KASPERSKY lab

MOBILE MALWARE EVOLUTION 2016

Contents

The year in figures

In 2016, Kaspersky Lab detected the following:

- 8,526,221 malicious installation packages
- 128,886 mobile banking Trojans
- 261,214 mobile ransomware Trojans

Trends of the year

- Growth in the popularity of malicious programs using super-user rights, primarily advertising Trojans.
- Distribution of malware via Google Play and advertising services.
- Emergence of new ways to bypass Android protection mechanisms.
- Growth in the volume of mobile ransomware.
- Active development of mobile banking Trojans.

Malicious programs using super-user rights

The year's most prevalent trend was Trojans gaining super-user privileges. To get these privileges, they use a variety of vulnerabilities that are usually patched in the newer versions of Android. Unfortunately, most user devices do not receive the latest system updates, making them vulnerable.

Root privileges provide these Trojans with almost unlimited possibilities, allowing them to secretly install other advertising applications, as well as display ads on the infected device, often making it impossible to use the smartphone. In addition to aggressive advertising and the installation of third-party software, these Trojans can even buy apps on Google Play.

This malware simultaneously installs its modules in the system directory, which makes the treatment of the infected device very difficult. Some advertising Trojans are even able to infect the recovery image, making it impossible to solve the problem by restoring to factory settings.

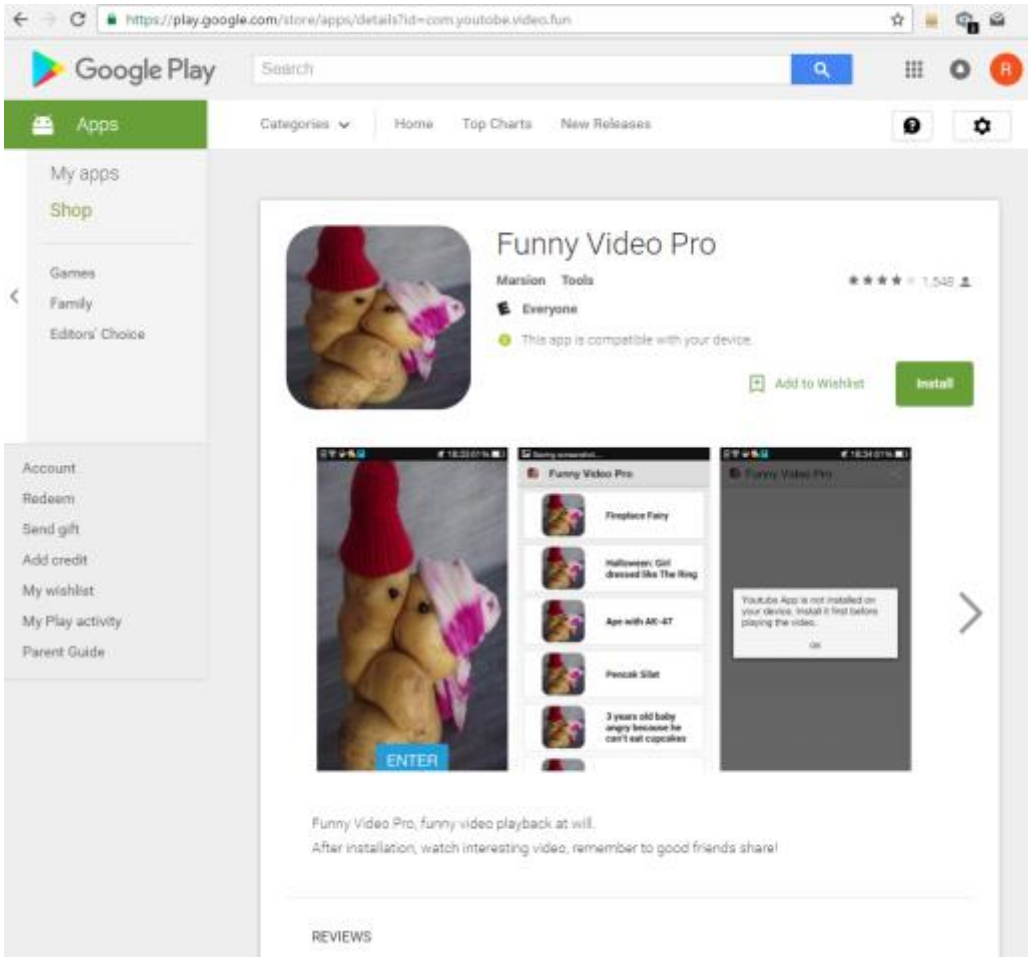
In addition to the secret installation of advertising apps, these Trojans can also install malware. We have registered installations of the modular trojan Backdoor.AndroidOS.Triada, which modified the Zygote processes. This allowed it to remain in the system and alter text messages sent by other apps, making it possible to steal money from the owner of the infected device. With super-user rights the Trojan can do almost anything, including substitute the URL in the browser.

Representatives of this class of malicious software have been repeatedly found in the official Google Play app store, for example, masquerading as a guide for Pokemon GO. This particular app was downloaded over half a million times and was detected as Trojan.AndroidOS.Ztorg.ad.

Trojan.AndroidOS.Ztorg.ad imitating a guide for Pokemon GO

Cybercriminals continue their use of Google Play

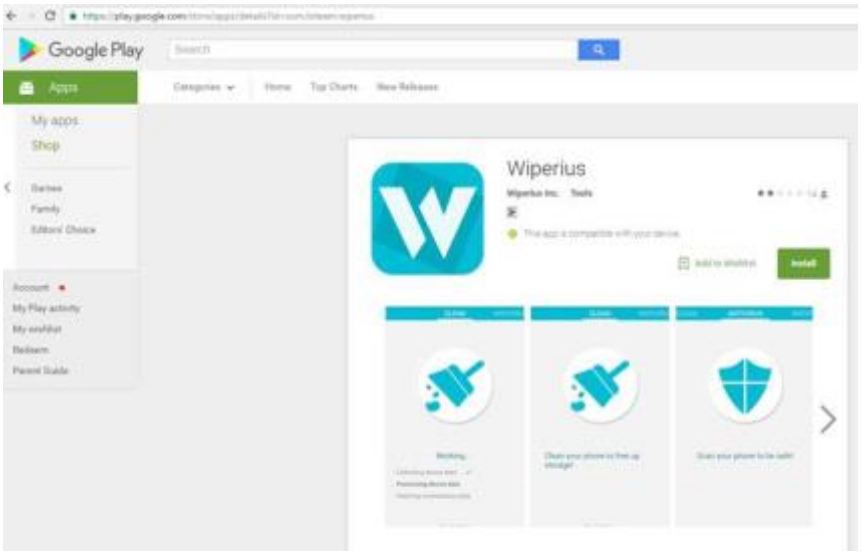
In Google Play in October and November, we detected about 50 new applications infected by Trojan.AndroidOS.Ztorg.am, the new modification of Trojan.AndroidOS.Ztorg.ad. According to installation statistics, many of them were installed more than 100,000 times.



Trojan.AndroidOS.Ztorg.ad imitating a video player

Google Play was used to spread Trojans capable of stealing login credentials. One of them was Trojan-Spy.AndroidOS.Instealy.a which stole logins and passwords for Instagram accounts. Another was Trojan-PSW.AndroidOS.MyVk.a: it was repeatedly published in Google Play and targeted user data from the social networking site VKontakte.

Yet another example is Trojan-Ransom.AndroidOS.Pletor.d, distributed by cybercriminals under the guise of an app for cleaning operating systems. Usually, representatives of the Trojan-Ransom.AndroidOS.Pletor family encrypt files on the victim device, but the detected modification only blocked the gadget and demanded a ransom to unblock it.



Trojan-Ransom.AndroidOS.Pletor.d imitating a system cleaner

Bypassing Android's protection mechanisms

Cybercriminals are constantly looking for ways to bypass Android's new protection mechanisms. For instance, in early 2016, we found that some modifications of the Tiny SMS Trojan were able to use their own window to overlay a system message warning users about sending a text message to a premium rate number. As the owner of the smartphone cannot see the original text, they are unaware of what they are agreeing to, and send the message to the number specified by the attacker.

A similar method was used by Trojan-Banker.AndroidOS.Asacub to get administrator rights on the device. The Trojan hides the system request from the user, cheating the latter into granting it extra privileges. In addition, Asacub asks for the right to be the default SMS application, which allows it to steal messages even in newer versions of Android.

The authors of Trojan-Banker.AndroidOS.Gugi went even further. This malicious program is able to bypass two new Android 6 security mechanisms using only social engineering techniques. Without exploiting system vulnerabilities, Gugi bypasses the request for Android's permission to display its window on top of other applications as well as the dynamic permission requirement for potentially dangerous actions.

Mobile ransomware

While the very first mobile encryptor Trojan really did encrypt user data on a device and demand money to decrypt them, current ransomware simply displays the ransom demand on top of other windows (including system windows), thus making it impossible to use the device.

The same principle was used by the most popular mobile ransom program in 2016 – Trojan-Ransom.AndroidOS.Fusob. Interestingly, this Trojan attacks users in Germany, the US and the UK, but avoids users from the CIS and some neighboring countries (once executed, it runs a check of the device language, after which it may stop working). The cybercriminals behind the Trojan usually demand between $100 and $200 to unblock a device. The ransom has to be paid using codes from pre-paid iTunes cards.

Yet another way to block devices is to use the Trojan-Ransom.AndroidOS.Congur family, which is popular in China. These Trojans change the PIN code for the gadget, or enable this safety function by setting their own PIN. To do this, the ransom program has to get administrator rights. The victim is told to contact the attackers via the QQ messenger to unblock the device.

Mobile banking Trojans continued to evolve through the year. Many of them gained tools to bypass the new Android security mechanisms and were able to continue stealing user information from the most recent versions of the OS. Also, the developers of mobile banking Trojans added more and more new features to their creations. For example, the Marcher family redirected users from financial to phishing sites over a period of several months.

In addition, many mobile banking Trojans include functionality for extorting money: upon receiving a command from a server, they can block the operation of a device with a ransom-demand window. We discovered that one modification of Trojan-Banker.AndroidOS.Faketoken could not only overlay the system interface but also encrypt user data.

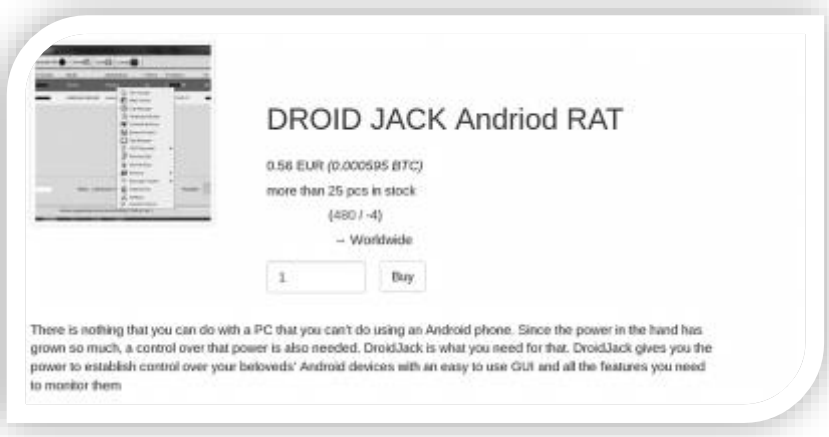
It is also worth noting that the cybercriminals behind malicious programs for Android did not forget about one of the hottest topics of 2016 – IoT devices. In particular, we discovered the 'attack-the-router' Trojan Switcher which targets the Wi-Fi network an infected device is connected to. If the Trojan manages to guess the password to the router, it changes the DNS settings, implementing a DNS-hijacking attack.

A glance into the Dark Web. *Contribution from INTERPOL's Global Complex for Innovation.*

The Dark Web provides a means for criminal actors to communicate and engage in commercial transactions, like buying and selling various products and services, including mobile malware kits. Vendors and buyers increasingly take advantage of the multiple security and business-oriented mechanisms put in place on Tor (The Onion Router) cryptomarkets, such as the use of cryptocurrencies, third-party administration services (escrow), multisignature transactions, encryption, reputation/feedback tracking and others. INTERPOL has looked into major Dark Web platforms and found that mobile malware is offered for sale as software packages (e.g. remote access trojans - RATs); individual solutions; sophisticated tools, like those developed by professional firms; or, on a smaller scale, as part of a 'Bot as a Service' model. Mobile malware is also a 'subject of interest' on vendor shops, forums and social media.

Marketplaces

A number of mobile malware products and services are offered for sale on Dark Web marketplaces. Mobile malware is often advertised as part of a package, which can include, for instance, remote access trojans (RATs), phishing pages, or 'hacking' software bundles which consist of forensic and password-breaking tools. Individual/one piece tools are also offered for sale. For example, *DroidJack* was offered by different vendors on four major marketplaces. This popular Android RAT is sold openly on the Clearnet for a high price, but on the Dark Web the price is much lower.



Both variants (package and individual) sometimes come with 'how-to' guides which explain the methods for hacking popular operating systems, such as Android and iOS. More sophisticated tools are also advertised on the Dark Web, such as *Galileo*, a remote control system developed by the Italian IT company Hacking Team in order to access remotely and then exploit devices that run Android, iOS, BlackBerry, Windows or OS X. Another example is the source code for Acecard. This malware is known for adding overlay screens on top of mobile banking applications and then forwarding the user's login credentials to a remote attacker. It can also access SMS, from which potentially useful two-factor authentication codes can be obtained by fraudsters.

The *Android bot rent service* (BaaS, or Bot as a Service) is also available for purchase. The bot can be used to gather financial information from Android phones and comes with many features and documentation, available in both Russian and English. More features and specifications can be developed on request. This service can cost up to USD 2,500 per month or USD 650 per week.

Mobile phishing products for obtaining financial information, tools that can control phones through Bluetooth or change their IMEI (International Mobile Equipment Identity), and various Android RATs that focus on intercepting text messages, call logs and locations, and accessing the device's camera, are also displayed on Dark Web marketplaces.

Vendor shops, forums and social media

Vendor shops are standalone platforms created by a single or group of vendors who have built up a customer base on a marketplace and then decided to start their own business. Generally, these shops do not have forums and merely advertise one specific type of illicit item, such as drugs or stolen personal information, but they also sell mobile malware (*DroidJack*). Tutorials are sometimes attached to mobile malware products, and information on which tools are fit for purpose and how to install and utilize them can also be found in forum threads and on social media. Furthermore, a Tor hidden service focused on hacking news was found to contain information on how to set up *Dendroid* (Figure 1) mobile malware. This RAT, which is capable of intercepting SMS messages, downloading pictures and opening a dialogue box to phish passwords, dates from 2014 but was still offered in 2016 as part of several advertisements (packages) on different marketplaces.

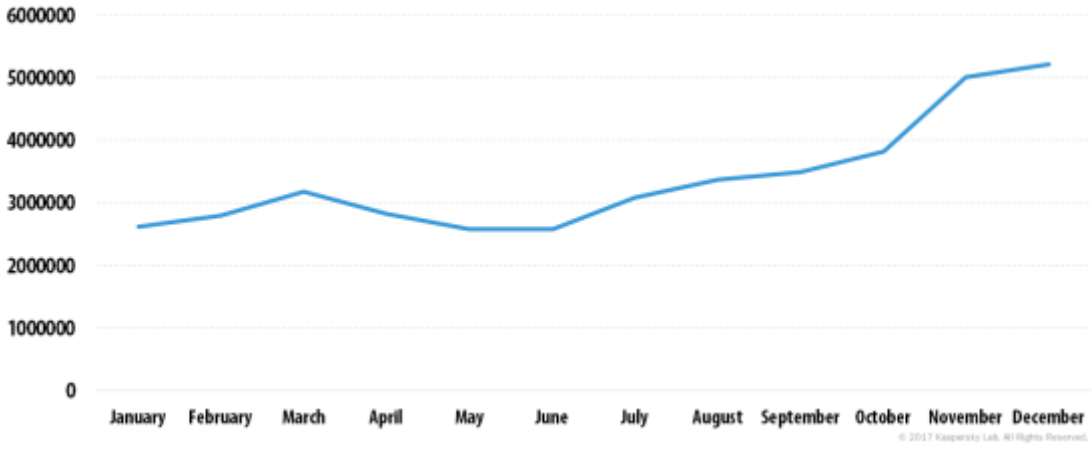
Figure 1

Due to its robust anonymity, OPSEC techniques, low prices and client-oriented strategy, the Dark Web remains an attractive medium for conducting illicit businesses and activities, and one where specific crime areas may arise or grow in the future. The development of innovative technical solutions (in close cooperation with academia, research institutes and private industry), international cooperation and capacity building are fundamental pillars in the fight against the use of Dark Web by criminals.

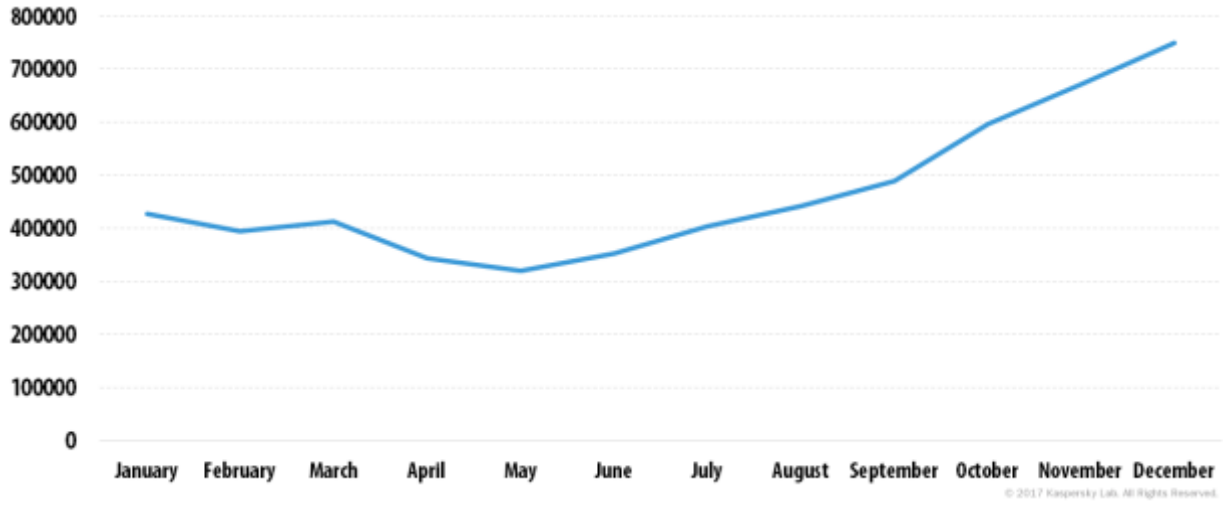
Statistics

In 2016, the number of malicious installation packages grew considerably, amounting to 8,526,221 – three times more than the previous year. As a comparison, from 2004 to 2013 we detected over 10,000,000 malicious installation packages; in 2014 the figure was nearly 2.5 million.

From the beginning of January till the end of December 2016, Kaspersky Lab registered nearly 40 million attacks by malicious mobile software and protected 4,018,234 unique users of Android-based devices (vs 2.6 million in 2015).



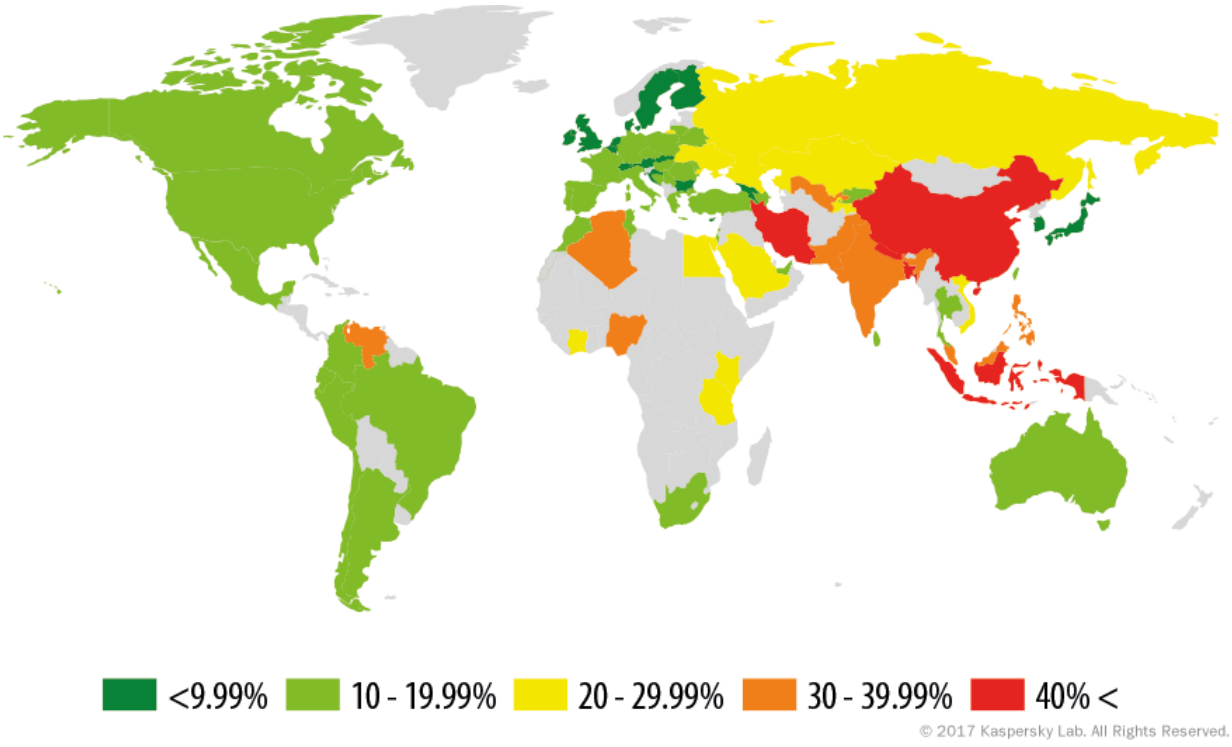
The number of attacks blocked by Kaspersky Lab solutions, 2016



The number of users protected by Kaspersky Lab solutions, 2016

Geography of mobile threats

Attacks by malicious mobile software were recorded in more than 230 countries and territories.



The geography of mobile threats by number of attacked users, 2016

TOP 10 countries by the percentage of users attacked by mobile malware

	Country*	%**
1	Bangladesh	50.09%
2	Iran	46.87%
3	Nepal	43.21%
4	China	41.85%
5	Indonesia	40.36%
6	Algeria	36.62%
7	Nigeria	35.61%
8	Philippines	34.97%
9	India	34.18%
10	Uzbekistan	31.96%

** We excluded those countries in which the number of users of Kaspersky Lab mobile security products over the reported period was less than 25,000.*
*** The percentage of attacked unique users as a percentage of all users of Kaspersky Lab's mobile security products in the country.*

China, which topped this rating in 2015, continued to lead the way in the first half of 2016 but dropped to fourth overall for the year, being replaced by Bangladesh, which led similar ratings throughout 2016. More than half of all users of Kaspersky Lab mobile security products in Bangladesh encountered mobile malware.

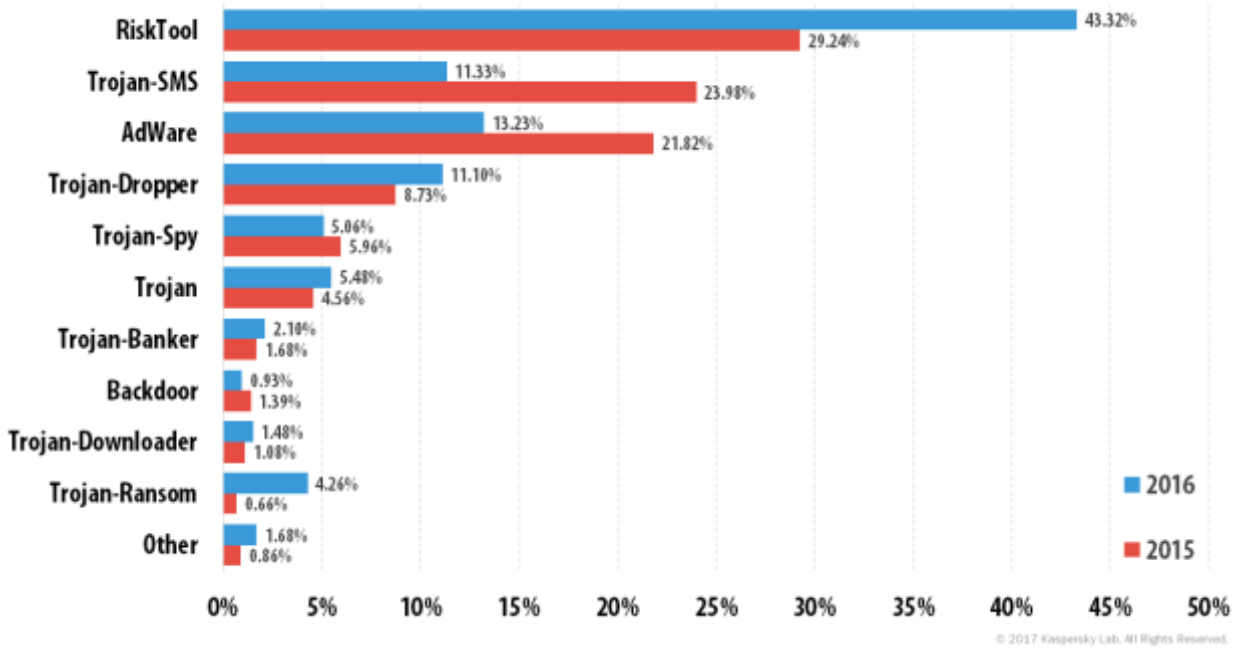
The most widespread mobile malware targeting users in Bangladesh in 2016 were representatives of advertising Trojans belonging to the Ztorg and Iop families, as well as advertising programs of the Sprovider family. This malware, as well as representatives of the AdWare.AndroidOS.Ewind and AdWare.AndroidOS.Sprovider families were most frequently found on user devices in all the countries in the Top 10, except China and Uzbekistan.

In China, a significant proportion of the attacks involved the Backdoor.AndroidOS.Fakengry.h and Backdoor.AndroidOS.GinMaster.a families as well as representatives of RiskTool.AndroidOS.

Most of the attacks on users in Uzbekistan were carried out by Trojan-SMS.AndroidOS.Podec.a and Trojan-FakeAV.AndroidOS.Mazig.b. Representatives of the advertising Trojans Iop and Ztorg, as well as the advertising programs of the Sprovider family were also quite popular in the country.

Types of mobile malware

*Starting this year, we calculate the distribution of mobile software by type, based on the **number of detected installation packages, rather than modifications**.*



Distribution of new mobile malware by type in 2015 and 2016

Over the reporting period, the number of new RiskTool files detected grew significantly – from 29% in 2015 to 43% in 2016. At the same time, the share of new AdWare files fell – 13% vs 21% in the previous year.

For the second year running, the percentage of detected SMS Trojan installation packages continued to decline – from 24% to 11%, which was the most notable fall. Despite this, we cannot say that the SMS Trojan threat is no longer relevant; in 2016, we detected nearly 700,000 new installation packages.

The most considerable growth was shown by Trojan-Ransom: the share of this type of malware among all installation packages detected in 2016 increased almost 6.5 times to 4%. This growth was caused by the active distribution of two families of mobile ransomware – Trojan-Ransom.AndroidOS.Fusob and Trojan-Ransom.AndroidOS.Congur.

Top 20 malicious mobile programs

Please note that the ranking of malicious programs below does not include potentially unwanted programs such as RiskTool or AdWare (advertising programs).

	Detection	%*
1	DangerousObject.Multi.Generic	67.93%
2	Backdoor.AndroidOS.Ztorg.c	6.58%
3	Trojan-Banker.AndroidOS.Svpeng.q	5.42%
4	Trojan.AndroidOS.Iop.c	5.25%
5	Backdoor.AndroidOS.Ztorg.a	4.83%
6	Trojan.AndroidOS.Agent.gm	3.44%
7	Trojan.AndroidOS.Ztorg.t	3.21%
8	Trojan.AndroidOS.Hiddad.v	3.13%
9	Trojan.AndroidOS.Ztorg.a	3.11%
10	Trojan.AndroidOS.Boogr.gsh	2.51%
11	Trojan.AndroidOS.Muetan.b	2.40%
12	Trojan-Ransom.AndroidOS.Fusob.pac	2.38%
13	Trojan-Ransom.AndroidOS.Fusob.h	2.35%
14	Trojan.AndroidOS.Sivu.c	2.26%
15	Trojan.AndroidOS.Ztorg.ag	2.23%
16	Trojan.AndroidOS.Ztorg.aa	2.16%
17	Trojan.AndroidOS.Hiddad.an	2.12%
18	Trojan.AndroidOS.Ztorg.i	1.95%
19	Trojan-Dropper.AndroidOS.Agent.cv	1.85%
20	Trojan-Dropper.AndroidOS.Triada.d	1.78%

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

First place in the Top 20 is occupied by DangerousObject.Multi.Generic (67.93%), used in malicious programs detected by cloud technologies. Cloud technologies work when the antivirus database contains neither the signatures nor heuristics to detect a malicious program. This is basically how the very latest malware is detected.

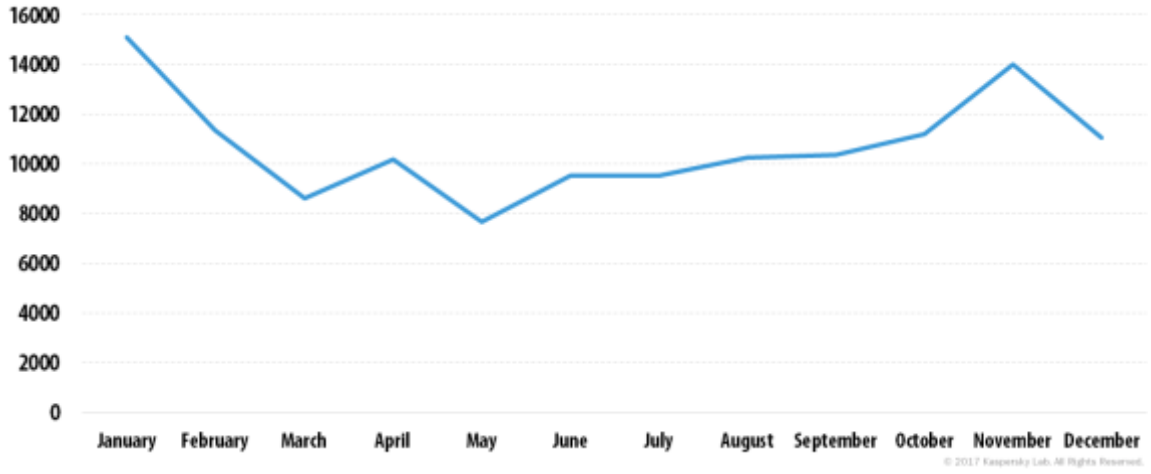
In second place was Backdoor.AndroidOS.Ztorg.c, the advertising Trojan using super-user rights to secretly install various applications. Noticeably, the 2016 rating included 16 advertising Trojans (highlighted in blue in the table), which is four more than in 2015.

The most popular mobile banking Trojan in 2016 was Trojan-Banker.AndroidOS.Svpeng.q in third place. The Trojan became so widespread after being distributing via the AdSense advertising network. Due to a vulnerability in the Chrome browser, the user was not required to take any action to download the Trojan on the device. It should be noted that more than half of the users attacked by mobile banking Trojans in 2016 encountered representatives of the Svpeng family. They use phishing windows to steal credit card data and also attack SMS banking systems.

Representatives of the Fusob family – Trojan-Ransom.AndroidOS.Fusob.pac and Trojan-Ransom.AndroidOS.Fusob.h – claimed 12th and 13th respectively. These Trojans block a device by displaying their own window and demanding a ransom to remove it.

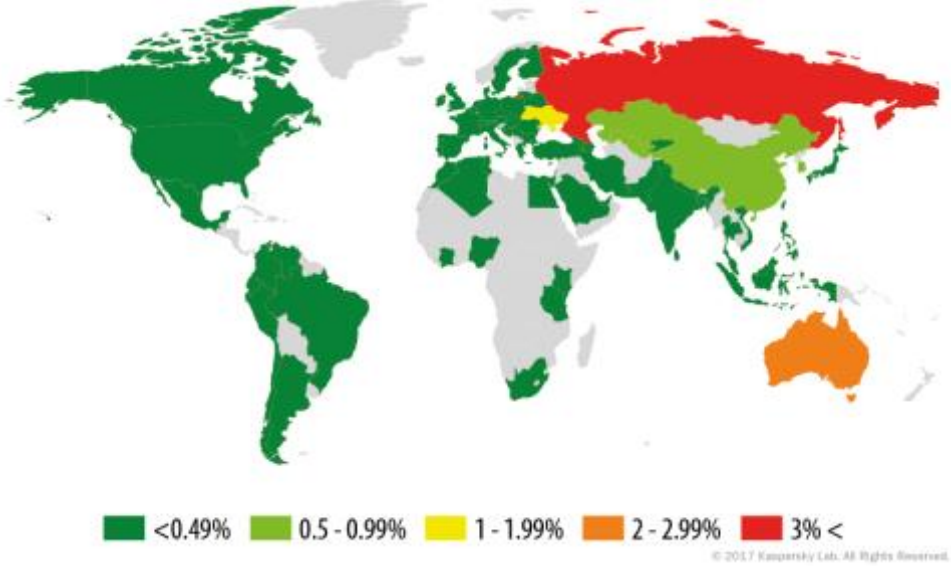
Mobile banking Trojans

In 2016, we detected 128,886 installation packages of mobile banking Trojans, which is 1.6 times more than in 2015.



Number of installation packages of mobile banking Trojans detected by Kaspersky Lab solutions in 2016

In 2016, 305,543 users in 164 countries were attacked by mobile banking Trojans vs 56,194 users in 137 countries the previous year.



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

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

	Country*	%**
1	Russia	4.01
2	Australia	2.26
3	Ukraine	1.05
4	Uzbekistan	0.70
5	Tajikistan	0.65
6	The Republic of Korea	0.59
7	Kazakhstan	0.57
8	China	0.54
9	Belarus	0.47
10	Moldova	0.39

** We excluded those countries in which the number of users of Kaspersky Lab mobile security products over the reported period was less than 25,000.*
*** Percentage of unique users attacked by mobile banking Trojans, relative to all users of Kaspersky Lab's mobile security products in the country.*

In Russia – ranked first in the Top 10 – mobile banking Trojans were encountered by 4% of mobile users. This is almost two times higher than in second-placed Australia. The difference is easily explained by the fact that the most popular mobile banking Trojan Svpeng was mostly spread in Russia. Representatives of the Asacub and Faketoken families were also popular there.

In Australia, the Trojan-Banker.AndroidOS.Acecard and Trojan-Banker.AndroidOS.Marcher families were responsible for most infection attempts. In South Korea (7th place) the most popular banking Trojans belonged to the Trojan-Banker.AndroidOS.Wroba family.

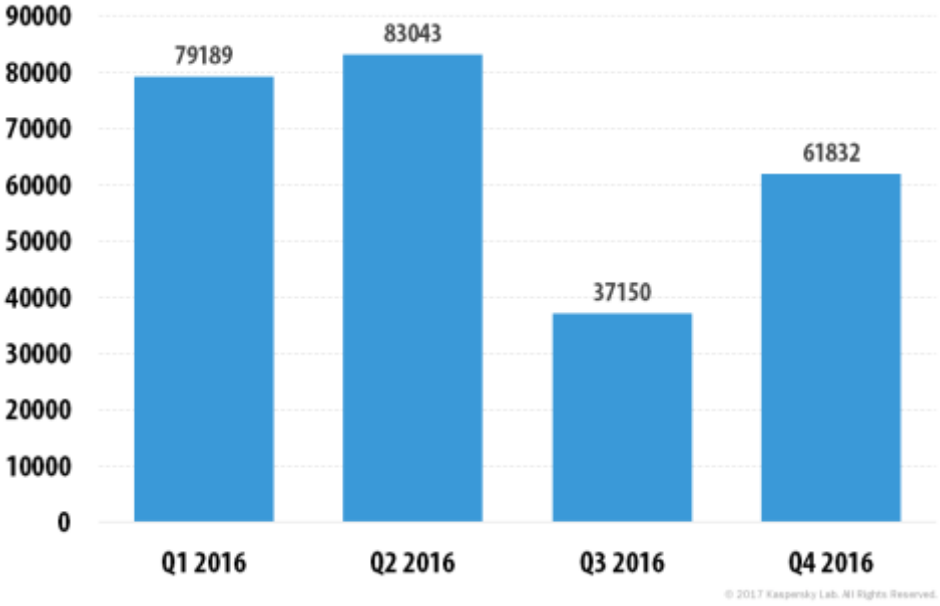
In the other countries of the Top 10, the most actively distributed mobile banking Trojan families were Trojan-Banker.AndroidOS.Faketoken and Trojan-Banker.AndroidOS.Svpeng. The representatives of the latter were especially widespread in 2016, with more than half of mobile users encountering them. As we have already mentioned, this was the result of them being distributed via the AdSense advertising network and being loaded stealthily via a mobile browser vulnerability.

The Trojan-Banker.AndroidOS.Faketoken family was in second place in this rating. Some of its modifications were capable of attacking more than 2,000 financial organizations.

Third place was occupied by the Trojan-Banker.AndroidOS.Asacub family, which attacked more than 16% of all users affected by mobile bankers. These Trojans are mainly distributed in Russia, often via SMS spam.

Mobile Trojan-Ransom

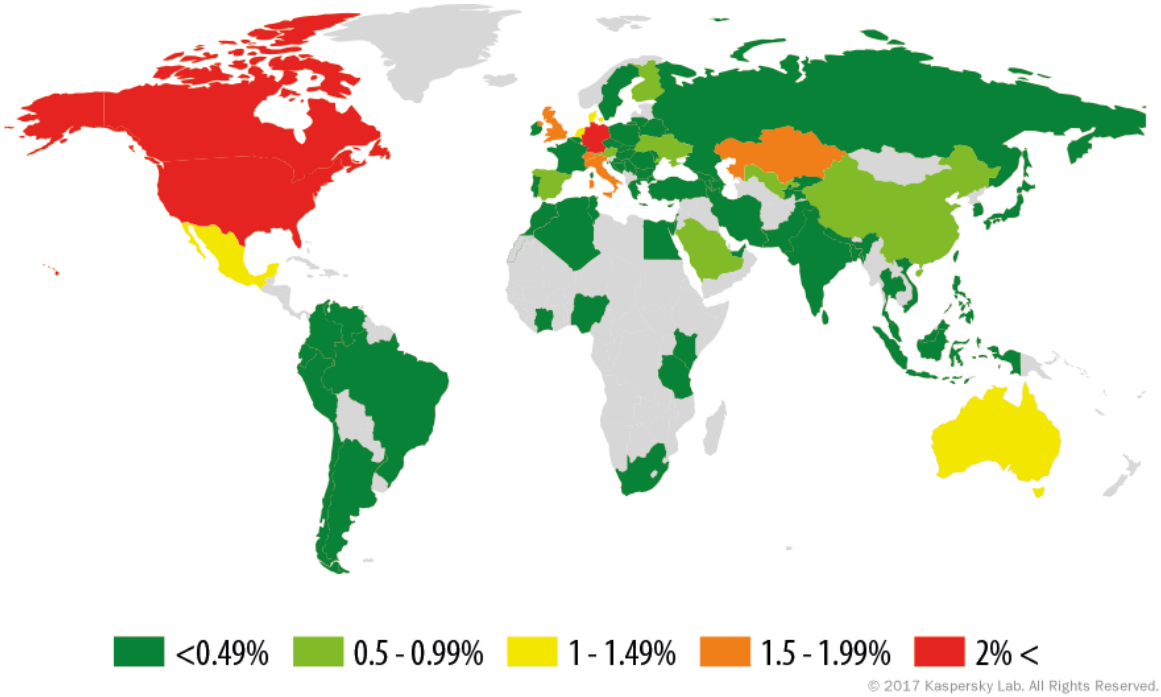
In 2016, the volume of mobile ransomware increased considerably both in the number of installation packages detected and in the number of users attacked. Over the reporting period, we detected 261,214 installation packages, which is almost 8.5 times more than in 2015.



Number of mobile Trojan-Ransomware installation packages detected by Kaspersky Lab (Q1 2016 – Q4 2016)

In 2016, 153,258 unique users from 167 countries were attacked by Trojan-Ransom programs; this is 1.6 times more than in 2015.

Interestingly, a large number of installation packages in the first two quarters of 2016 belonged to the Trojan-Ransom.AndroidOS.Fusob family, though there was a fall in activity in the third quarter. The subsequent growth in the fourth quarter was fueled by an increase in activity by the Trojan-Ransom.AndroidOS.Congur family: it includes relatively simple Trojans that either block a device using their own window, or change the device's password.



Geography of mobile ransomware threats in 2016 (number of users attacked)

TOP 10 countries attacked by Trojan-Ransom malware – share of users relative to all attacked users in the country.

	Country*	%**
1	Germany	2.54
2	USA	2.42
3	Canada	2.34
4	Switzerland	1.88
5	Kazakhstan	1.81
6	United Kingdom	1.75
7	Italy	1.63
8	Denmark	1.29
9	Mexico	1.18
10	Australia	1.13

** We excluded those countries in which the number of users of Kaspersky Lab mobile security products over the reported period was less than 25,000.*
*** Percentage of unique users attacked by mobile Trojan ransomware, relative to all users of Kaspersky Lab's mobile security products in the country.*

The largest percent of mobile users attacked by ransomware was in Germany – over 2.5%. In almost all the countries in this ranking, representatives of the Trojan-Ransom.AndroidOS.Fusob and Trojan-Ransom.AndroidOS.Svpeng families were particularly popular. Kazakhstan (5th place) was the only

exception – the most frequently used ransom programs there were various modifications of the Trojan-Ransom.AndroidOS.Small family.

More information about these three families of mobile Trojan ransomware can be found in a dedicated study.

Conclusion

In 2016, the growth in the number of advertising Trojans capable of exploiting super-user rights continued. Throughout the year it was the No. 1 threat, and we see no sign of this trend changing. Cybercriminals are taking advantage of the fact that most devices do not receive OS updates (or receive them late), and are thus vulnerable to old, well-known and readily available exploits.

This year, we will continue to closely monitor the development of mobile banking Trojans: the developers of this class of malware are the first to use new technologies and are always looking for ways to bypass security mechanisms implemented in the latest versions of mobile operating systems.

In 2016, one of the most controversial issues was the safety of IoT devices. Various Internet-connected 'smart' devices are becoming increasingly popular, though their level of security is fairly low. Also in 2016, we discovered an 'attack-the-router' Trojan. We see that the mobile landscape is getting a little crowded for cybercriminals, and they are beginning to interact more with the world beyond smartphones. Perhaps in 2017 we will see major attacks on IoT components launched from mobile devices.