Mobile Malware Evolution: 2013

By Victor Chebyshev

Published: 2014-02-24 · Archived: 2026-04-05 15:00:50 UTC

The mobile malware sector is growing rapidly both technologically and structurally. It is safe to say that today's cybercriminal is no longer a lone hacker but part of a serious business operation.

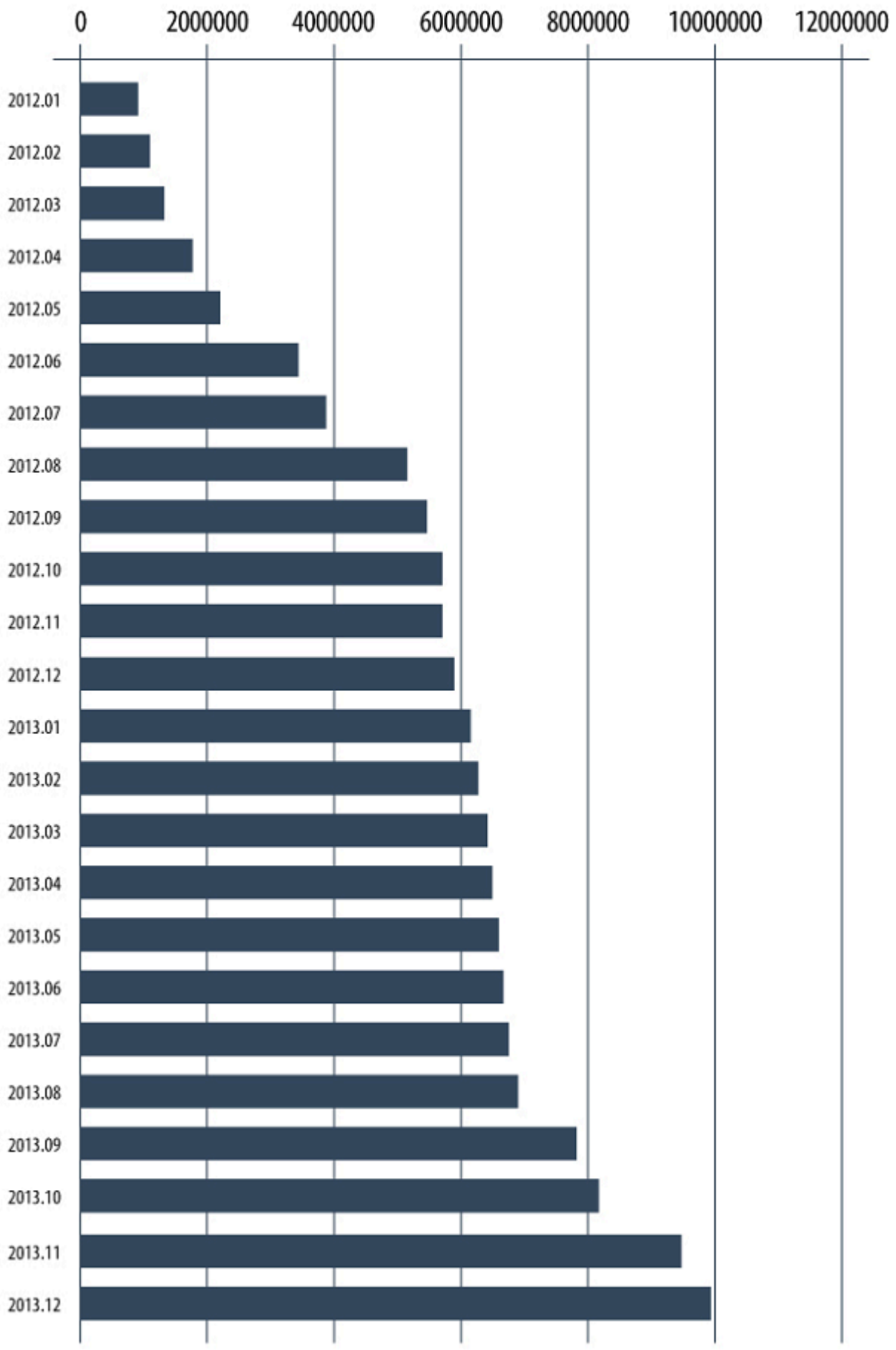
There are various types of actors involved in the mobile malware industry: virus writers, testers, interface designers of both the malicious apps and the web pages they are distributed from, owners of the partner programs that spread the malware, and mobile botnet owners.

This division of labor among the cybercriminals can also be seen in the behavior of their Trojans. In 2013, there was evidence of cooperation (most probably on a commercial basis) between different groups of virus writers. For example, the botnet Trojan-SMS.AndroidOS.Opfake.a, in addition to its own activity, also spread Backdoor.AndroidOS.Obad.a by sending spam containing a link to the malware to the victim's list of contacts.

It is now clear that a distinct industry has developed and is becoming more focused on extracting profits, which is clearly evident from the functionality of the malware.

2013 in figures

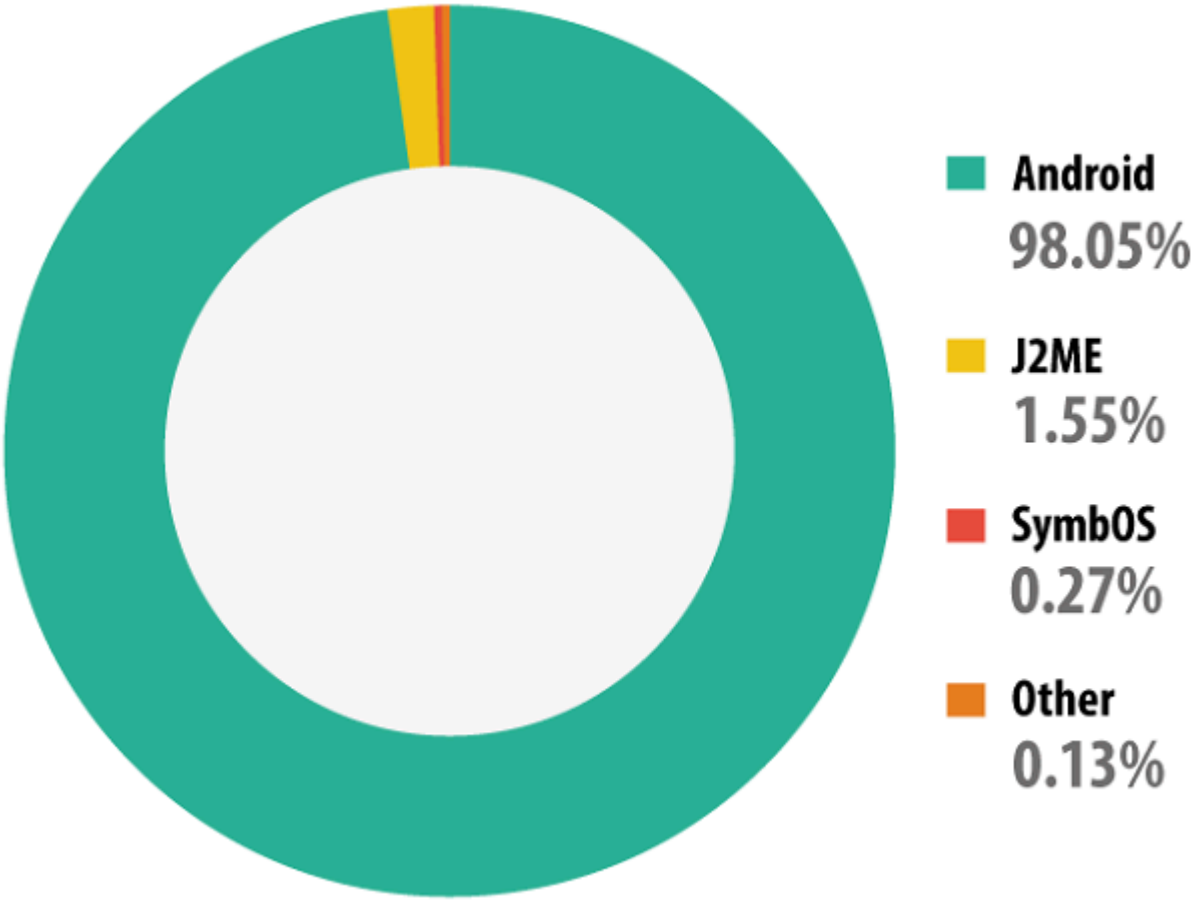
- A total of 143,211 new modifications of malicious programs targeting mobile devices were detected in all of 2013 (as of January 1, 2014).
- In 2013, 3,905,502 installation packages were used by cybercriminals to distribute mobile malware. Overall in 2012-2013 we detected approximately 10,000,000 unique malicious installation packages:


0
2000000
4000000
6000000
8000000
10000000
12000000
2012.01
2012.02
2012.03
2012.04
2012.05
2012.06
2012.07
2012.08
2012.09
2012.10
2012.11
2012.12
2013.01
2013.02
2013.03
2013.04
2013.05
2013.06
2013.07
2013.08
2013.09
2013.10
2013.11
2013.12

The number of installation packages detected in 2012-2013

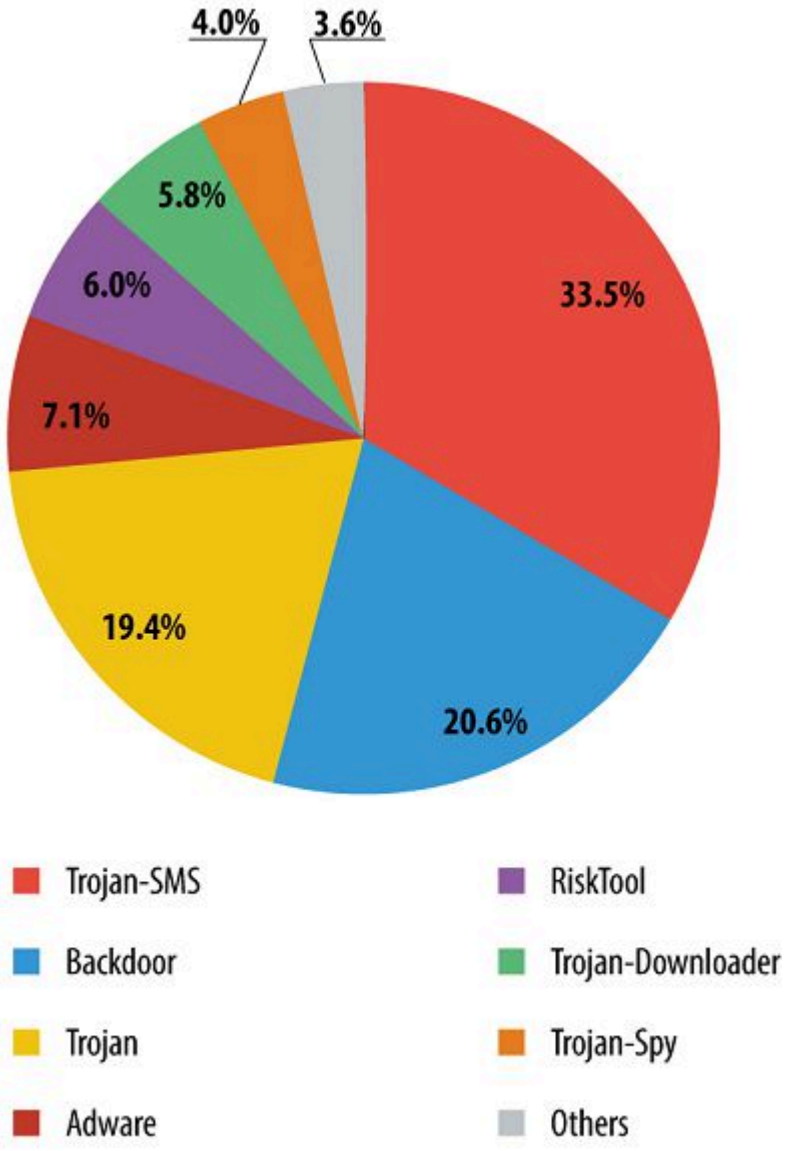
Different installation packages can install programs with the same functionality that differ only in terms of the malicious app interface and, for instance, the content of the text messages it spreads.

- Android remains a prime target for malicious attacks. 98.05% of all malware detected in 2013 targeted this platform, confirming both the popularity of this mobile OS and the vulnerability of its architecture.



The distribution of mobile malware detected in 2013 by platform

- Most mobile malware is designed to steal users' money, including SMS-Trojans, and lots of backdoors and Trojans.



The distribution of mobile malware by category

- Over the year, the number of mobile malware modifications designed for phishing, the theft of credit card information and money increased by a factor of 19.7. In 2013, Kaspersky Lab mobile products prevented 2,500 infections by banking Trojans.

Methods and techniques

2013 not only saw a radical increase in output from mobile virus writers but also saw them actively applying methods and technologies that allowed cybercriminals to use their malware more effectively. There were several distinct areas where mobile malware underwent advances.

Distribution

Cybercriminals made use of some exceptionally sophisticated methods to infect mobile devices.

Infecting legal web resources help spread mobile malware via popular websites. More and more smartphone and tablet owners use their devices to access websites, unaware that even the most reputable resources can be hacked. According to our data, 0.4% of the websites visited by users of our products were compromised sites.

Distribution via alternative app stores. In Asia there are numerous companies producing Android-based devices and Android apps, and many of them offer users their own app stores containing programs that cannot be found in Google Play. The purely nominal control over the applications uploaded to these stores means attackers can conceal Trojans in apps made to look like innocent games or utilities.

Distribution via botnets. As a rule, bots self-proliferate by sending out text messages with a malicious link to addresses in the victim's address book. We also registered one episode of mobile malware spreading via a third-party botnet.

Resistance to anti-malware protection

The ability of malicious software to operate continuously on the victim's mobile device is an important aspect of its development. The longer a Trojan "lives" on a smartphone, the more money it will make for the owner. This is an area where virus writers are actively working, resulting in a large number of technological innovations.

Criminals are increasingly using **obfuscation**, the deliberate act of creating complex code to make it difficult to analyze. The more complex the obfuscation, the longer it will take an antivirus solution to neutralize the malicious code. Tellingly, current virus writers have mastered commercial obfuscators. This implies they have made considerable investments. For example, one commercial obfuscator, which cost €350, was used for Trojans and Opfak.bo Obad.a

Android vulnerabilities are used by criminals for three reasons: to bypass the code integrity check when installing an application (vulnerability Master Key); to enhance the rights of malicious applications, considerably extending their capabilities; and to make it more difficult to remove malware. For example, Svpeng uses a previously unknown vulnerability to protect itself from being removed manually or by the antivirus program.

Cybercriminals also exploit the Master Key vulnerability and have learned to embed unsigned executable files in Android installation packages. Digital signature verification can be bypassed by giving the malicious file exactly the same name as a legitimate file and placing it on the same level in the archive. The system verifies the signature of the legitimate file while installing the malicious file.

Unfortunately, there is a specific feature of Android vulnerabilities that means it is only possible to get rid of them by receiving an update from the device manufacturers. However, many users are in no hurry to update the operating systems of their products. If a smartphone or tablet was released more than a year ago, it is probably no longer supported by the manufacturer and patching of vulnerabilities is no longer provided. In that case, the only help comes from an antivirus solution, for example, Kaspersky Internet Security for Android.

Embedding malicious code in legitimate programs helps conceal infections from the victim. Of course, this does not mean the digital signature of the software developer can be used. However, due to the absence of certification centers verifying the digital signatures of Android programs, nothing prevents criminals from adding

their own signature. As a result, a copy of Angry Birds installed from an unofficial app store or downloaded from a forum could easily contain malicious functionality.

Capabilities and functionality

In 2013, we detected several technological innovations developed and used by criminals in their malicious software. Below are descriptions of some of the most interesting.

Control of malware from a single center provides maximum flexibility. Botnets can make considerably more money than autonomous Trojans. It comes as no surprise then that many SMS-Trojans include bot functionality. According to our estimates, about 60% of mobile malware are elements of both large and small mobile botnets.

By using Google Cloud Messaging botnet owners can operate without a C&C server, thus eliminating the threat of the botnet being detected and blocked by law enforcement authorities. Google Cloud Messaging is designed to send short message (up to 4 KB) to mobile devices via Google services. The developer simply has to register and receive a unique ID for his applications. The commands received via GCM cannot be blocked immediately on an infected device.

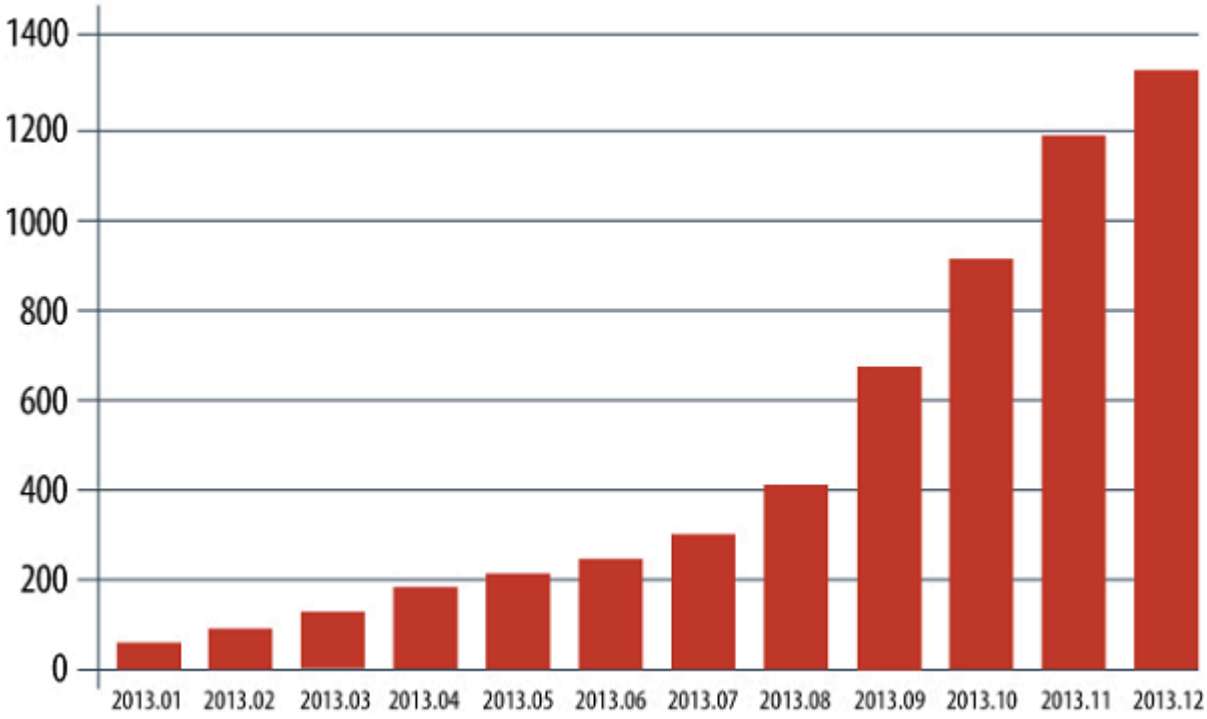
We have detected several malicious programs using GCM for command and control – the widespread Trojan-SMS.AndroidOS.FakeInst.a, Trojan-SMS.AndroidOS.Agent.ao, and Trojan-SMS.AndroidOS.OpFake.a among others. Google is actively combating this use of the service, responding quickly to reports from antivirus companies and blocking the IDs of cybercriminals.

Attacks on Windows XP allows mobile malware to infect a PC after connecting a smartphone or tablet. In early 2013 we detected two identical applications on Google Play that were allegedly designed for cleaning the operating system of Android-based devices from unnecessary processes. In fact, the applications are designed to download the autorun.inf file, an icon file and the win32-Trojan file, which the mobile malicious program locates in the root directory of an SD card. On connecting a smartphone in the USB drive emulation mode to a computer running Windows XP, the system automatically starts the Trojan (if AutoPlay on the external media is not disabled) and is infected. The Trojan allows the criminals to remotely control the victim's computer and is capable of recording sound from a microphone. We would like to emphasize that this method of attack only works on Windows XP and Android versions prior to 2.2.

The most advanced mobile malicious programs today are Trojans targeting users' bank accounts – the most attractive source of criminal earnings.

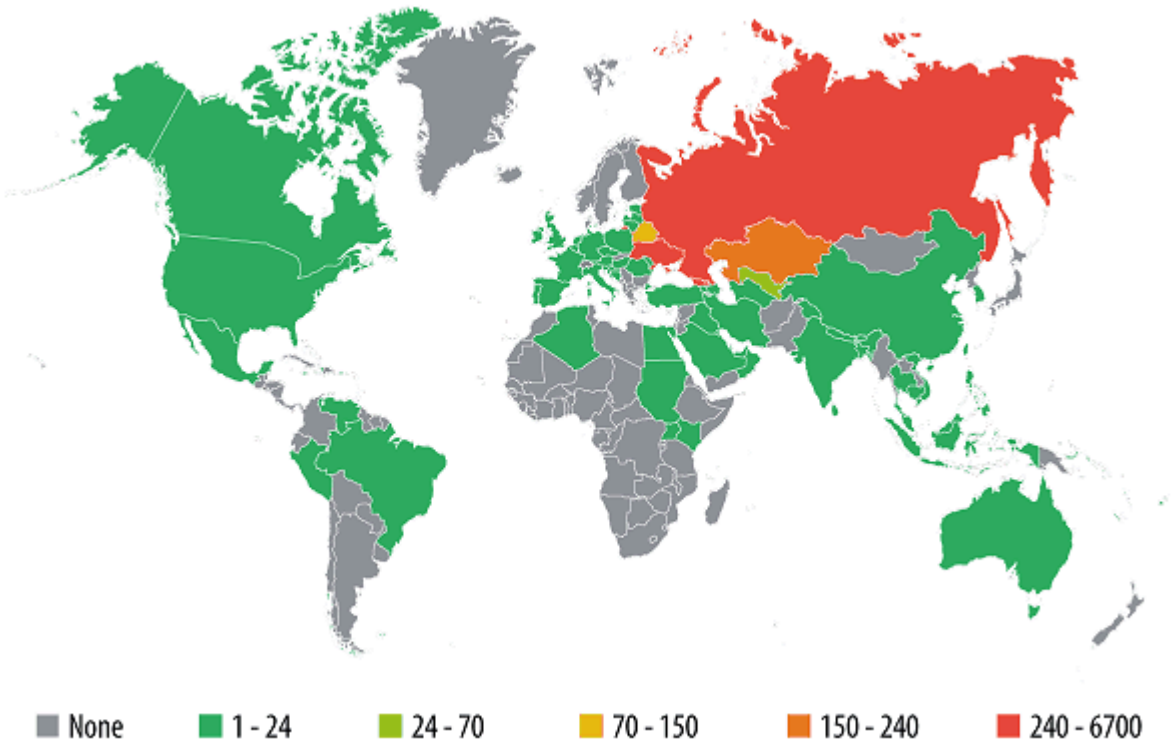
Trend of the year: mobile banking Trojans

2013 was marked by a rapid rise in the number of Android banking Trojans. The cyber industry of mobile malware is becoming more focused on making profits more effectively, i.e., mobile phishing, theft of credit card information, money transfers from bank cards to mobile phones and from phones to the criminalas' e-wallets. Cybercriminals have become obsessed by this method of illegal earnings: at the beginning of the year we knew only 67 banking Trojans, but by the end of the year there were already 1321 unique samples. Kaspersky Lab mobile products prevented 2,500 infections by banking Trojans.



The number of mobile banking Trojans in our collection

Mobile banking Trojans can run together with Win-32 Trojans to bypass the two-factor authentication – mTAN theft (the theft of banking verification codes that banks send their customers in SMS messages). However, in 2013, autonomous mobile banking Trojans developed further. Currently, such Trojans attack a limited number of bank customers, but it is expected that cybercriminals will invent new techniques that will allow them to expand the number and the geography of potential victims.



Infections caused by mobile banking programs

Today, the majority of banking Trojan attacks affect users in Russia and the CIS. However, this situation will not last long: given the cybercriminals' interest in user bank accounts, the activity of mobile banking Trojans is expected to grow in other countries in 2014.

As mentioned above, banking Trojans are perhaps the most complex of all mobile threats, and Svpeng is one of the most striking examples.

Svpeng

In mid-July, we detected Trojan-SMS.AndroidOS.Svpeng.a which, unlike its SMS Trojan counterparts, is focused on stealing money from the victiim's bank account rather than from his mobile phone. It cannot act independently and operates strictly in accordance with commands received from the C&C server. This malicious program spreads via SMS spam and from compromised legitimate sites that redirect mobile users to a malicious resource. There the user is prompted to download and install a Trojan imitating an Adobe Flash Player update.

Svpeng is capable of doing lots of things.

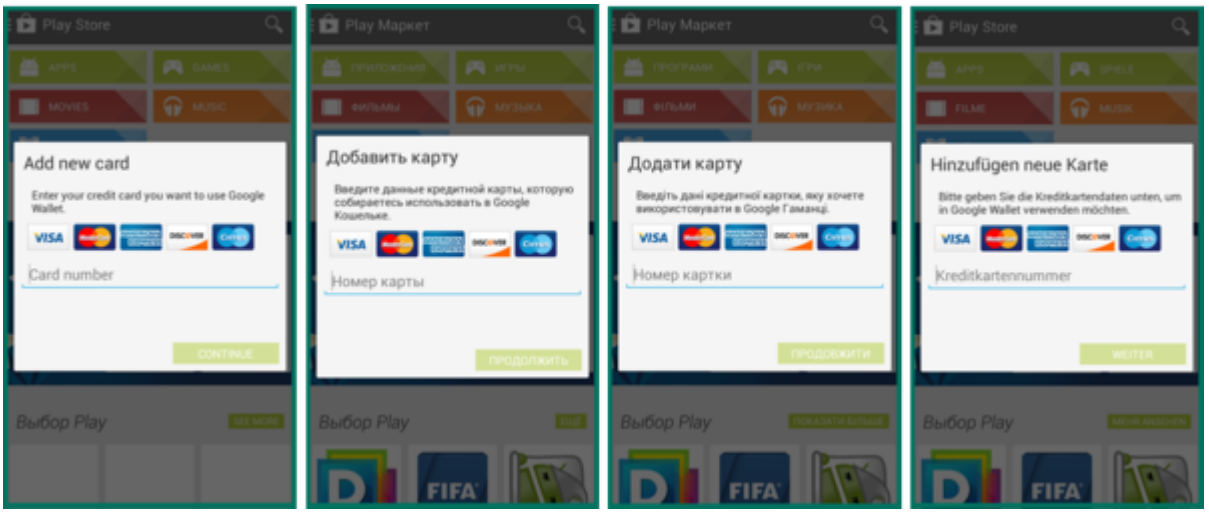
It collects information about the smartphone (IMEI, country, service provider, operating system language) and sends it to the host via the HTTP POST request. This appears to be necessary to determine the number of banks the victim may use. Svpeng is only currently attacking clients of Russian banks. Typically, however, cybercriminals first test-run a technology on the Russian sector of the Internet and then roll it out globally, attacking users in other countries.

It steals SMS messages and information about voice calls. It helps the attacker find out which banks the owner of the smartphone calls – the Trojan receives a list of bank phone numbers from its C&C server.

It steals money from the victim's bank account. In Russia, some major banks offer their clients a special service that allows them to transfer money from their bank card to their mobile phone account. Customers have to send a set text message from their phone to a specific bank number. Svpeng sends the corresponding messages to the SMS services of two banks. Svpeng does this to check if the cards from these banks are attached to the number of the infected phone and to find out the account balance. If the phone is attached to a bank card, commands are sent from the C&C server with instructions to transfer money from the user's bank account to his/her mobile account. The cybercriminals then send this money to a digital wallet or to a premium number and cash it in.

It steals logins and passwords to online banking accounts by substituting he window displayed by the bank application. Currently, this only affects Russian banks, but the technology behind Svpeng could easily be used to target other banking applications.

It steals bank card information (the number, the expiry date, CVC2/CVV2) imitating the process of registering the bank card with Google Play. If the user has launched Play Market, the Trojan intercepts the event and displays a window on top of the Google Play window, prompting the user to enter his/her bank card details in the fake window. The data entered by the user is sent to the cybercriminals.



It extorts money from users by threatening to block the smartphone: it displays a message demanding $500 to unblock the device. In actual fact, the Trojan does not block anything and the phone can be used without any problems.

It hides traces of its activity by masking the outgoing and incoming text messages and blocking calls and messages from numbers belonging to the bank. The Trojan gets the list of bank phone numbers from its C&C server.

It protects itself from deletion by requesting Device Administrator rights during the installation. As a result, the Trojan delete button in the list of applications becomes inactive, which may cause problems for inexperienced users. It is impossible to deprive it of these rights without the use of specialized tools (such as Kaspersky Internet

Security for Android). To protect itself from being removed, Svpeng uses a previously unknown vulnerability in Android. It uses the same trick to prevent the smartphone from being returned to its factory settings.

The Trojan is distributed in Russia and CIS countries. But, as we have already mentioned, the criminals could easily turn their attention to users in other countries.

Perkele and Wroba

Foreign users have also been on the receiving end of several malicious innovations targeting bank accounts.

The **Perkele** Android Trojan not only attacks Russian users but also clients of several European banks. It is of interest primarily because it operates in conjunction with various banking win32-Trojans. Its main task is to bypass the two-factor authentication of the client in the online banking system.

Due to the specific nature of its activity, Perkele is distributed in a rather unusual way. When a user enters an Internet banking site on a computer infected by banking malware (ZeuS, Citadel), a request about the smartphone number and type of operating system is injected into the code of the authentication page. This data is immediately sent to the cybercriminals and the computer displays the QR code containing a link to the alleged certificate of the online banking system. After scanning the QR code and installing a component downloaded from the link, the user infects his smartphone with the Trojan program that boasts functionality that is of great interest to the attackers.

Perkele intercepts mTANs (confirmation codes for banking operations) sent by the bank via text message. By using the login and password stolen from the browser, the Windows Trojan initiates a fake transaction while Perkele intercepts (via the C&C server) the mTAN sent by the bank to the user. Money then disappears from the victim’s account and is cashed in without the owner’s knowledge.

The Korean malware Wroba, in addition to the traditional vector of infection via file-sharing services, spreads via alternative app stores. Once it infects a device, Wroba behaves very aggressively. It searches for mobile banking applications, removes them and uploads counterfeit versions. From the outside, they are indistinguishable from the legitimate applications. However, they possess no banking functions, and merely steal the logins and passwords entered by users.

TOP 10 mobile threats detected in 2013

	Name*	% of all attacks
1	DangerousObject.Multi.Generic	40.42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3	AdWare.AndroidOS.Ganlet.a	12.40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5	RiskTool.AndroidOS.SMSreg.cw	8.80%
6	Trojan-SMS.AndroidOS.Agent.u	8.03%

7	Trojan-SMS.AndroidOS.OpFake.a	5.49%
8	Trojan.AndroidOS.Plangton.a	5.37%
9	Trojan.AndroidOS.MTK.a	4.25%
10	AdWare.AndroidOS.Hamob.a	3.39%

1. DangerousObject.Multi.Generic. This verdict means that we are aware of an application's malicious character, but for one reason or another have not provided our users with signatures to detect it. In such cases, detection is available through cloud technologies implemented by the company in the Kaspersky Security Network, which enable our products to minimize the time it takes to respond to new and unknown threats.

2. Trojan- SMS.AnroidOS.OpFake.bo This is one of the most sophisticated SMS Trojans. Its distinguishing features are a well-designed interface and the greed of its developers. When launched, it steals money from the mobile device's owner – from $9 to the entire amount in the user's account. There is also the risk of the user's telephone number being discredited, since the Trojan can collect numbers from the contact list and send SMS messages to all of those numbers. The malware targets primarily Russian-speakers and users in CIS countries.

3. AdWare.AndroidOS.Ganlet.a. An advertising module that possesses the functionality necessary to install other applications.

4. Trojan-SMS.AndroidOSFakeInst.a. This malware has evolved over the past few years from a simple SMS Trojan to a fully functional bot controlled via various channels (including Google Cloud Messaging). The Trojan can steal money from a user's account and send messages to numbers in the victim's list.

5. RiskTool.ANdroidOS.SMSreg.cw. This payment module is widespread in China. It is included in various games as a module for making online purchases via SMS within an application. It removes confirmation text messages from the billing system without the user's knowledge. Victims have no idea money was stolen from their mobile until they check the balance.

6. Trojan-SMS.AndroidOS.Agent.u. This was the first Trojan to use a vulnerability in Android OS to gain DEVICE ADMIN privileges, thereby making its removal a very difficult task. In addition, it is capable of rejecting incoming calls and of making calls on its own. Possible damage: sending multiple SMS messages with costs totaling $9 or more.

7. Trojan,AndroidOSPlangton.a. This advertising module sends user's personal information (without their knowledge) to an advertising server, making it look like a targeted advertising campaign. The resulting damage includes the user's mobile number, Google account and some other data being discrediting. This Trojan also arbitrarily changes the home page of the browser and adds advertising bookmarks.

8. Trojan-SMS.AndroidOS.OpFake.a. This multifunctional bot helps distribute the sophisticated Android malware **Backdoor.AndroidOS.Obad.a.** A composite of these two is extremely dangerous because of its:

1. 1 wide range of capabilities: identity theft, sending text messages to any number. Installation of an application like this could lead to all the money being stolen from a mobile account. It may also result in

the affected phone number being discredited after the contact numbers stolen from the account are used to send text messages. The list of contacts will also be uploaded to the criminal's server.

2. 2 extremely complex self-defense mechanisms and counter measures that prevent deletion. Due to the exploitation of an Android vulnerability, this Trojan cannot be removed without a special program such as KIS for Android.

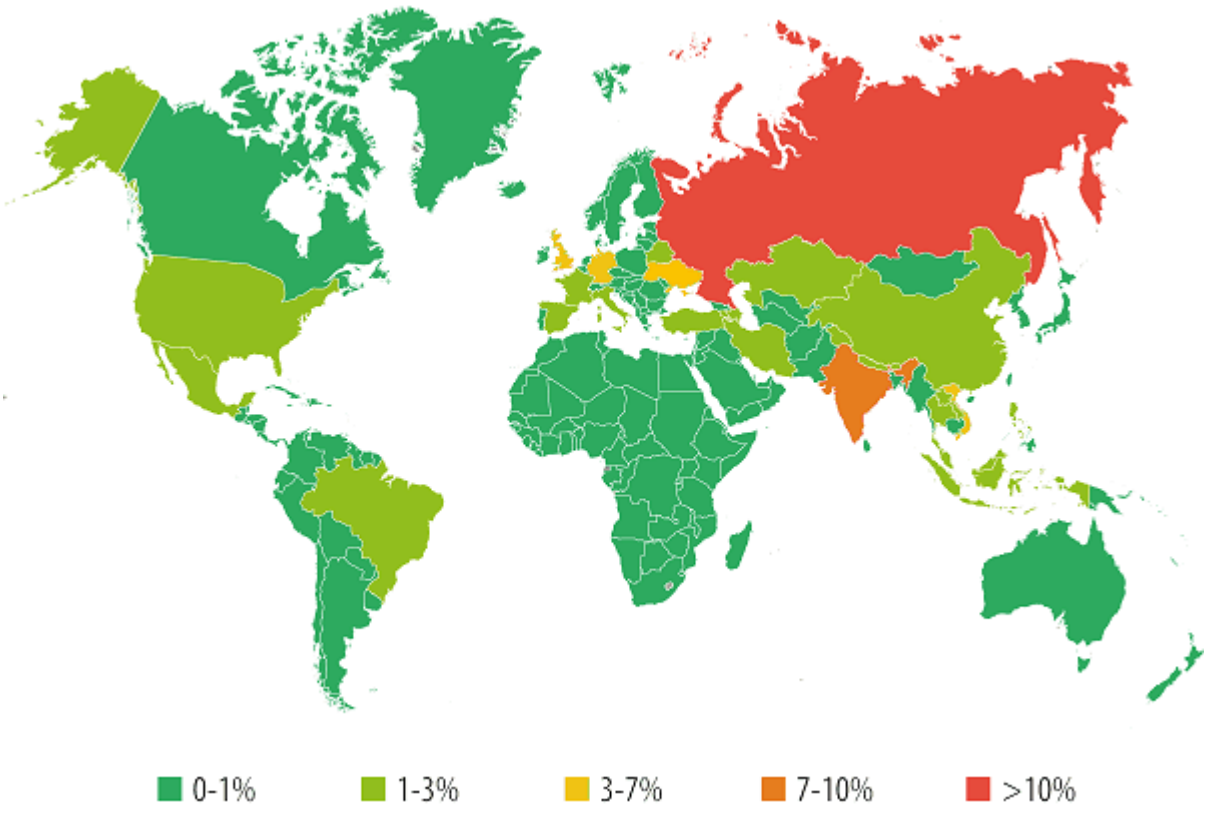
It should be noted that **Trojan-SMS.AndroidOS.OpFake.a.** is spread over a larger geographical area than the other Top 10 leaders. We often register attempts to infect devices not only in the CIS countries but also in Europe.

9. Trojan.AndroidOS.MTK.a. This is a sophisticated Trojan program with wide functionality and sophisticated encryption methods. Its main task is to run malicious apps that have been downloaded to the infected device.

10. AdWare.AndroidOS.Hamoba.a is an advertising application imitating legitimate programs (by using the name and the icon, for example, WinRAR), while its only functionality is to display adverts.

The Top 10 includes four SMS Trojans, although some of them possess control mechanisms that convert infected devices into bots.

The geography of threats



Countries where users face the greatest risk of mobile malware infection (the percentage of all attacked unique users)

The TOP 10 countries by number of attacked unique users:

	Country	% of all attacked unique users
1	Russia	40.34%
2	India	7.90%
3	Vietnam	3.96%
4	Ukraine	3.84%
5	United Kingdom	3.42%
6	Germany	3.20%
7	Kazakhstan	2.88%
8	USA	2.13%
9	Malaysia	2.12%
10	Iran	2.01%

Mobile threats have region-specific features – attackers use different categories of mobile malware depending on the region or the country. Below are a few examples of mobile malware distribution by country.

Russia

In Russia, mobile cybercrime is particularly prevalent – 40.3% of all users attacked worldwide in 2013 were located in this country.

Top 5 families of mobile malware distributed in Russia

Family	% of all attacked unique users
Trojan-SMS.AndroidOS.OpFake	40.19%
Trojan-SMS.AndroidOS.FakeInst	28.57%
Trojan-SMS.AndroidOS.Agent	27.11%
DangerousObject.Multi.Generic	25.30%
Trojan-SMS.AndroidOS.Stealer	15.98%

In 2013, Russia again led the way in the number of SMS Trojan infections and there are currently no signs that the situation will improve. As has already been mentioned above, the majority of mobile banking Trojans target Russian users.

Russia and the CIS countries often serve as a testing ground for new technologies: having perfected their technologies in the Russian-language sector of the Internet, the cybercriminals then turn their attention to users in

other countries.

Germany

Germany is one of the Western European countries where SMS Trojans are quite active. In 2013, Europe was clearly a target for Russian virus writers, as their monetization scams involving text messages being sent to premium numbers works well in this region. In Germany, we registered constant attempts at SMS Trojan infection, especially by the Agent malware family.

Mobile banking Trojans are also actively used in this country: Germany ranks first among Western European countries by the number of unique users attacked (6th place in the world rating).

Top 5 families of mobile malware distributed in Germany

Family	% of all attacked unique users
RiskTool.AndroidOS.SMSreg	25.88%
DangerousObject.Multi.Generic	20.83%
Trojan-SMS.AndroidOS.Agent	9.25%
Trojan.AndroidOS.MTK	8.58%
AdWare.AndroidOS.Ganlet	5.92%

The USA

The situation in the USA is different. There are no monetization scams involving text messages, meaning there is no clear dominance by mobile SMS Trojans. The leaders include bots collecting data about infected smartphones.

Top 5 families of mobile malware distributed in the US

Family	% of all attacked unique users
DangerousObject.Multi.Generic	19.75%
RiskTool.AndroidOS.SMSreg	19.24%
Monitor.AndroidOS.Walien	11.24%
Backdoor.AndroidOS.GinMaster	8.05%
AdWare.AndroidOS.Ganlet	7.29%

China

In China, there are a lot of advertising modules integrated into clean and even malicious applications. The functions of advertising modules are diverse, even going as far as downloading malware to the victim’s phone.

SMS Trojans and backdoors are also very popular in China.

Top 5 families of mobile malware distributed in China

Family	% of all attacked unique users
RiskTool.AndroidOS.SMSreg	46.43%
AdWare.AndroidOS.Dowgin	19.18%
DangerousObject.Multi.Generic	13.89%
Trojan-SMS.AndroidOS.Agent	10.55%
Trojan.AndroidOS.MTK	10.13%

Conclusion

Malicious software that attacks users of mobile banking accounts continues to develop and the number of programs is growing rapidly. It is obvious that this trend will continue, with more mobile banking Trojans and new technologies to avoid detection and removal.

Of all the mobile malware samples detected in 2013, bots were the most numerous category. The attackers have clearly seen the benefits of mobile botnets when it comes to making profits. New mechanisms for controlling mobile botnets may appear in the near future.

In 2014 we expect to see vulnerabilities of all types being actively exploited to give malware root access on devices, making removal even more difficult.

2013 saw the first registered malware attack on a PC launched from a mobile device. We forecast future Wi-Fi attacks from mobile devices on neighboring workstations and the wider infrastructure.

SMS Trojans are likely to remain among the mobile malware leaders and even conquer new territories.
