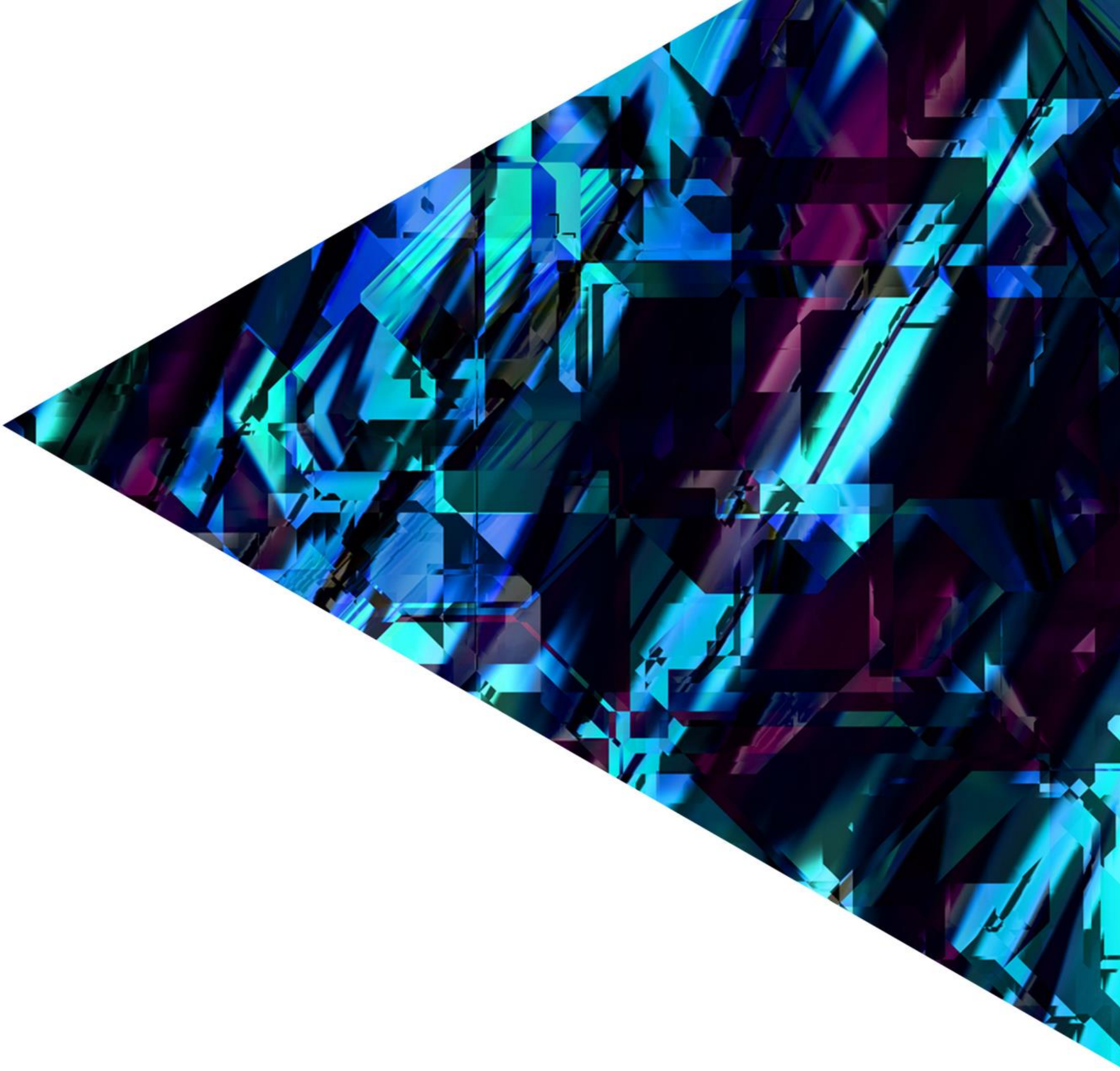


IT THREAT EVOLUTION IN Q1 2016

Alexander Gostev, Roman Unuchek, Maria Garnaeva,
Denis Makrushin, Anton Ivanov

Contents

Q1 figures

- According to KSN data, Kaspersky Lab solutions detected and repelled **228,420,754** malicious attacks from online resources located in 195 countries all over the world.
- **74,001,808** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **18,610,281** unique malicious objects: scripts, exploits, executable files, etc.
- There were **459,970** registered notifications about attempted malware infections that aim to steal money via online access to bank accounts.
- Crypto ransomware attacks were blocked on **372,602** computers of unique users.
- Kaspersky Lab's file antivirus detected a total of **174,547,611** unique malicious and potentially unwanted objects.
- Kaspersky Lab mobile security products detected:
  - **2,045,323** malicious installation packages;
  - **4,146** mobile banker Trojans;
  - **2,896** mobile ransomware Trojans.

Overview

2016 has only just got underway, but the first three months have already seen the same amount of cybersecurity events that just a few years ago would have seemed normal for a whole year. The main underlying trends remained the same, while there was significant growth in trends related to traditional cybercrime, especially mobile threats and global ransomware epidemics.

Ransomware became the main theme of the quarter after knocking targeted attacks from the top of the most popular threat rating. Unfortunately, this is a situation that will continue to evolve, and those behind the extortion could well end up being named "problem of the year".

Targeted attacks

BlackEnergy2/3

The BlackEnergy cyberattack on the Ukrainian energy sector was the most high-profile incident. Although it occurred at the end of last year, a fuller picture of what happened only appeared in the course of the subsequent analysis. Moreover, attempts by cybercriminals to arrange new attacks continued in 2016.

The attack was unique because of the damage it caused – the hackers managed to disable the power distribution system in Western Ukraine, launch the Wiper program on the targeted systems and carry out a telephone DDoS on the technical support services of the affected companies.

There were numerous publications about the attack, and Kaspersky Lab's experts revealed several aspects of the activities of the group responsible. In particular, they published an analysis of the tool used to penetrate the systems – a malicious DOC file.

For those who want to learn more about the attack, we recommend the report prepared by the American SANS Institute and ICS-CERT.

Poseidon

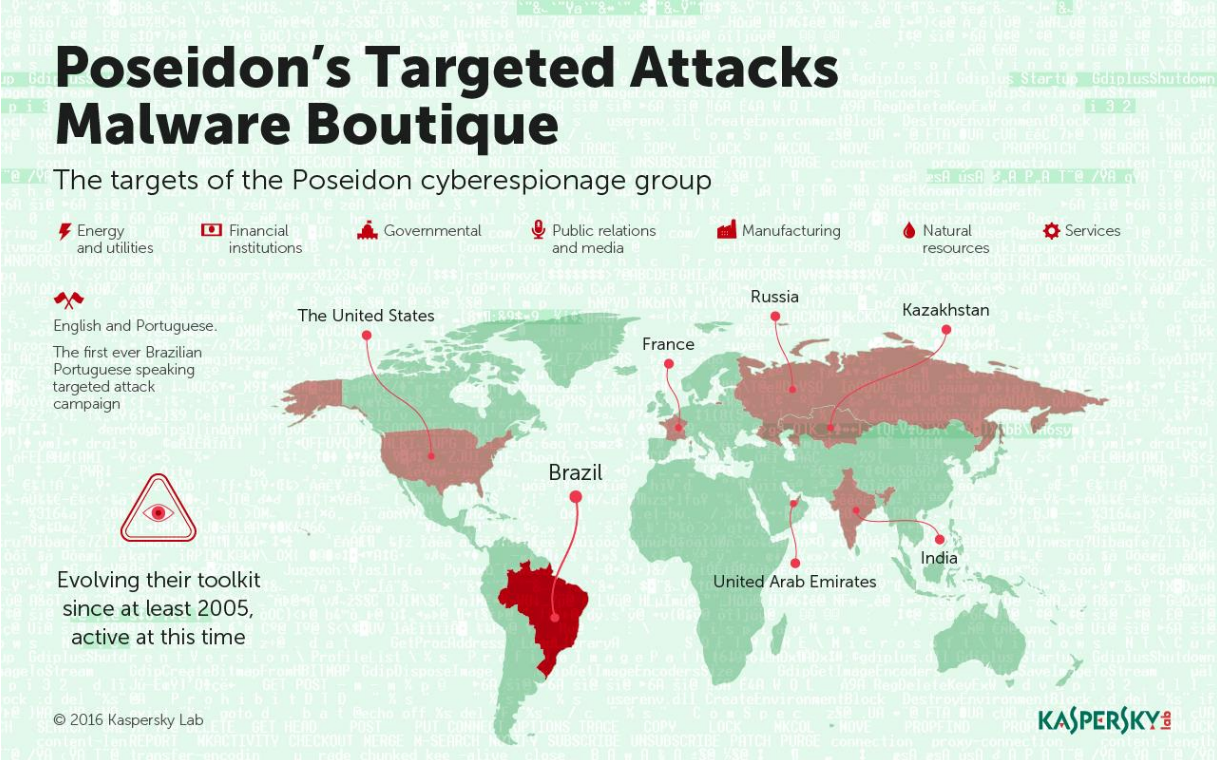
In February, the experts at Kaspersky Lab revealed details about the activities of Poseidon – the first Portuguese-speaking targeted attack group which had set up a custom-tailored malware boutique.

Although the report was only released in 2016, the group has been operational for a long time. Malware campaigns that were most probably supported by Poseidon were detected as far back as 2005, while the first sample dates back to 2001. Poseidon's arsenal is focused primarily on the Microsoft Windows operating system family: from Windows 95, which the group targeted in its early days, to Windows 8.1 and Windows Server 2012, which were targeted by the most recently detected malware samples.

The attack scenario is carefully tailored to the victim. Although the initial infection occurs according to the same scenario, the following stages of the campaign specifically customize the infection method for each new victim. That is why the specialists from the Global

Research & Analysis Team (GReAT) decided to call Poseidon a “custom-tailored malware boutique”.

Having gained access to the corporate network, the criminals move across the network and collect as much data as possible in order to escalate their privileges, create a network map and to identify the computer they need. The main target of the attack is usually the local Windows domain controller. Once they have control over it, the attackers can steal intellectual property, data, trade secrets, and other valuable information.



The information collected by Poseidon for its owners was in most cases used to blackmail victim companies into contracting the Poseidon Group as a security firm. Regardless of whether a contract was signed, Poseidon remained on the network.

Hacking Team

Yet another infamous "boutique" creating cyber-espionage tools, the Italian company Hacking Team, fell victim to a cyberattack last year in which a huge database of its employee email correspondence was stolen, as well as project source codes.

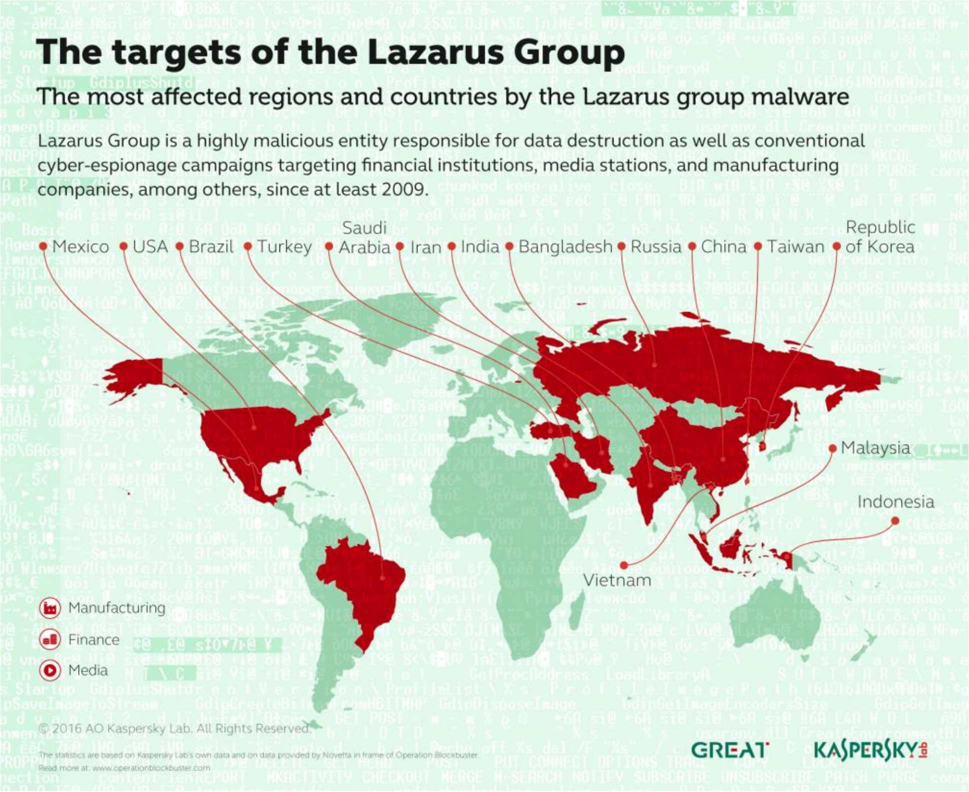
The incident revealed a lot of problems in the work of the company and many thought it would be very difficult for the business to develop further. However, at the beginning of 2016 new Hacking Team implants for OSX were found. This indicates that the group has no intention of halting its work and is continuing to develop in the sphere of secondary operating systems. This means their "creations" will continue to be a problem for users who have become an object of interest for HT customers.

Yet another story related to Hacking Team was the hunt for a Microsoft Silverlight 0-day. Information about the possible presence of this vulnerability was found in the Italian company’s documents. Based on very little initial data and armed with the Yara and

VirusTotal tools, our experts set a trap and waited. And sure enough, they detected a 0-day exploit.

Operation BLOCKBASTER

Kaspersky Lab was among the participants in operation Blockbaster, a joint investigation conducted by several major IT security companies. The subject of the investigation was activity by the Lazarus Group, a cybercriminal gang of supposedly North Korean origin that was involved in the attack on Sony Pictures in 2014.



The targets of the Lazarus Group
The most affected regions and countries by the Lazarus group malware
Lazarus Group is a highly malicious entity responsible for data destruction as well as conventional cyber-espionage campaigns targeting financial institutions, media stations, and manufacturing companies, among others, since at least 2009.
Mexico
USA
Brazil
Turkey
Saudi Arabia
Iran
India
Bangladesh
Russia
China
Taiwan
Republic of Korea
Malaysia
Indonesia
Vietnam
Manufacturing
Finance
Media
© 2016 AO Kaspersky Lab. All Rights Reserved.
The statistics are based on Kaspersky Lab's own data and on data provided by Novetta in frame of Operation Blockbuster
Read more at: www.operationblockbuster.com
GREAT
KASPERSKY lab

The Lazarus Group has been around since 2009, but their activities moved up a gear from 2011. The group is responsible for such well-known attacks as Troy, Dark Seoul (Wiper), WildPositron. During the investigation over 40 different types of malicious program, which they had created over the years, were detected. In particular, the group used their malware to attack companies, financial institutions, radio and television. Use of exploits for 0-day vulnerabilities was also recorded.

Hospitals under attack

This section on targeted attacks should also include Sergei Lozhkin's research on how hackers can penetrate the internal network of hospitals and gain full access to patient data using publicly available tools and services.

Unfortunately, medical institutions are being targeted more and more by such attacks. In the first quarter of 2016, there were several incidents of hospital networks being infected with various types of Trojan ransomware that encrypts data and demands a ransom to decrypt it.

The latest incident was an attack on the MedStar network that affected 10 hospitals. According to the network's official report, the data was saved without paying a ransom to the blackmailers, while another hospital in California ended up paying $17,000 for a ransomware crypto key.

Cybercrime

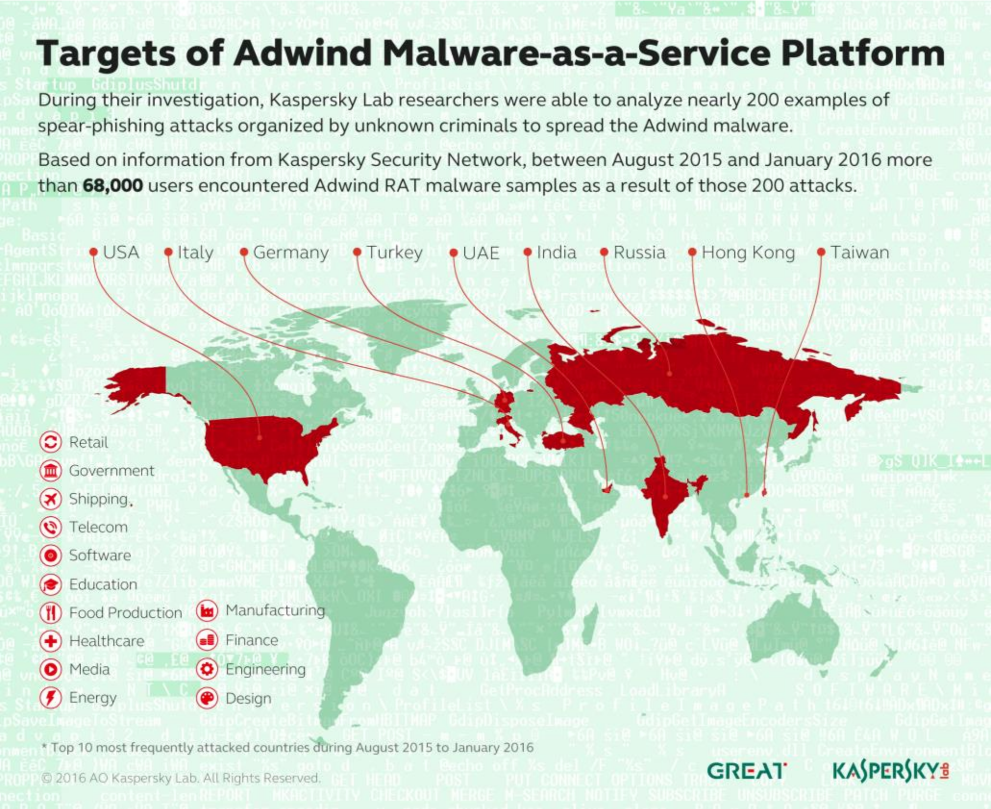
Adwind

At the Security Analyst Summit 2016 (SAS 2016) our GReAT experts presented the results of their investigation into the Trojan known as Adwind RAT (Remote Access Tool). Having studied the activity of the malware, the researchers came to the conclusion that even the story behind the Trojan's creation was out of the ordinary.

The Trojan was developed continuously over several years, with the first samples appearing in 2012. It has had different names at different times: in 2012, the creators were selling it as Frutas; in 2013 it was called Adwind; in 2014 the Trojan was known as Unrecom and AlienSpy; and in 2015 it was named JSocket.

The GReAT experts believe that Adwind and all its incarnations have been developed by one hard-working hacker who has been releasing new features and modules for four years.

The Adwind platform was initially only available in Spanish, but an English-language interface was added later, allowing cybercriminals worldwide to evaluate it. The main users of this Trojan are those conducting advanced cyber fraud, unscrupulous competitors, as well as so-called Internet mercenaries who are paid for spying on people and organizations online. Adwind can also be used by anyone wishing to spy on their friends.



Targets of Adwind Malware-as-a-Service Platform

During their investigation, Kaspersky Lab researchers were able to analyze nearly 200 examples of spear-phishing attacks organized by unknown criminals to spread the Adwind malware.

Based on information from Kaspersky Security Network, between August 2015 and January 2016 more than **68,000** users encountered Adwind RAT malware samples as a result of those 200 attacks.

* Top 10 most frequently attacked countries during August 2015 to January 2016

© 2016 AO Kaspersky Lab. All Rights Reserved.

Geographically, the biggest concentration of victims has also changed over the last four years. In 2013, the targets were mostly in Spanish- and Arabic-speaking countries. The following year, cybercriminals focused on Turkey and India, as well as the United Arab Emirates, the United States and Vietnam. In 2015, Russia topped the rating with the United Arab Emirates, Turkey, the United States and Germany close behind.

Fortunately, our investigation was not in vain – a few days after its publication, the JSocket website stopped working and the Adwind author ceased their activity. Since then, no new versions of the Trojan have appeared. Perhaps we can expect another reincarnation of the Trojan, or maybe this is the end of the story.

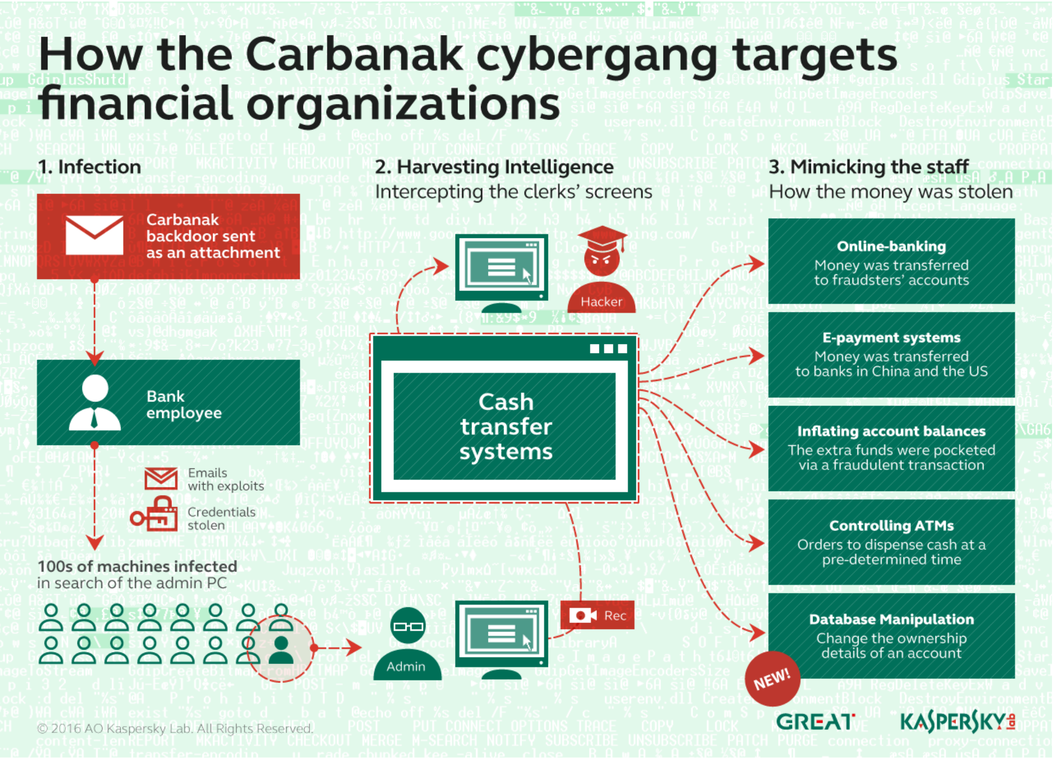
Banking threats

At the Security Analyst Summit (SAS in 2016), Kaspersky Lab announced the discovery of two new gangs engaged in APT-style bank robberies – Metel and GCMAN – and the reemergence of the Carbanak group with new targets in its sights.

In 2015, Kaspersky Lab researchers conducted incident response investigations for 29 organizations located in Russia that were infected by these three groups.

There are other cybercriminal groups currently attacking banks in Russia, but these three are the most active and are involved in the most high-profile thefts from both customer bank accounts and the banks themselves.

The activity of Carbanak 2.0 is of particular interest. In December 2015, Kaspersky Lab confirmed that the group was still active after discovering signs of Carbanak in a telecommunications company and a financial organization. An interesting feature of the Carbanak 2.0 group is that they have a different type of victim. The group has moved beyond banks and is now targeting the budgeting and accounting departments of any organization that interests them, using the same APT-style tools and techniques.


How the Carbanak cybergang targets financial organizations
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
Admin
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
Database Manipulation
Change the ownership details of an account
NEW!
GReAT
KASPERSKY lab
© 2016 AO Kaspersky Lab. All Rights Reserved.

In one remarkable case, the Carbanak 2.0 gang used its access to a financial institution that stored information about shareholders to change the ownership details of a major company. The information was modified to name a money mule as a shareholder of the company, displaying their IDs.

FakeCERT

Yet another criminal gang known as Buhtrap came to the fore in the first quarter. It is responsible not only for the theft of hundreds of millions of rubles from Russian banks but also for organizing a targeted attack on banks using the names and attributes of FinCERT, a special department of the Central Bank of Russia created to detect cyberattacks and notify member banks. It was the first time that attackers had used the FinCert “brand” and the attack was carefully prepared; a corresponding domain name was created and the identifiers used by FinCERT were studied closely.

The malicious mass mailing affected hundreds of banks in Russia. The attackers have a database of their employee email addresses, including names and surnames. A legitimate remote administration tool was used as the remote access module installed in the system.

Bangladesh

On the global arena, the most prominent attack on banks was that involving the Central Bank of Bangladesh. It was not just the object of the attack – the Central Bank – that was remarkable but also the amount of money the attackers managed to steal, plus the amount they tried to steal but failed.

The investigation is still ongoing, but according to the information that has been made public, it is possible to put together a picture of what happened. Back in early February, hackers managed to access the workstations of several employees at the national bank. Using their identities, the fraudsters began to send out transfer orders for money held in different banks including the New York Federal Reserve Bank. With full access and posing as employees, they were able to steal approximately $80 million. The money was transferred to accounts in the Philippines and then passed through a money-laundering scheme involving local casinos and forex brokers.

Another $20 million would have been transferred to Sri Lanka, but the hackers made an error in the name of a recipient organization; this aroused the suspicion of Deutsche Bank, which was the correspondent bank of the Central Bank of Bangladesh. An investigation found that the payment order had been initiated by hackers, and approximately $900 million was still waiting to be transferred.

It’s worth noting that Bangladesh’s Minister of Finance only learned about the incident a month later from the mass media. The head of the Central Bank was forced to resign, the investigators are currently trying to trace those responsible, and the bank is taking measures to return at least some of the stolen funds.

Ransomware Trojans

As we mentioned above, ransomware Trojans were the main theme of the quarter and could well become the main problem of the year.

Making the situation worse is the fact that a number of ransomware Trojans have become accessible to anyone with a little bit of cyber know-how in the form of source code. As a consequence, even the average script-kiddy can deploy their own version of the Trojan which, together with the active use of Bitcoin for paying ransoms, makes it much easier to organize attacks with impunity.

Moreover, the term Ransomware-as-a-Service (RaaS) has already come into use. This involves the attackers offering to pay for Trojan distribution, promising a cut of any ransom money received. The clients of these services are usually webmasters of porn sites. There are services that work the other way round, offering a complete set of tools to the encryptor who takes responsibility for distributing the Trojan and takes 10% of the ransom as commission.

According to reports from several companies, the first quarter of 2016 saw incidents where ransomware was used by a number of well-known APT-groups, mainly Chinese. We also identified similar cases, and not only involving Chinese groups. If these incidents become a trend, the threat will move to a new level because the damage caused by ransomware is not much different from that caused by Wiper-type Trojans. In both cases, user data becomes inaccessible.

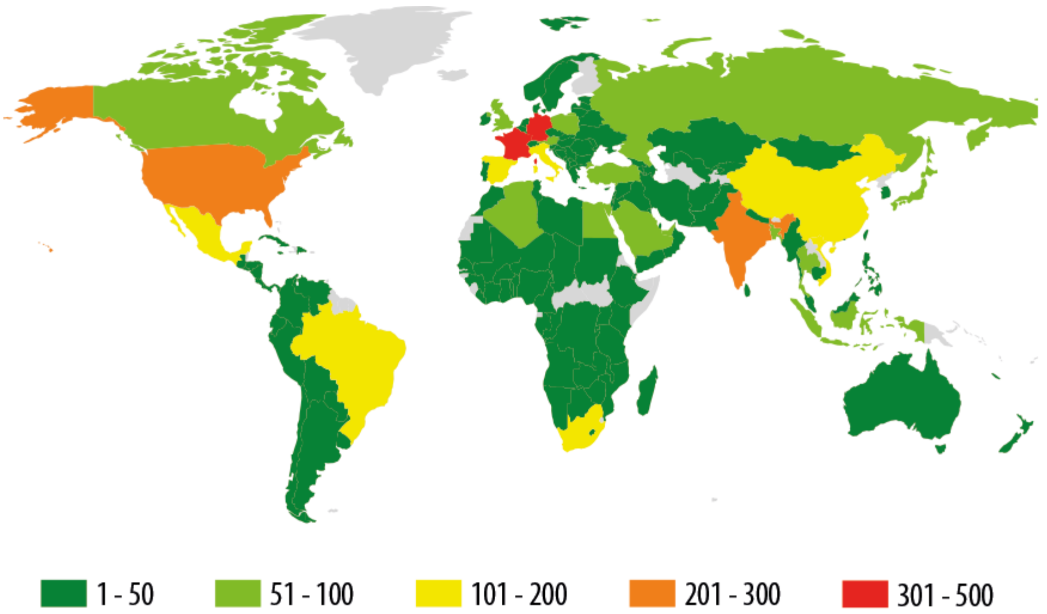
In addition, ransomware Trojans are expanding their sphere of activity; in Q1 2016, CTB-Locker targeted web servers.

The earlier version of CTB-Locker known as crypto-ransomware Onion differed from other ransomware in that it used the anonymous network Tor to protect its command servers from being disabled because, as a rule, it is only possible to disable static servers. The use of Tor also helped the malware avoid detection and blocking. There was one more thing that protected CTB-Locker operators: payment was only accepted in Bitcoins, a decentralized anonymous cryptocurrency.

The new version of this malicious program encrypts web servers, and demands less than half a Bitcoin (~ $150) as ransom. If the money is not paid on time, the ransom is doubled to about $300. Once the ransom is paid, a key is generated to decrypt the web server files.

However, the biggest crypto epidemic of Q1 2016 was caused by the ransomware Trojan Locky (detected by Kaspersky Lab products as Trojan-Ransom.Win32.Locky).

This Trojan is continuing to spread; Kaspersky Lab products have recorded attempts to infect users in 114 countries around the world.

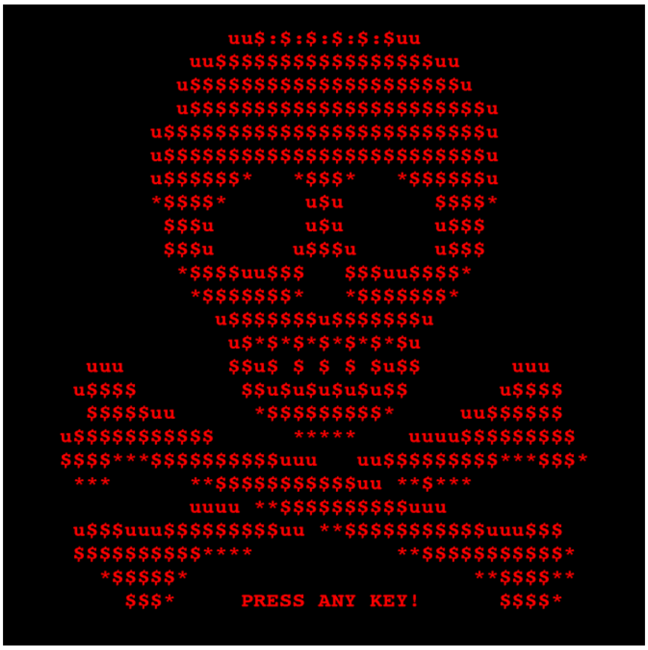


In order to spread the Trojan, the cybercriminals use mass mailings in which malicious loaders are attached to spam messages. Initially, the malicious spam messages contained a DOC file attachment with a macro that downloaded the Locky Trojan from a remote server and executed it.

At the time of writing, the malicious spam is still being sent, but instead of DOC files being attached there are now ZIP archives containing one or more obfuscated scripts in JavaScript. The messages are mostly in English, though some bilingual variants have appeared.

The most significant technical innovation in ransomware was full disk encryption (more specifically, encryption of the file system table) rather than file encryption. This trick was used by the Petya Trojan (the fact that it has a Russian name does not necessarily mean that it was created by Russian-language malware writers).

After encrypting the main file table, Petya shows its true face – a skull and crossbones composed of ASCII characters. Then the typical encryptor routine begins: the Trojan demands a ransom from the victim, 0.9 Bitcoin (about $380) in this case.



```
             uu$:$:$:$:$:$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$u$u$u$u$u$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$$     *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

At this stage, the only thing that distinguishes Petya from other ransomware is the fact that it operates without an Internet connection. This is hardly surprising though, because Petya basically "eats" the operating system, including its ability to connect to the Internet. This means the user has to go to another computer to pay the ransom and recover their data.

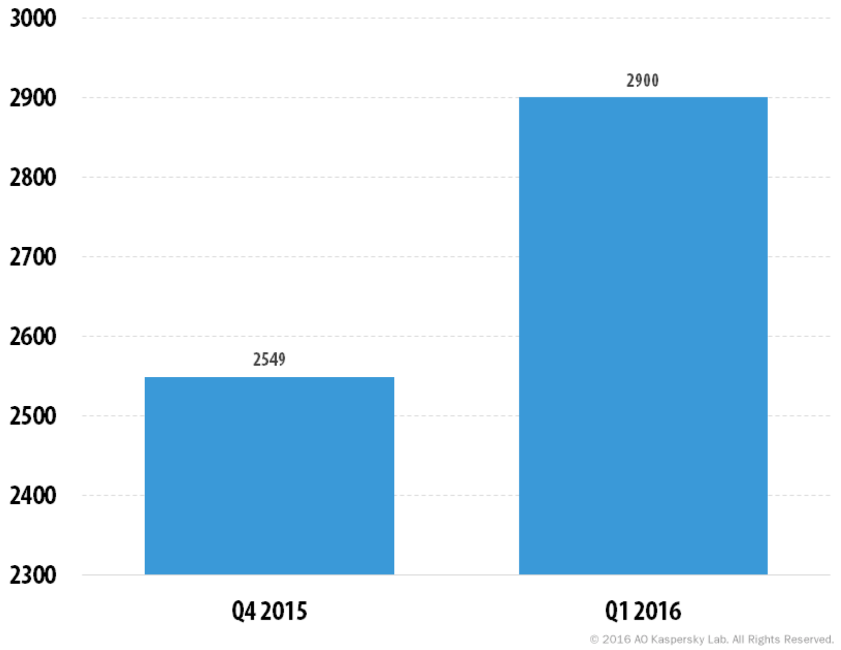
In March, yet another encryptor for Mac OS X was discovered – Trojan-Ransom.OSX.KeRanger. The attackers used it to infect two BitTorrent client installers from the open source Transmission project, which were available for download on their official website. Most likely, the project site was hacked, and the files for download were substituted for malicious recompiled versions. The KeRanger Apple encryptor was signed with a valid Apple certificate, and could therefore bypass the Gatekeeper security feature.

Statistics on Trojan encryptors

Encryptors belong to the Trojan-Ransom class of malware, i.e. to ransomware. Today, in addition to encryptors this class of malicious programs also includes so-called browser ransomware. In the general flow of Trojan-Ransom detections the share of browser ransomware accounts for 25%, and that is mainly in Russia and the CIS. In this section, we will not dwell on browser ransomware, but will look at malicious encryptors in more detail.

The number of new Trojan-Ransom encryptors

The following graph represents the rise in the number of newly created encryptor modifications over the last two quarters.

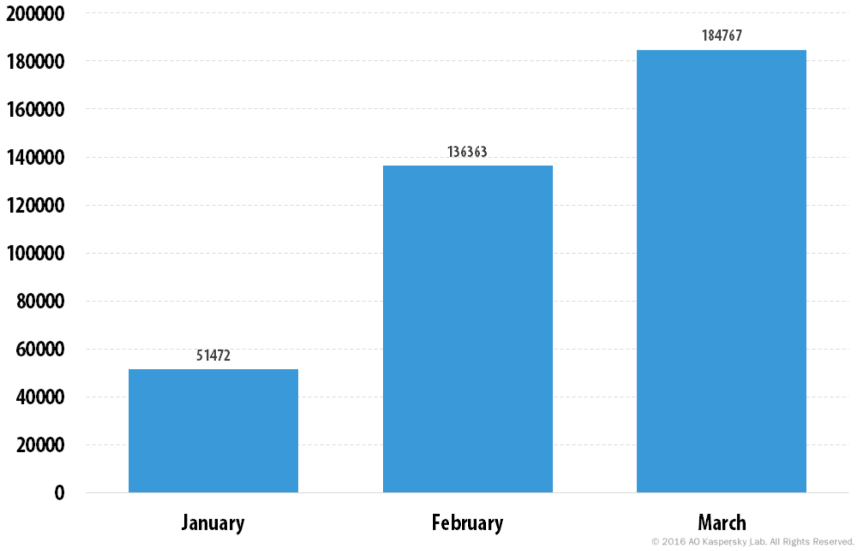


Number of Trojan-Ransom encryptor modifications in Kaspersky Lab's Virus Collection

(Q4 2015 vs Q1 2016)

The overall number of encryptor modifications in our Virus Collection to date is at least 15,000. Nine new encryptor families and 2,900 new modifications were detected in Q1.

The number of users attacked by encryptors



Number of users attacked by Trojan-Ransom encryptor malware (Q1 2016)

In Q1 2016, **372,602** unique users were attacked by encryptors, which is 30% more than in the previous quarter. Approximately 17% of those attacked were in the corporate sector.

It is important to keep in mind that the real number of incidents is several times higher: the statistics reflect only the results of signature-based and heuristic detections, while in most cases Kaspersky Lab products detect encryption Trojans based on behavior recognition models and issue the Generic verdict, which does not distinguish the types of malicious software.

Top 10 countries attacked by encryptors

	Country*	% of users attacked by encryptors**
1	Italy	3.06
2	Netherlands	1.81
3	Belgium	1.58
4	Luxembourg	1.36
5	Bulgaria	1.31
6	Croatia	1.16
7	Rwanda	1.15
8	Lebanon	1.13
9	Japan	1.11
10	Maldives	1.11

** We excluded those countries in which the number of Kaspersky Lab product users is relatively small (less than 10,000).*
*** Unique users whose computers have been targeted by Trojan-Ransom encryptor malware as a percentage of all unique users of Kaspersky Lab products in the country.*

In Q1, the first six places in the Top 10 were occupied by European countries. Italy (3.06%) topped the rating; the most widespread encryptor family in this country was Teslacrypt (Trojan-Ransom.Win32.Bitman). Italy was followed by the Netherlands (1.81%) and Belgium (1.58%).

Top 10 most widespread encryptor families

	Name	Verdict*	Percentage of users**
1	Teslacrypt	Trojan-Ransom.Win32.Bitman/Trojan-Ransom.JS.Cryptoload	58.43%
2	CTB-Locker	Trojan-Ransom.Win32.Onion/Trojan-Ransom.NSIS.Onion	23.49%
3	Cryptowall / Cryptodef	Trojan-Ransom.Win32.Cryptodef	3.41%
4	Cryakl	Trojan-Ransom.Win32.Cryakl	3.22%
5	Scatter	Trojan-Ransom.BAT.Scatter/Trojan-Downloader.JS.Scatter/Trojan-Dropper.JS.Scatter/Trojan-Ransom.Win32.Scatter	2.47%
6	Rakhni	Trojan-Ransom.Win32.Rakhni/Trojan-Downloader.Win32.Rakhni	1.86%
7	Locky	Trojan-Ransom.Win32.Locky	1.30%

8	Shade	Trojan-Ransom.Win32.Shade	1.21%
9	iTorLock / Troli	Trojan-Ransom.MSIL.Lortok	0.84%
10	Mor / Gulcrypt	Trojan-Ransom.Win32.Mor	0.78%

** These statistics are based on detection verdicts received from users of Kaspersky Lab products who have consented to provide their statistical data.*

*** Unique users whose computers have been targeted by a specific Trojan-Ransom family as a percentage of all users of Kaspersky Lab products attacked by Trojan-Ransom malware.*

First place in Q1 was occupied by the Teslacrypt family represented by two verdicts: Trojan-Ransom.Win32.Bitman and Trojan-Ransom.JS.Cryptoload. The second verdict is typical for scripts that are sent out in ZIP archives as part of spam mailings. In the past, these scripts downloaded malware such as Fareit and Cryptowall, but recently the attackers have switched to TeslaCrypt. Noticeably, in Q1 new versions of this encryptor with an improved encryption algorithm were spread this way: the authors used the “reliable” RSA-4096 instead of AES.

Second came the CTB-Locker (Trojan-Ransom.Win32 / NSIS.Onion) family. The members of this family are usually distributed via an affiliate program, and are supported in many languages. As mentioned above, in the first quarter of 2016, a new variant of the CTB-Locker that targets web servers only was discovered. It has already successfully encrypted web-root files in more than 70 servers located in 10 countries.

The Trojan-Ransom.Win32.Cryptodef family also known as Cryptowall came third. Its representatives, as in the case of Teslacrypt, are spread via spam mass mailings.

In fifth place is the Scatter family. Earlier this year, a new wave of proliferation involving this encryptor via spam mailings was registered. The emails contained a link to a JS script that was masked in order to make the user download and launch it locally. Interestingly, when the script runs, in addition to Scatter, it saves two other malicious programs to the disk: Nitol (DDoS-bot) and Pony (a Trojan designed to steal information, mostly passwords).

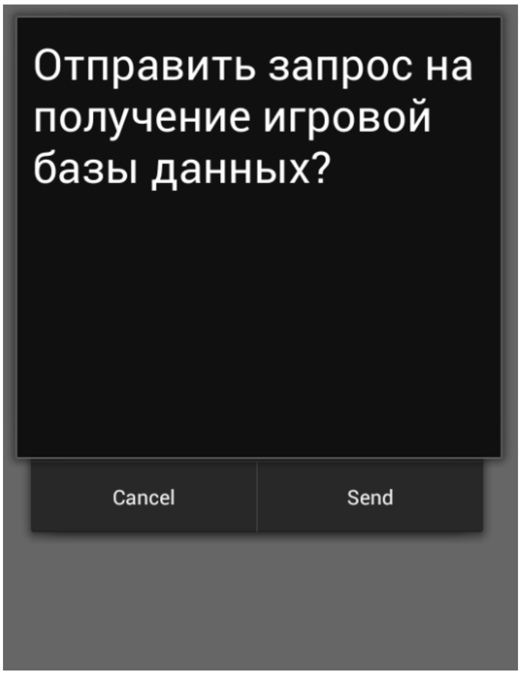
The Locky family, which occupied seventh place in the Q1 rating, was notable for its wide geographic spread, mainly across Europe. Located on the Tor network, the site containing the criminals’ demands supports more than two dozen languages, which doesn’t include Russian or other CIS languages. This may mean that cybercriminals are not interested in attacking victims in these countries, something that is confirmed by the KSN statistics.

Statistics

All the statistics used in this report were obtained using Kaspersky Security Network (KSN), a distributed antivirus network that works with various anti-malware protection components. The data was collected from KSN users who agreed to provide it. Millions of Kaspersky Lab product users from 213 countries and territories worldwide participate in this global exchange of information about malicious activity.

Mobile threats

Cybercriminals continue to improve **new techniques for deceiving users.** This quarter, we identified two mobile Trojans that counter standard security mechanisms used by operating systems. One version of Trojan-Banker.AndroidOS.Asacub overlays the regular system window requesting device administrator privileges with its own window containing buttons. The Trojan thereby conceals the fact that it is gaining elevated privileges in the system from the user, and tricks the user into approving these privileges. Another Trojan using a similar method is Trojan-SMS.AndroidOS.Tiny.aw. In recent versions of Android the system asks for the user's approval when an SMS is sent to a premium number. The Tiny SMS Trojan overlays this dialog with its own screen without covering the buttons in the original window.



Отправить запрос на получение игровой базы данных?

Request screen of Trojan-SMS.AndroidOS.Tiny.aw overlaying a notification about the sending of an SMS to a premium-rate number *(The message states: Would you like to send a request to receive a gaming database?)*

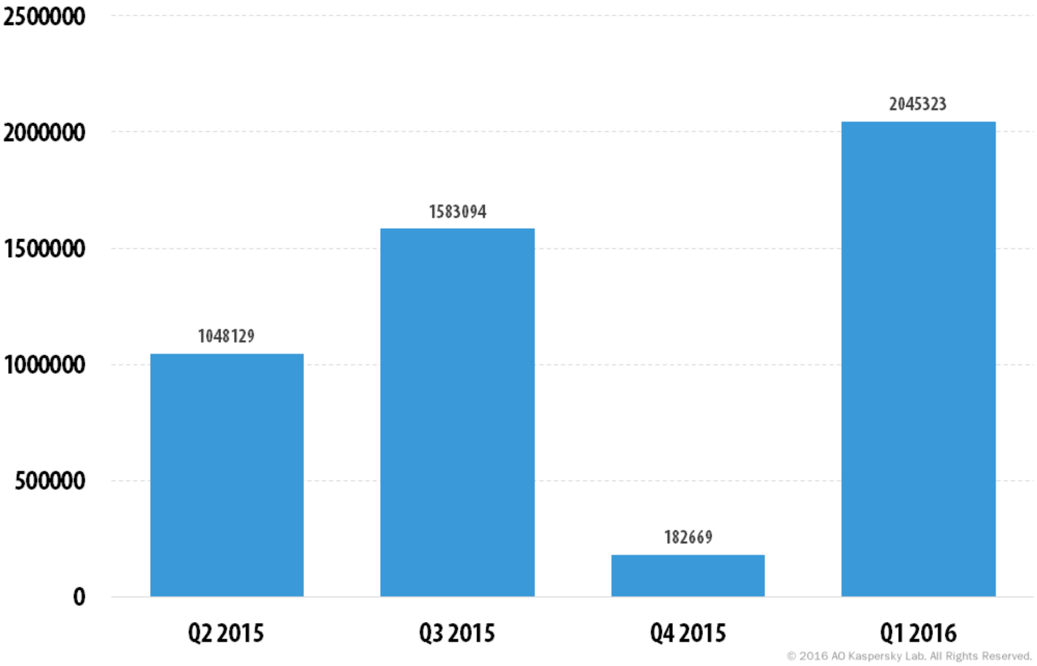
The Trojan's request is presented in such a way that the user will most probably agree to send the SMS to a premium-rate number without having the vaguest idea of what happened next.

In the Q3 2015 report we mentioned the banking Trojan Trojan-Banker.AndroidOS.Marcher. This quarter, we were able to detect **new versions of Marcher** which attacked nearly 40 banking apps, mostly belonging to European banks. Unlike most other mobile Trojans, Marcher uses phishing web pages rather than its own windows to overlay banking app screens.

In Q1, we saw an **increase in activity by the mobile ransomware Trojan-Ransom.AndroidOS.Fusob.pac,** which blocks the user's device and demands a ransom for decryption. In the first three months of 2016, Fusob became the most popular mobile Trojan of this type – it accounted for over 64% of users attacked by mobile ransomware. The total number of users attacked by mobile ransomware Trojans increased more than 1.8 times compared to the previous quarter.

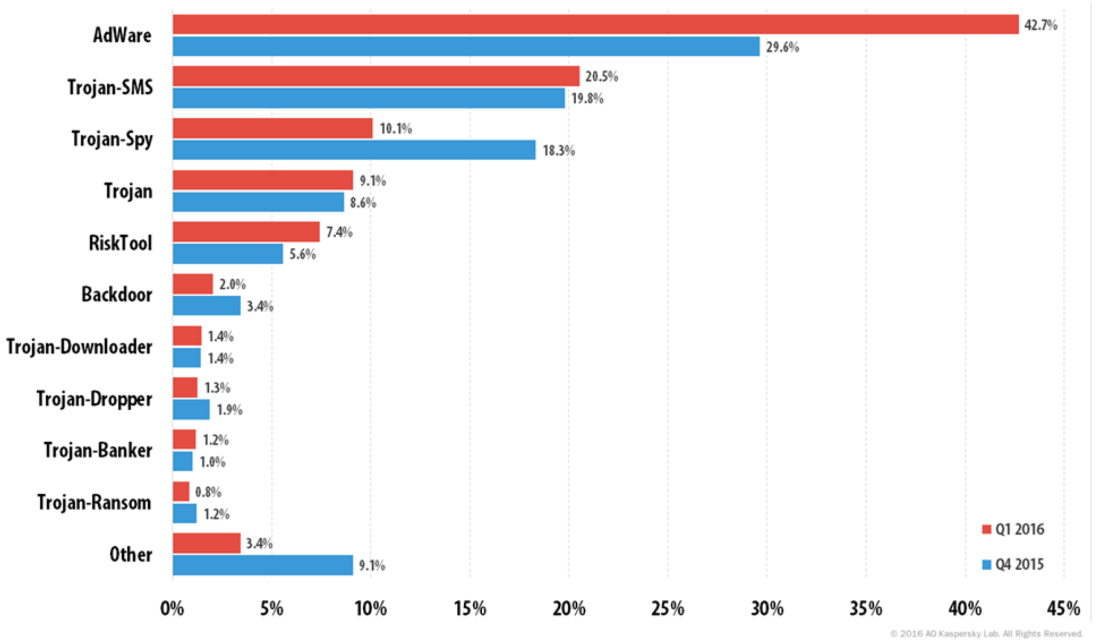
The number of new mobile threats

In Q1 2016, Kaspersky Lab detected **2,045,323** malicious installation packages **–** this is 11 times greater than in Q4 2015, and 1.2 times more than in Q3 2015.



Number of detected malicious installation packages (Q2 2015 – Q1 2016)

Distribution of mobile malware by type



Distribution of new mobile malware by type, Q1 2016 vs. Q4 2015

In Q1 2016, adware programs continued to top the rating of detected malicious objects for mobile devices. The share of adware programs grew 13 p.p. compared to Q4 2015, and reached 42.7%. Notably, this is lower than in Q3 2015 (52.5%).

Second place is occupied by an SMS Trojan, and it is the second quarter in a row that we have seen a growth in the share of detections of this type of object. In Q4 2015, the share of SMS Trojans rose dramatically from 6.2% to 19.8%, and grew by another 0.7 p.p. in Q1 2016, and amounted to 20.5%.

Trojan spyware programs, with a 10% share, were right behind the SMS Trojans. These programs steal the user's personal data, including incoming messages (mTANs) from banks.

RiskTool software, or legal applications that are potentially dangerous to users, had occupied the first or second position in this rating for nearly two years. However, starting in Q4 2015 they fell to the fifth place. In Q4 2014, there share was 5.6%, and in Q1 2016 7.4%.

The share of banking Trojans has continued to grow, and amounted to 1.2% in Q1 2016.

TOP 20 mobile malware programs

Please note that this ranking of malicious programs does not include potentially dangerous or unwanted programs such as RiskTool or adware.

	Name	% of attacked users*
1	DangerousObject.Multi.Generic	73.7
2	Backdoor.AndroidOS.Ztorg.c	11.3
3	Trojan.AndroidOS.Iop.c	8.9
4	Trojan.AndroidOS.Ztorg.a	8.7
5	Trojan-Ransom.AndroidOS.Fusob.pac	6.2

6	Trojan-Dropper.AndroidOS.Agent.ar	4.6
7	Trojan-Clicker.AndroidOS.Gopl.a	4.5
8	Backdoor.AndroidOS.Ztorg.b	4.3
9	Trojan.AndroidOS.Iop.m	3.7
10	Trojan.AndroidOS.Agent.ej	3.7
11	Trojan.AndroidOS.Iop.q	3.5
12	Trojan.AndroidOS.Ztorg.i	3.3
13	Trojan.AndroidOS.Muetan.b	3.1
14	Trojan.AndroidOS.Agent.gm	3.1
15	Trojan-SMS.AndroidOS.Podec.a	3.1
16	Trojan-Downloader.AndroidOS.Leech.a	3.0
17	Trojan-Dropper.AndroidOS.Guerrilla.b	2.8
18	Exploit.AndroidOS.Lotoor.be	2.8
19	Backdoor.AndroidOS.Ztorg.a	2.8
20	Backdoor.AndroidOS.Triada.d	2.4

** Percentage of users attacked by the malware in question, relative to all users attacked*

First place is occupied by DangerousObject.Multi.Generic (44.2%), used for malicious programs detected by cloud technologies. Cloud technologies work when the antivirus database contains neither the signatures nor heuristics to detect a malicious program, but the cloud of the antivirus company already contains information about the object. This is basically how the very latest malware is detected.

An increasing number of entries in the TOP 20 are occupied by Trojans that use advertising as their main means of monetization. Their goal is to deliver as much advertisements as possible to the user, employing various methods, including the installation of new adware. These Trojans may use superuser privileges to conceal themselves in the system application folder, from which it will be very difficult to delete them. In Q1, 16 such programs made it into the TOP 20: three programs from the family Backdoor.AndroidOS.Ztorg, three from the family Trojan.AndroidOS.Iop, two from the family Trojan.AndroidOS.Ztorg, plus Trojan-Dropper.AndroidOS.Agent.ar, Trojan-Clicker.AndroidOS.Gopl.a, Trojan.AndroidOS.Agent.ej, Trojan.AndroidOS.Muetan.b, Trojan.AndroidOS.Agent.gm, Trojan-Downloader.AndroidOS.Leech.a, Trojan-Dropper.AndroidOS.Guerrilla.b, and Backdoor.AndroidOS.Triada.d.

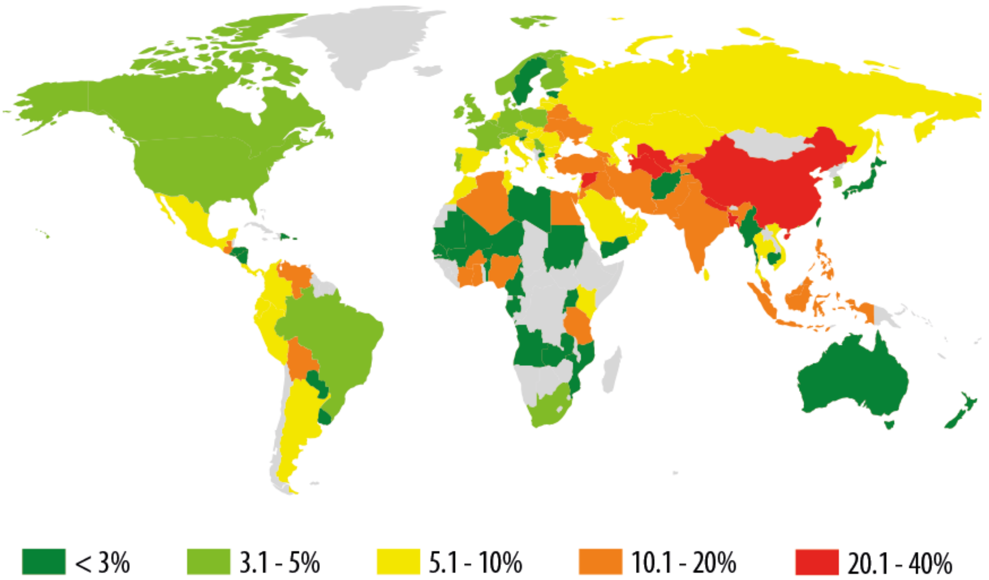
Backdoor.AndroidOS.Triada is a new entry in the TOP 20 of mobile malware. The main function of this Trojan is to redirect financial SMS transactions when the user makes online payments to buy additional content in legitimate apps. The money goes to the attackers rather than to the software developer. Triada is the most complex mobile malware program that we know of. Its distinctive feature is the use of the Zygote process to implement its code in the context of all the applications on the device. Triada penetrates virtually all applications running on the infected device, and continues to exist in the RAM memory only. In addition, all the Trojan’s separately launched processes are concealed from the user and other applications.

The ransomware Trojan Trojan-Ransom.AndroidOS.Fusob.pac is in fifth place (6.2%). This Trojan demands a $200 ransom from victims to unblock their devices. A substantial number of the victims are located in North America (the US and Canada) and Europe (mostly in Germany, Italy, the UK, Spain and Switzerland).

Trojan-SMS.AndroidOS.Podec.a (3%) has spent over a year now in the mobile malware TOP 20, although now it is beginning to lose ground. Earlier it was consistently among the top 5 mobile threats, but in Q1 2016 it only made it into the bottom half of the rating. The number of users attacked by this Trojan fell 1.7 times compared to Q4 2015. Its functionality has remained practically unchanged; the main means of monetization is still achieved by subscribing the user to paid services.

Also making it into the rating is Exploit.AndroidOS.Lotoor.be, an exploit used to gain local super-user rights.

The geography of mobile threats



© 2016 AO Kaspersky Lab. All Rights Reserved.

The geography of mobile malware infection attempts in Q1 2016 (percentage of all users attacked)

Top 10 counties attacked by mobile malware (ranked by percentage of users attacked)

	Country*	% of users attacked**
1	China	38.2
2	Bangladesh	27.6
3	Uzbekistan	21.3
4	Algeria	17.6
5	Nigeria	17,4
6	India	17.0
7	Philippines	15.7

8	Indonesia	15,6
9	Ukraine	15.0
10	Malaysia	14.0

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*

*** Percentage of unique users attacked in each country relative to all users of Kaspersky Lab's mobile security product in the country.*

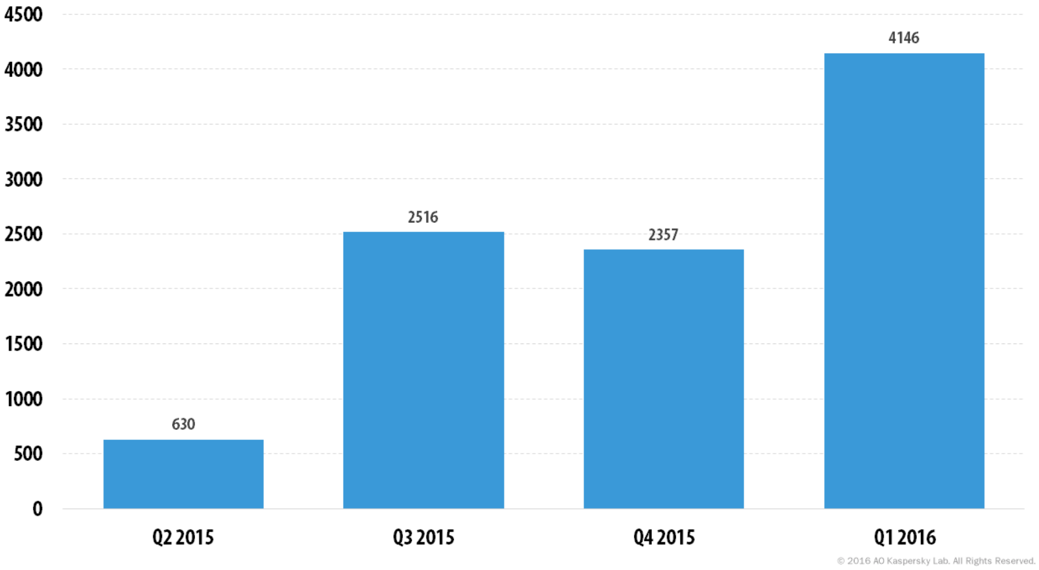
China topped the ranking, with 40% of users encountering a mobile threat at least once during the year. To recap, in 2015 China also came first in the ranting.

In all the countries of the Top 10 except for China the most popular mobile malware was the same – advertising Trojans that appeared in the TOP 20 mobile malware, and AdWare. In China, a significant proportion of attacks also involved advertising Trojans, but the majority of users encountered the Backdoor.AndroidOS.GinMaster and Backdoor.AndroidOS.Fakengry families. Representatives of the RiskTool.AndroidOS.SMSreg family were also popular. If used carelessly, these programs could result in money being withdrawn from a mobile account.

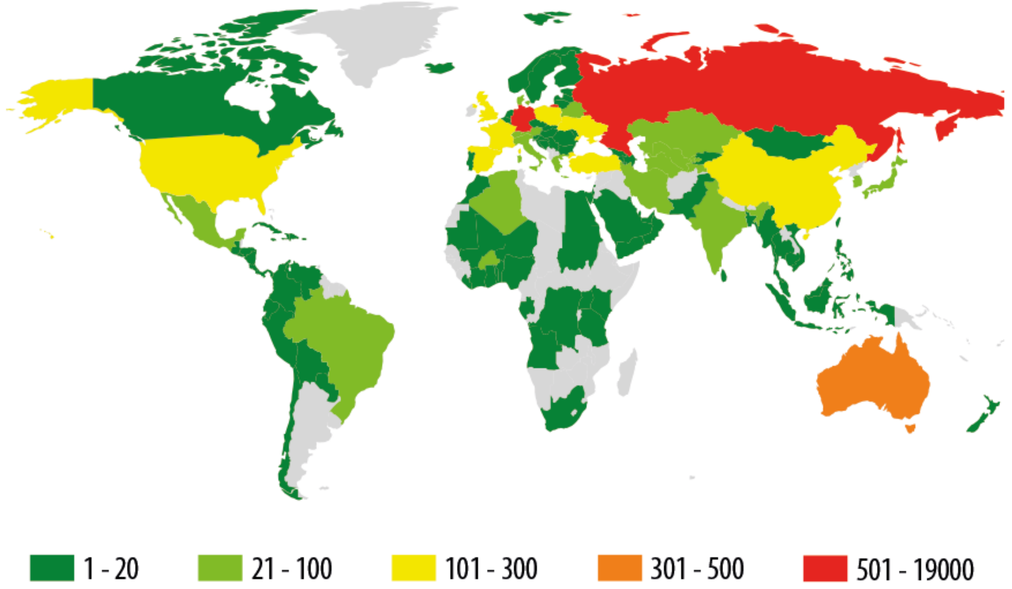
The safest countries are Taiwan (2.9%), Australia (2.7%) and Japan (0.9%).

Mobile banking Trojans

Over the reporting period, we detected 4,146 mobile Trojans, which is 1.7 times more than in the previous quarter.



Number of mobile banking Trojans detected by Kaspersky Lab solutions (Q2 2015 – Q1 2016)



Geography of mobile banking threats in Q1 2016 (number of users attacked)

The number of attacked users depends on the overall number of users within each individual country. To assess the risk of a mobile banker Trojan infection in each country, and to compare it across countries, we created a country ranking according to the percentage of users attacked by mobile banker Trojans.

Top 10 counties attacked by mobile banker Trojans (ranked by percentage of users attacked)

	Country*	% of users attacked**
1	China	0.45
2	Australia	0.30
3	Russia	0.24
4	Uzbekistan	0.20
5	Ukraine	0.08
6	France	0.06
7	Byelorussia	0.05
8	Turkey	0.05
9	Japan	0.03
10	Kazakhstan	0.03

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*
*** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all users of Kaspersky Lab's mobile security product in the country.*

In Q1 2016, first place was occupied by China where the majority of affected users encountered the Backdoor.AndroidOS.GinMaster and Backdoor.AndroidOS.Fakengry families of mobile banker Trojans. In second place was Australia where the Trojan-

Banker.AndroidOS.Acecard family was replaced by the Trojan-Banker.AndroidOS.Marcher family as the most popular threat.

TOP 10 countries by the percentage of users attacked by mobile banking Trojans relative to all attacked users

An indication of how popular mobile banker Trojans are with cybercriminals in each country can be provided by the percentage of users who were attacked at least once by mobile banker Trojans during the quarter, relative to all users in the same country whose mobile security product was activated at least once in the reporting period. This ranking differs from the one above:

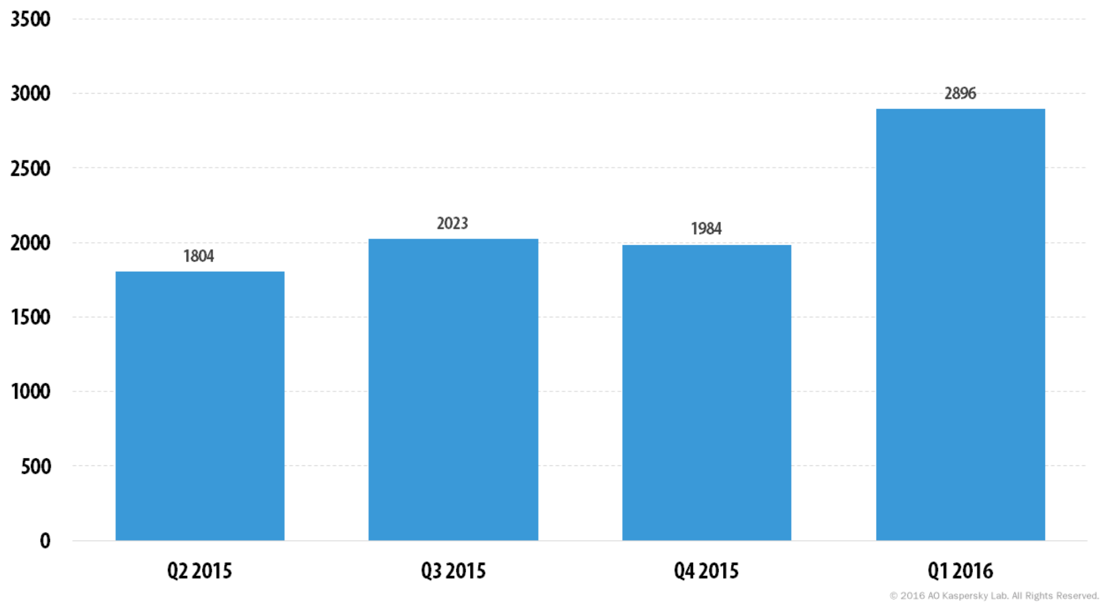
	Country*	% of users attacked**
1	Australia	13.4
2	Russia	5.1
3	United Kingdom	1.6
4	Turkey	1.4
5	Austria	1.3
6	France	1.3
7	Poland	1.2
8	China	1.1
9	Hong Kong	1
10	Switzerland	0.9

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*
*** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all unique users attacked by mobile malware in the country.*

To recap, Australia was among the Top 3 countries with the lowest percentage of users attacked by mobile malware. However, in this ranking Australia ended in first place: more than 13% of all users attacked by mobile malicious programs were attacked by mobile bankers. Meanwhile China, which came first in the previous ranking, ended the quarter in tenth place. In other words, in China the cybercriminals' mobile banking Trojans are less popular than other types of mobile malware.

Mobile Trojan-Ransom

In Q1 2016, we detected 2,896 mobile ransomware samples, which is 1.4 times more than in the previous quarter.



Number of mobile Trojan-Ransomware programs detected by Kaspersky Lab (Q2 2015 – Q1 2016)

TOP 10 countries attacked by Trojan-Ransomware as a percentage of attacked users:

	Country*	% of users attacked**
1	Kazakhstan	0.92
2	Germany	0.83
3	Uzbekistan	0.80
4	Canada	0.71
5	Italy	0.67
6	Netherlands	0.66
7	United Kingdom	0.59
8	Switzerland	0.58
9	USA	0.55
10	Spain	0.36

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*
*** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all users attacked by mobile malware in the country.*

In all the countries of the TOP 10, except for Kazakhstan and Uzbekistan, the most popular Trojan-Ransom family was Fusob, especially its Trojan-Ransom.AndroidOS.Fusob.pac modification (note, this malicious program was fifth in the ranking of mobile threats).

In Kazakhstan and Uzbekistan, which came first and third respectively, the main threat to users originated from representatives of the Small family of mobile Trojan-Ransom. This is a fairly simple ransomware program that blocks operation of a device by overlaying all the windows on the device with its own window and demands $10 to unblock it.

Vulnerable applications used by cybercriminals

In Q1 2016, exploits for Adobe Flash Player remained popular. During the reporting period two new vulnerabilities in this software were detected:

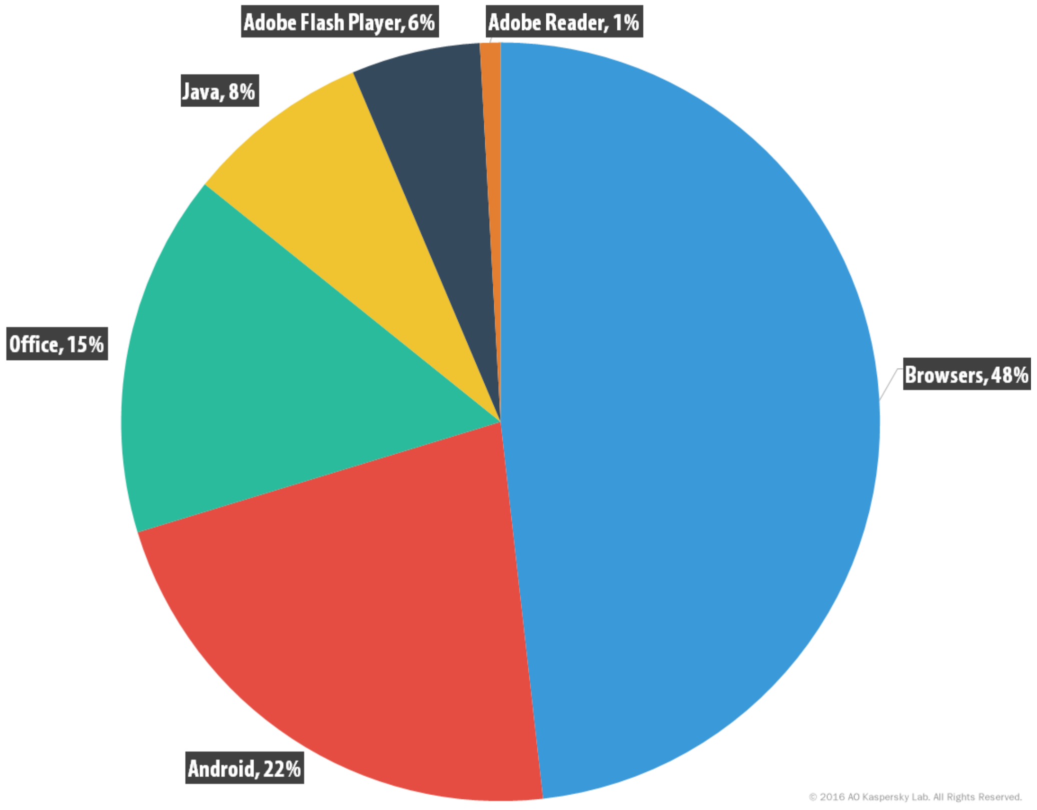
- CVE-2015-8651
- CVE-2016-1001

The first exploit pack to add support for these vulnerabilities was Angler.

One notable event in the first quarter was the use of an exploit for Silverlight - CVE-2016-0034. At the time of publication, this vulnerability is used by the Angler and RIG exploit packs.

As is now traditional, some popular packs included an exploit for the Internet Explorer (CVE-2015-2419) vulnerability.

The overall picture of the use of exploits in the first quarter looks as follows:



Distribution of exploits used in attacks by the type of application attacked, Q1 2016

As expected, we have seen a decline in the share of exploits for Java (-3 percentage points) and an increase in the use of Flash exploits (+1 p.p.). There was also a significant increase in the percentage of exploits for Microsoft Office (+10 p.p.): this group mainly includes exploits for vulnerabilities in Microsoft Word. This significant growth was caused by spam mailings containing these exploits.

Overall, the first quarter of 2016 continued the trend of the past few years – cybercriminals are focused on exploits for Adobe Flash Player and Internet Explorer. In our chart, the latter is included in the "Browsers" category together with detections of landing pages that "distribute" exploits.

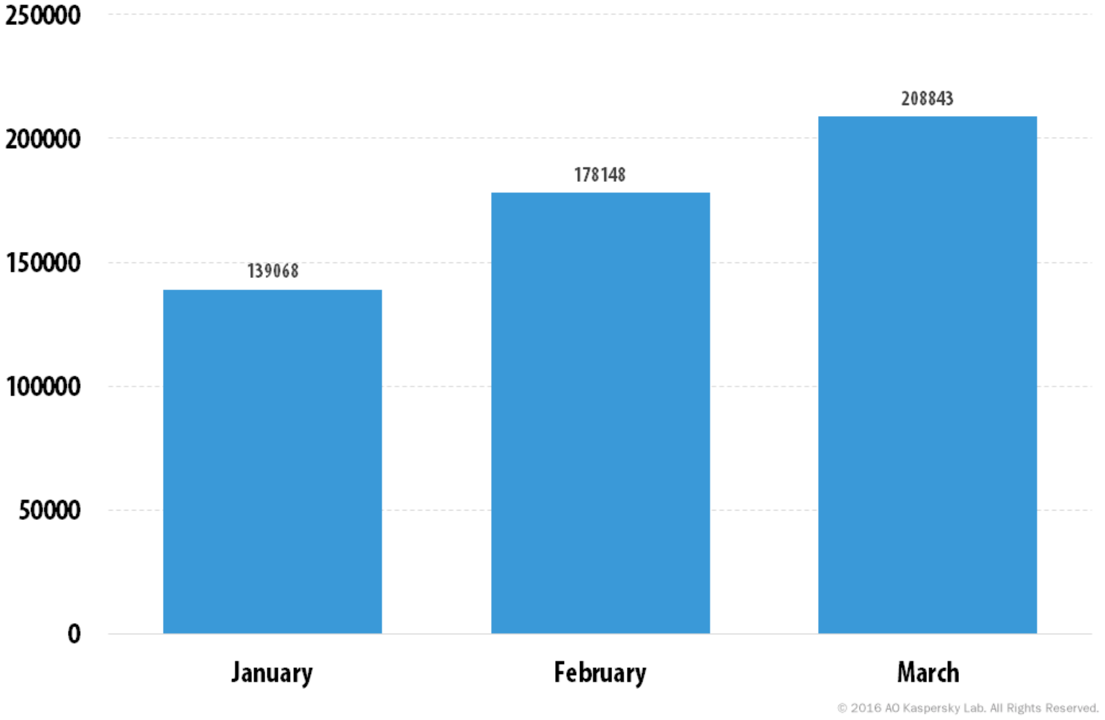
Online threats (Web-based attacks)

The statistics in this section were derived from web antivirus components that protect users from attempts to download malicious objects from a malicious/infected website. Malicious websites are created deliberately by malicious users; infected sites include those with user-contributed content (such as forums), as well as compromised legitimate resources.

In the first quarter of 2016, Kaspersky Lab’s web antivirus detected 18,610,281 unique malicious objects: scripts, exploits, executable files, etc. 74,001,808 unique URLs were recognized as malicious by web antivirus components.

Online threats in the banking sector

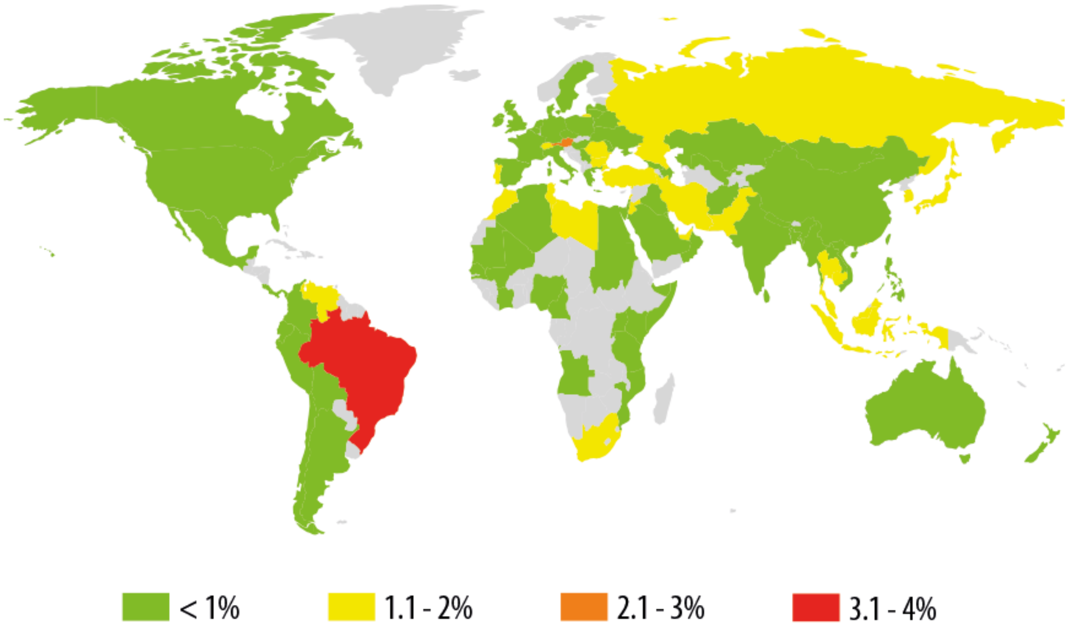
In the first three months of 2016, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on 459,970 computers. We are witnessing a decline in financial malware activity: the figure for Q1 is 23.3% lower than in the previous quarter (597,415). A year ago, in Q1 2015 this figure was 699,652, which translates into a 34.26% fall in the number of victims over the past year.



Number of attacks by financial users, Q1 2016

Geography of attacks

To evaluate and compare the degree of risk of being infected by banking Trojans worldwide, we calculate the percentage of Kaspersky Lab product users who encountered this type of threat during the reporting period in the country, relative to all users of our products in the county.



© 2016 AO Kaspersky Lab. All Rights Reserved.

Geography of banking malware attacks in Q1 2016 (percentage of attacked users)

Top 10 countries by the percentage of attacked users

	Country*	% attacked users**
1	Brazil	3.86
2	Austria	2.09
3	Tunisia	1.86
4	Singapore	1.83
5	Russia	1.58
6	Venezuela	1.58
7	Morocco	1.43
8	Bulgaria	1.39
9	Hong Kong	1.37
10	United Arab emirates	1.30

These statistics are based on the detection verdicts returned by the antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.
** We excluded those countries in which the number of Kaspersky Lab product users is relatively small (less than 10,000).*

*** Unique users whose computers have been targeted by banking Trojan attacks as a percentage of all unique users of Kaspersky Lab products in the country.*

In Q1 2016, Brazil had the highest percentage of Kaspersky Lab users who were attacked by banking Trojans. One of the reasons for the growth of financial threats in this country was the emergence of cross-platform Trojan bankers. Noticeably, most countries in the TOP 10 have a high level of technological development and/or well-developed banking system which attracts cybercriminals.

In Russia, 1.58% of users encountered a banking Trojan at least once in Q1 (an increase of 1 p.p. compared to the previous quarter). In the US, the figure was 0.26%; Spain - 0.84%; Italy - 0.79%; Germany - 0.52%; the UK - 0.48%; France - 0.36%.

The Top 10 banking malware families

The table below shows the Top 10 malware families most commonly used in Q1 2016 to attack online banking users:

	Name	Number of users attacked
1	Trojan-Spy.Win32.Zbot	419940
2	Trojan-Downloader.Win32.Upatre	177665
3	Trojan-Banker.Java.Agent	68467
4	Trojan-Banker.Win32.Gozi	53978
5	Trojan-Banker.Win32.BestaFera	25923
6	Trojan.Win32.Tinba	24964
7	Trojan-Banker.Win32.Banbra	22942
8	Trojan-Banker.AndroidOS.Agent	19782
9	Trojan-Banker.AndroidOS.Abacus	13446
10	Trojan-Banker.Win32.ChePro	9209

Trojan-Spy.Win32.Zbot topped the ranking. It has become a permanent resident in this ranking, and it is no coincidence that it consistently occupies a leading position. The Trojans of the Zbot family were among the first to use web injections to compromise the payment details of online banking users and to modify the contents of banking web pages. They encrypt their configuration files at several levels; the decrypted configuration file is never stored in the memory in its entirety, but is instead loaded in parts.

The Trojan-Downloader.Win32.Upatre family of malicious programs came second in Q1 2016. The malware is no larger than 3.5 KB in size, and is limited to downloading the payload to the victim computer, most typically a banker Trojan from the Dyre/Dyzap/Dyreza family. The main aim of this family of banking Trojans is to steal the user's payment details. Dyre does this by intercepting the data from a banking session between the victim's browser and the online banking web app, in other words, it uses the “Man-in-the-Browser” (MITB) technique.

It is worth noting that the vast majority of the TOP 10 malware uses the technique of embedding arbitrary HTML code in the web page displayed by the browser and intercepting payment data entered by the user into the original and the inserted web forms.

The TOP 3 threats in the first quarter of 2016 include cross-platform banking malware written in Java. Brazilian cybercriminals have started actively using cross-platform Java Trojans. In addition, Kaspersky Lab experts detected new malicious software also written in Java and used to steal financial information – Adwind RAT. Adwind is written entirely in Java, which is why it can attack all popular platforms: Windows, Mac OS, Linux and Android. The malicious program allows attackers to collect and extract data from the system, as well as remotely control an infected device. To date, it is able to take screenshots, memorize keystrokes, steal passwords and data stored in browsers and web forms, take photos and videos via the webcam, make audio recordings using the microphone built into the device, collect general data about the user and the system, steal VPN certificates and keys from crypto currency wallets and, finally, manage SMS.

Fourth place in the TOP 10 is occupied by Trojan-Banker.Win32.Gozi, which penetrates working processes of popular web browsers to steal payment information. Some samples of this Trojan can infect the MBR (Master Boot Record) and maintain their presence in the operating system, even if it has been reinstalled.

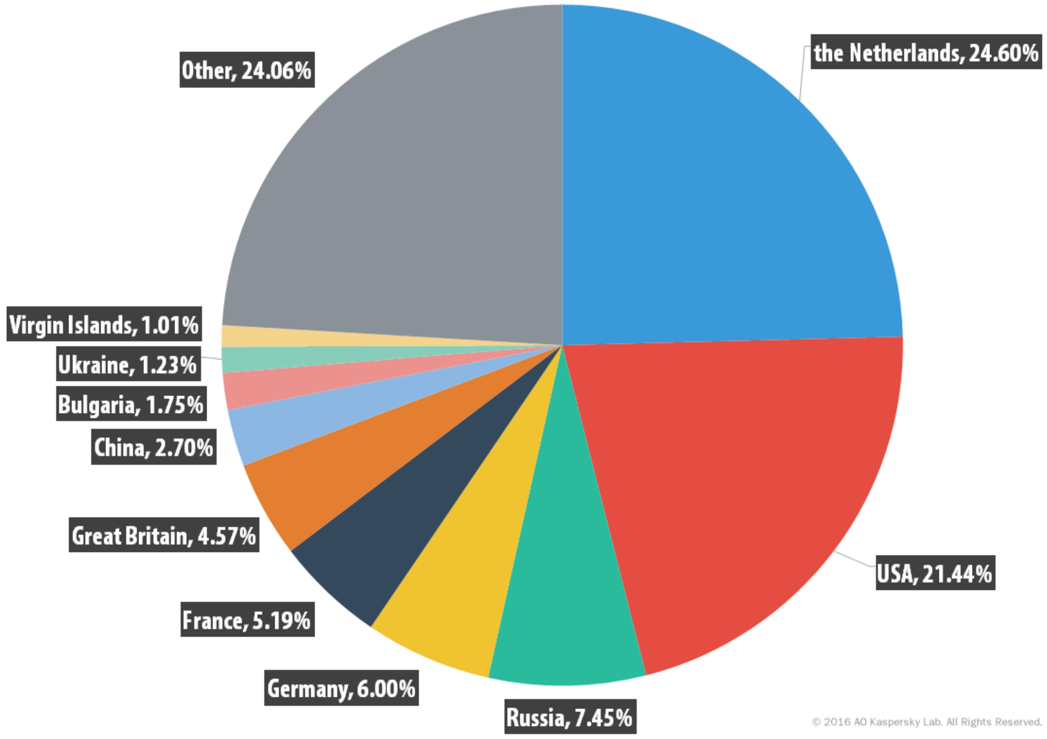
One of the most interesting pieces of malware designed to steal financial data that did not make it into the TOP 10 is Gootkit. It is written using the software platform NodeJS and has a modular architecture. The malicious code interpreter is contained in its body; as a result, it is big - approximately 5 MB. To steal payment data, Gootkit uses http traffic interception and embeds itself in the browser. Other standard Trojan features include execution of arbitrary commands, auto-update, and capturing screenshots. However, this banking Trojan is not particularly widespread.

Top 10 countries where online resources are seeded with malware

The following statistics are based on the physical location of the online resources that were used in attacks and blocked by our antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host could be the source of one or more web attacks.

In order to determine the geographical source of web-based attacks, domain names are matched up against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In Q1 2016, Kaspersky Lab solutions blocked 228,420,754 attacks launched from web resources located in 195 countries around the world. 76% of notifications on blocked web attacks were triggered by attacks coming from web resources located in 10 countries.



Distribution of web attack sources by country, Q1 2016

Q1 saw the Netherlands take over first place (24.6%) from the US (21.44%). Russia (7.45%) and Germany (6%), which followed them, also swapped places. Vietnam has dropped out the Top 10, while Bulgaria is a newcomer in eighth place with 1.75%.

Countries where users faced the greatest risk of online infection

In order to assess the risk of online infection faced by users in different countries, we calculated the percentage of Kaspersky Lab users in each country who encountered detection verdicts on their machines during the quarter. The resulting data provides an indication of the aggressiveness of the environment in which computers work in different countries.

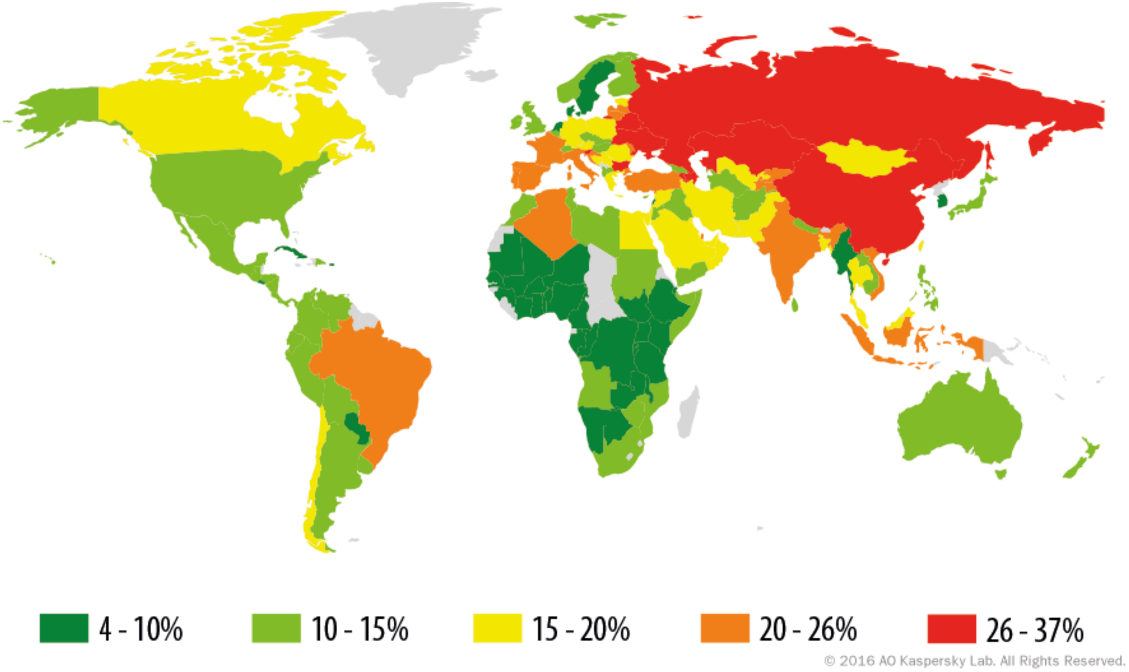
	Country*	% of unique users attacked **
1	Russia	36.28
2	Kazakhstan	33.19
3	China	32.87
4	Azerbaijan	30.28
5	Ukraine	29.96
6	Belarus	29.16
7	Slovenia	26.88
8	Armenia	26.27
9	Vietnam	25.14
10	Moldova	24.68

11	Kyrgyzstan	24.46
12	Spain	24.00
13	India	23.98
14	Brazil	23.68
15	Italy	22.98
16	Algeria	22.88
17	Lithuania	22.58
18	Croatia	22.04
19	Turkey	21.46
20	France	21.46

These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

** These calculations excluded countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).*
*** Unique users whose computers have been targeted by web attacks as a percentage of all unique users of Kaspersky Lab products in the country.*

The leader of this ranking remained unchanged – it is still Russia with 36.3%. Since the previous quarter, Chile, Mongolia, Bulgaria and Nepal have left the Top 20. Newcomers to the ranking are Slovenia (26.9%), India (24%) and Italy (23%).



The countries with the safest online surfing environments included Germany (17.7%), Canada (16.2%), Belgium (14.5%), Switzerland (14%), the US (12.8%), the UK (12.7%), Singapore (11.9%), Norway (11.3%), Honduras (10.7%), the Netherlands (9.6%) and Cuba (4.5%).

On average, 21.42% of computers connected to the Internet globally were subjected to at least one web attack during the three months. This is a fall of 1.5 p.p. compared to Q4 2015.

Local threats

Local infection statistics for users computers are a very important indicator: they reflect threats that have penetrated computer systems using means other than the Internet, email, or network ports.

Data in this section is based on analyzing statistics produced by antivirus scans of files on the hard drive at the moment they were created or accessed, and the results of scanning removable storage media.

In Q1 2016, Kaspersky Lab’s file antivirus detected a total of 174,547,611 unique malicious and potentially unwanted objects.

Countries where users faced the highest risk of local infection

For each of the countries, we calculated the percentage of Kaspersky Lab product users on whose computers the file antivirus had been triggered during the quarter. These statistics reflect the level of personal computer infection in different countries.

Top 20 countries with the highest levels of computer infection

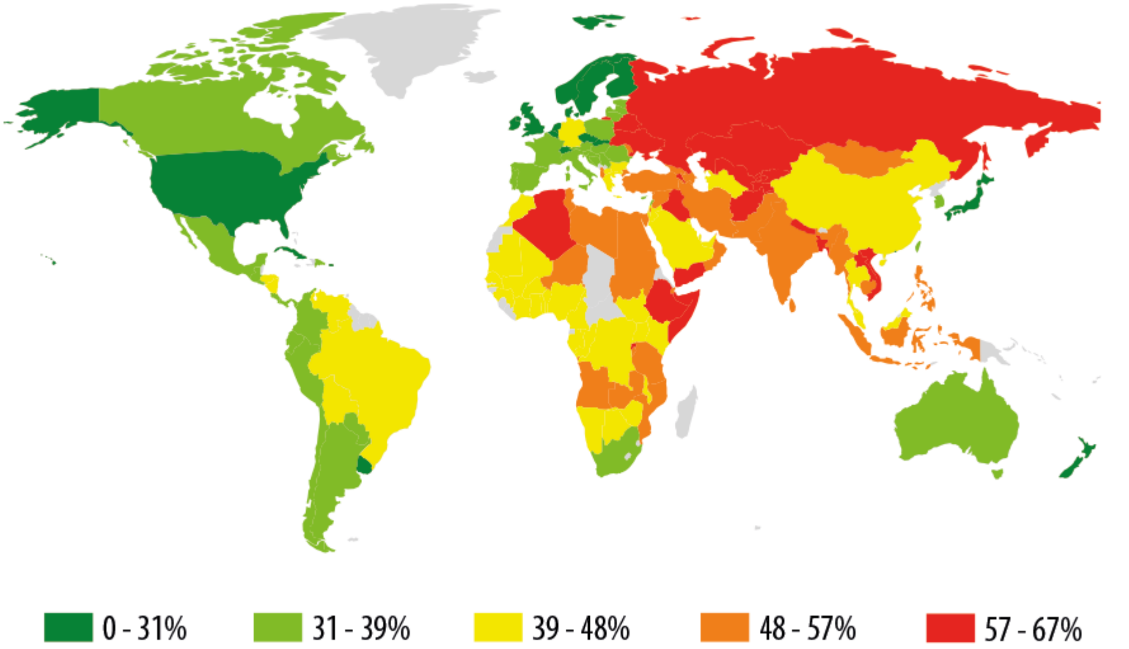
	Country*	% of unique users**
1	Somalia	66.88
2	Yemen	66.82
3	Armenia	65.17
4	Kyrgyzstan	64.45
5	Russia	64.18
6	Tajikistan	64.06
7	Bangladesh	63.00
8	Vietnam	61.31
9	Afghanistan	60.72
10	Kazakhstan	60.62
11	Nepal	59.60
12	Uzbekistan	59.42
13	Ethiopia	59.23
14	Ukraine	58.90
15	Byelorussia	58.51
16	Laos	58.46
17	Rwanda	58.10
18	Iraq	57.16
19	Algeria	57.50
20	Moldova	56.93

These statistics are based on the detection verdicts returned by on-access and on-demand antivirus modules, received from users of Kaspersky Lab products who have consented to provide their statistical data. The data include detections of malicious programs located on users' computers or on removable media connected to the computers, such as flash drives, camera and phone memory cards, or external hard drives.

** These calculations exclude countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).*

*** The percentage of unique users in the country with computers that blocked local threats as a percentage of all unique users of Kaspersky Lab products.*

Somalia became the new leader of this rating in Q1, with 66.9%. Bangladesh, the leader for the past few quarters, dropped to seventh place (63.6%). Newcomers to this ranking are Uzbekistan in 12th place (59.4%), Ukraine in 14th place (58.9%), Belarus in 15th place (58.5%), Iraq in 18th place (57.2%) and Moldova in 20th (57.0%).



The safest countries in terms of local infection risks were the Czech Republic (27.2%), Denmark (23.2%) and Japan (21.0%).

An average of 44.5% of computers globally faced at least one local threat during Q1 2016, which is 0.8 p.p. more than in Q4 2015.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

Tel: +7-495-797-8700
+7-495-737-3412
Fax: +7-495-797-8709