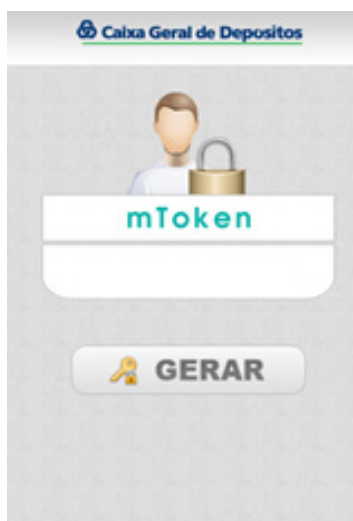


The graph below shows the programs most commonly used to attack online banking users, based on the number of infection attempt alerts:



malware developers are developing 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.