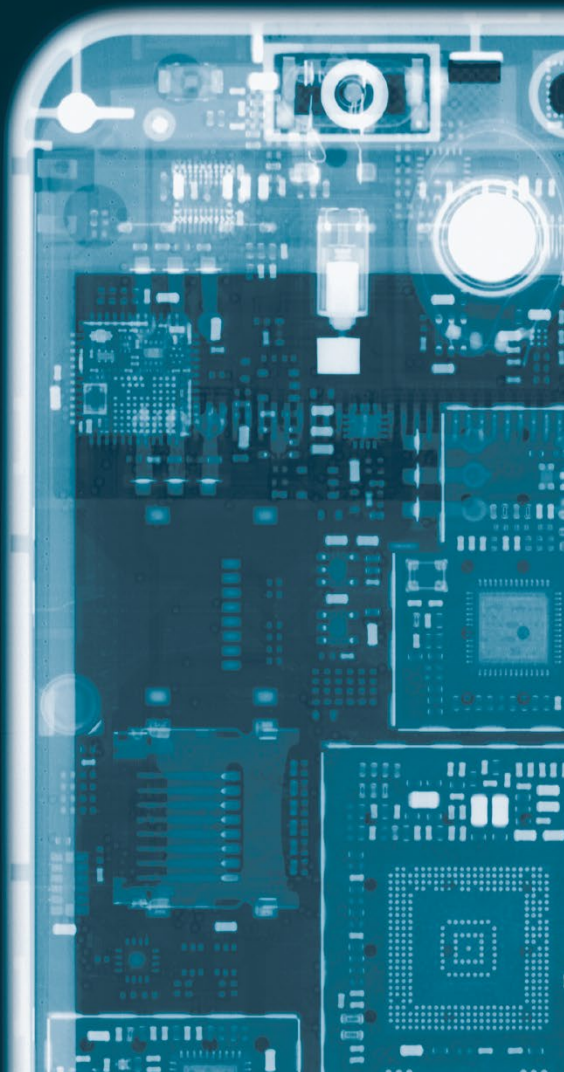
MOBILE CYBER THREATS

Kaspersky Lab & INTERPOL Joint Report

October 2014



INTERPOL | KASPERSKY lab

INTERPOL | KASPERSKY

Note on Responsible Distribution of Information

This document presents an analysis of the cyber-threat landscape as it relates to Android-based mobile platforms. It is based on information about instances of Kaspersky Lab security products detecting applications considered insecure or malicious due to their functionality. To avoid possible misinterpretation of the facts presented in this document, Kaspersky Lab would like to highlight a number of issues related to the way this report was prepared.

1. Terminology

The report uses several terms describing how a security product interacts with malicious software. The term “Attack” is among those used most frequently. In Kaspersky Lab’s terminology, an attack is an instance of a security product detecting any software considered malicious on the protected device, regardless of whether an attempt to execute malicious code was detected. The term “User” denotes exclusively the owner of the device protected by Kaspersky Lab’s product.

2. Dataset and its geographical distribution

All calculations and conclusions made in this study rely on data from Kaspersky Lab’s mobile customer community, which exceeds 5 million users in over 200 countries and territories. It should be emphasized that the number of Kaspersky Lab’s product users varies from country to country, so the results of this study may not fully reflect the situation existing in some countries. However, many years’ experience of monitoring the statistics collected by Kaspersky Security Network (KSN) shows that in most cases KSN data is about 95% accurate concerning the prevalence of specific cyber-threats or cyber-threat classes, and

concerning on the percentage distribution of consumers using devices running different operating systems. It also correlates very well with data received from other sources, namely from companies which specialize in collecting and analyzing statistical data.

Responsible distribution of information

This study can be freely shared or distributed. Kaspersky Lab requests that those who find the information presented in this document interesting and useful make allowances for the abovementioned issues related to the ways in which KSN statistics are collected when preparing public materials in which this information is to be used.

Contents

International Cooperation to Combat Cybercrime

Cyber-threats, including those targeting mobile devices, are directly linked to cybercrime. In most developed countries, creating and distributing malicious software is a criminal offence. Although such criminal acts are perpetrated in virtual environments, their victims lose real assets, such as personal data and money.

Combating cybercrime is particularly difficult because cybercriminals do not need to cross the borders of other countries to commit crimes in those territories. At the same time, enforcement authorities in these same countries have to overcome numerous barriers in order to administer justice. Therefore, international cooperation between information security experts and law enforcement authorities is required to effectively combat crime in the virtual world. Kaspersky Lab is an international company that brings together IT security experts from all over the world and seeks to provide detailed and highly qualified technical consultations to assist local law-enforcement agencies investigating cybercrime.

To cooperate as effectively as possible against international cybercrime, Kaspersky Lab and the International Criminal Police Organization (INTERPOL) have established a partnership, under which Kaspersky Lab experts will share their expertise in cyber-threat analysis with INTERPOL officers.

This “Mobile cyber-threats” report has been prepared by Kaspersky Lab and INTERPOL within that partnership framework. It aims to evaluate how widespread mobile threats are, and to alert the international IT security and law enforcement community to the problem of crime in the area of mobile communications.

Introduction:
The Mobile Leader and Target no. 1

Smartphones and tablets have long been established as popular personal electronics devices. A joint Kaspersky Lab and B2B International survey conducted in the spring of 2014 found that 77% of the Internet users surveyed use several devices to access the World Wide Web; alongside traditional computers, they typically use smartphones and tablets. So what types of smartphones and tablets are used?

According to IDC's Q2 2014 report, the sales of such devices have, for the first time ever, passed the mark of 300,000,000 devices sold per quarter. This is an important milestone in the market that has been growing for several years.

According to the same IDC report, the distribution of operating systems for mobile devices looks like this:

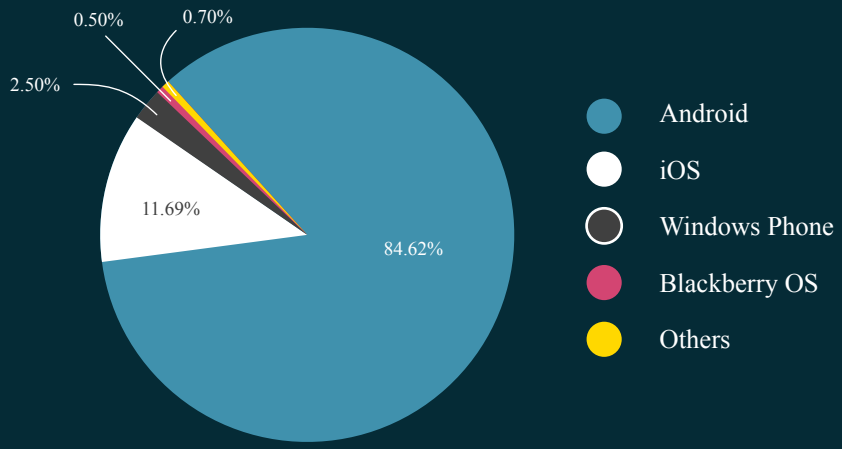


Figure 1. Distribution of mobile operating systems in Q2 2014, according to IDC. Source: IDC

As the diagram shows, nearly 85% of the mobile device market was occupied by Android in Q2 2014. These numbers an another acknowledgement of Android's undisputed leadership among mobile environments. This operating system is free for device manufacturers and can be easily modified to match various business needs, which has helped it achieve popularity among smartphone and tablet developers as well as consumers across the world. This also means that Android-based devices inevitably attract the attention of cybercriminals who are creating and distributing malicious programs

Kaspersky Lab experts estimate that 98.05% of all existing mobile malware targets the users of Android devices. So, how much is "all existing malware"? Kaspersky Lab experts report that in the first half of 2014 alone, 175,442 new unique Android malicious programs were detected. That is 18.3% (or 32,231 malicious programs) more than in the entire year of 2013.

For these and other reasons, it is safe to say that that vast majority of mobile cyber-threats are targeting Android.

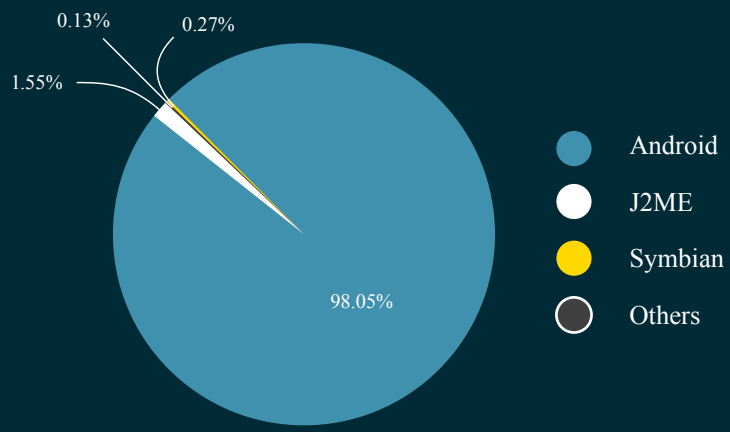


Figure 2. The distribution of Kaspersky Lab products' malware detections in 2013 between different mobile environments

It is easy to understand why cybercriminals create so many malicious programs targeting Android devices: these days, smartphones are increasingly often used as a tool to pay online for merchandise and services.

Apps can be installed through Google Play as well as third parties such as Amazon App store. Third party apps pose a security threat to users who enable the installation of apps from unverified sources. These unverified packages may carry malware that would be installed on a device without the user's permission or knowledge.

Another danger is the possibility of an attacker gaining access to personal data such as the user's cloud storage accounts and associated email identifiers. This information can be used to access personal content that is stored in cloud base storage without the user's knowledge or permission.

Smartphones can also be regarded as a kind of mobile sensor, since they routinely collect a multitude of personal information about their owners. In other words, mobile device users are a very valuable target for cybercriminals.

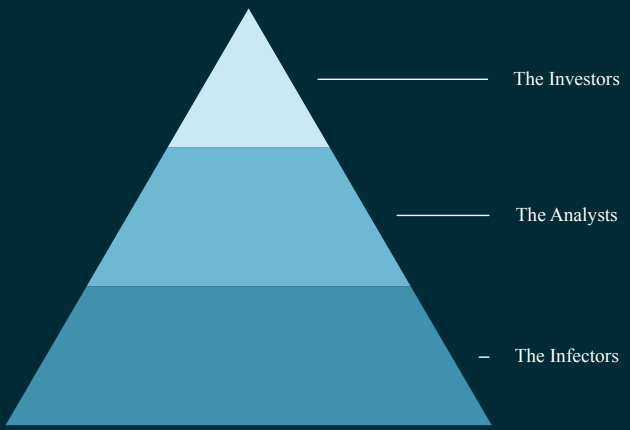


Figure 3. The scheme of actors involved in cybercrime. Source: INTERPOL

Information is the new currency and this has led to a drastic change in the structure of organized criminal groups, which now support a larger group of actors. The bottom to top approach leaves us with three basic categories (1) The Infectors, (2) The Analysts, and (3) The Investors. The Infectors' role is to mass-propagate and exploit devices as well as picking up data from the devices with very little discrimination about the type of data collected — the more the better. The Analysts' job revolves around studying and processing the data that was collected, monetizing it by offering it on underground markets, blackmailing individuals or using the information to invest into markets that would eventually allow the criminals to profit from illegally obtained information or insider trading. The Investors are responsible for funding and providing financial support to the pyramid –obviously they then receive the majority of the profits made over time.

This model has overtaken the lone hacker scenario, which is now merely a media misconception. When it comes to mobile devices, it has been underlined that they can be a greater source of personal or business information than desktop computers. That, coupled with the fact that these devices are often less secure, has caused Infectors to refocus their efforts onto the mobile device sector.

Of course these and other factors have an effect on how often smartphone and tablet users encounter dangerous software while accessing the Internet from their mobile devices.

How much risk is there in being an active Android user, and how can users reduce that risk? Details on this are provided in this report.

Methodology

This study focused on the **12-month period of 1 August 2013 through 31 July 2014.** This study period was chosen based on Kaspersky Lab data. Kaspersky Lab began to collect statistics on attacks against Android users in May 2012. During the more than two years that followed, it was the above mentioned time frame that showed that the number of Android threats, the number of attacks and the number of attacked users grew particularly sharply.

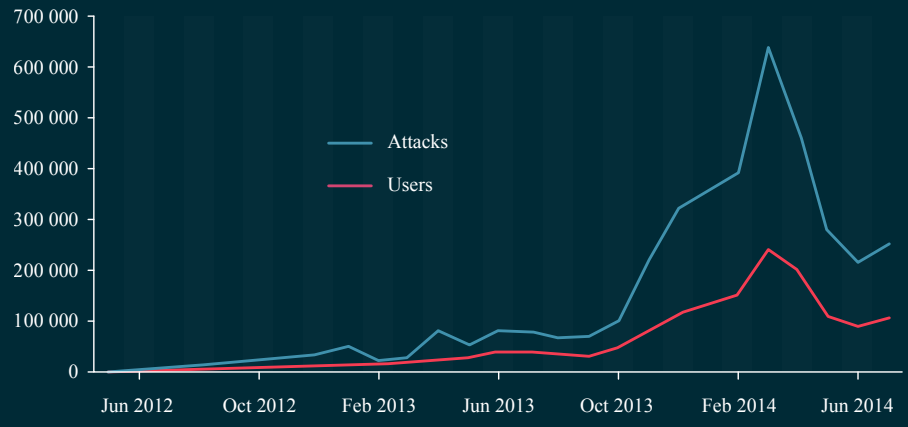


Figure 4. Detections by Kaspersky Lab's security products of cyber-attacks on Android devices throughout the entire history of observations. All data sourced from Kaspersky Security Network, unless stated otherwise

Naturally, this dramatic increase partly comes from the increasing numbers of users who purchased Kaspersky Lab's mobile security products. However, this is not the sole, nor even the main factor, behind this growth.

Apart from changes in the numbers of launched attacks and attacked users, this study will also focus on the geographic distribution of attacks and users. Additionally, a list of the most widespread malicious programs for Android will be analyzed.

Data used in this research was sourced from the cloud-based Kaspersky Security Network (KSN), which includes more than 5,000,000 users of Android-based smartphones and tablets protected by Kaspersky Lab products. This research analyzes threat data collected from these devices.

The Main Findings

- Over a 12 month period, Kaspersky Lab security products reported **3,408,112** malware detections on the devices of **1,023,202 users.**
- Over the 10 month period from August 2013 through March 2014, the number of attacks per month was up **nearly tenfold**, from 69,000 in August 2013 to 644,000 in March 2014.
- The number of users attacked also increased rapidly, from 35,000 in August 2013 to 242,000 in March.
- 59.06% of malware detections related to programs capable of stealing users' money
- About **500,000 users** have encountered mobile malware designed to steal money at least once.
- Russia, India, Kazakhstan, Vietnam, Ukraine and Germany are the countries with the largest numbers of attacks reported.
- Trojans designed to send SMSs were the most widespread malicious programs in the reporting period. They accounted for 57.08% of all detections.
- The number of modifications for mobile banking Trojans **increased 14 times** over 12 months, from a few hundred to more than 5000

Part 1: General trends in the evolution of mobile threats

There are those who believe that Android is a secure platform. When confronted with the fact that new Android malware emerges every day, these people often say that those malicious programs are in fact very rare and pose only a limited threat to the owners of Android devices. For a long time, these views have been justified. If we look at the historical course of the number of existing Android threats (see Figure 4), we will indeed see that before the summer of 2013 the numbers of attacks and attacked users were well below 100,000 a month. That looked very modest as compared to PC attack numbers.

However, this situation changed dramatically during the period analyzed in this paper. In the 12 months from August 2013 through July 2014, over **1,020,000 Android users** across the globe encountered more than **3,400,000 attacks**. That was six times more than the number of attacks in the whole of the previous 1.5 years when records were kept.

Over the reporting period, the number of attacks showed a dramatic growth, increasing nearly 10 times from 69,000 in August 2013 to 644,000 in March 2014. Then there was a sudden fall in activity, down to 216,000 incidents in June.

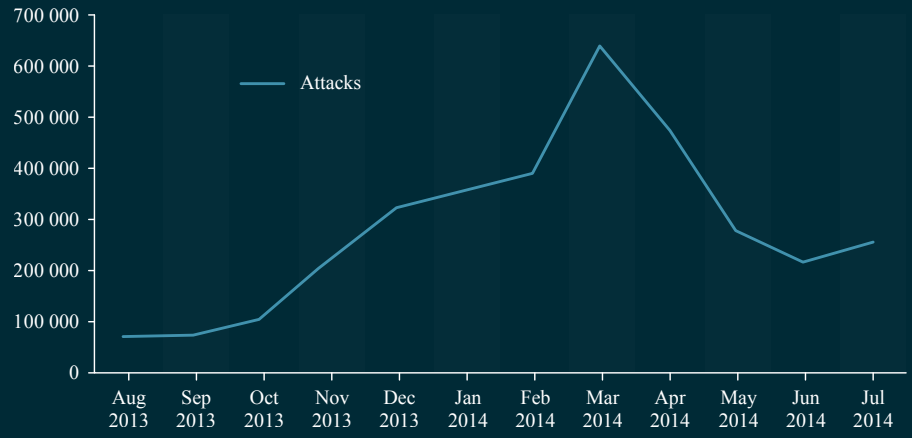


Figure 5. Number of Kaspersky Lab Android product detections of malware targeting Android devices. August 2013 through July 2014.

At the end of the Holiday season, there was no decrease in the activity, despite expectations. Instead, there was a further dramatic spike. The decline only began in April.

The geographic distribution of attacks and attacked users

More than half (52%) of attacks during the study period were reported in Russia. This is primarily due to the fact that Russian residents form a particularly large proportion of the users who agreed to have their statistics sent to Kaspersky Security Network.

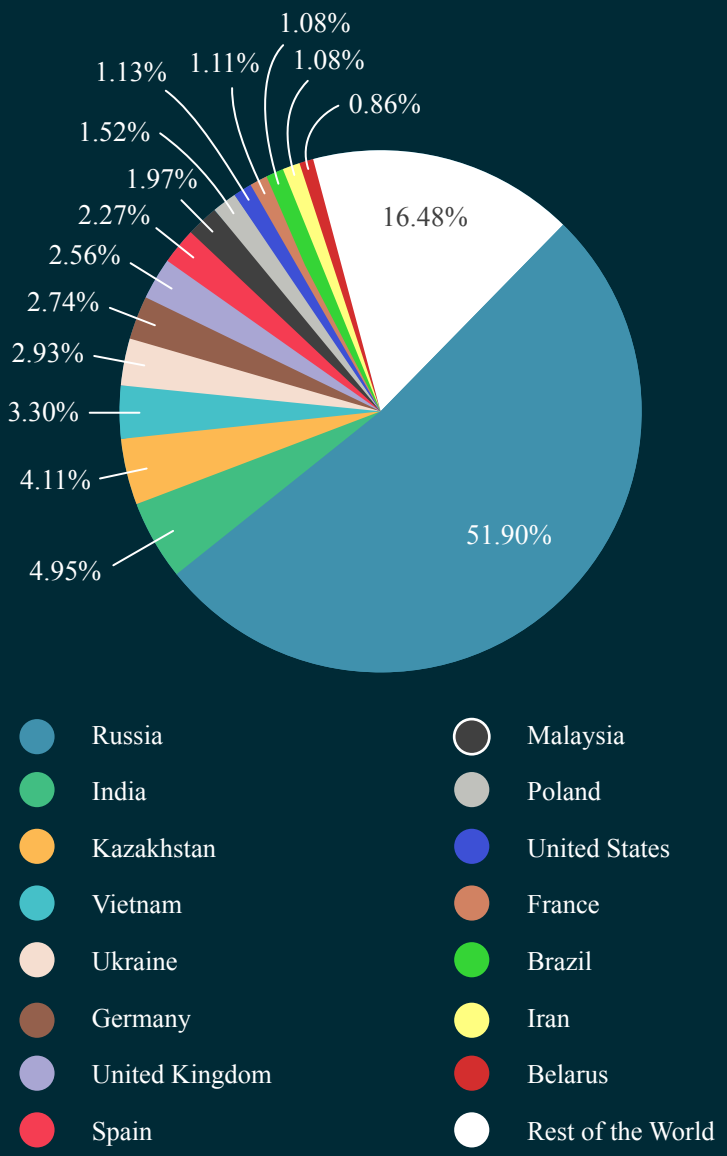


Figure 6. Top 15 countries with highest numbers of users attacked between April 2013 and July 2014.

Another contributing factor is the wide popularity of various mobile payment services in Russia. These allow users to pay for goods or services by sending premium SMSs. This encourages cybercriminals to create and distribute Android malware exploiting these services.

However, it may be misleading to think that the malware industry is well-developed in Russia and comparatively calm in the rest of the world. Russian-speaking cybercriminals are definitely interested in foreign markets. Two banking Trojans, Faketoken and Svpeng, are vivid examples of such attempts at globalization. These two were created to launch attacks on the clients of foreign banks, and only a few versions target Russian users.

Part 2: The ‘Star’ Performers

As predicted, the number of attacks increased over time, more malware modifications were detected.

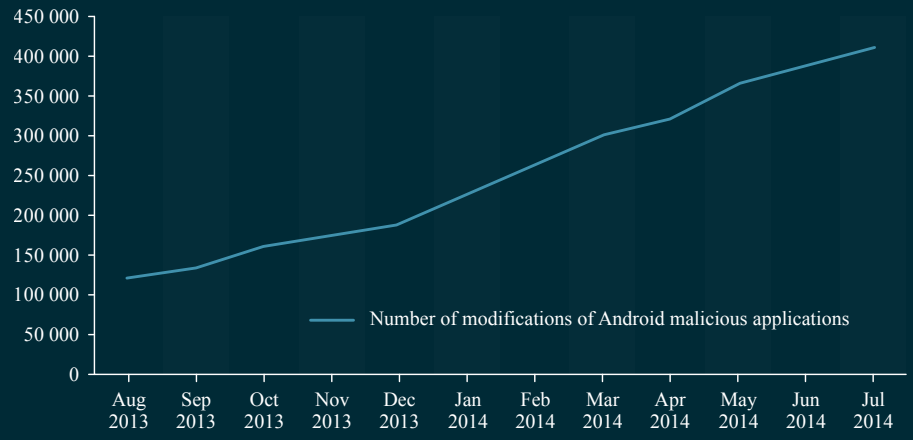


Figure 7. Number of modifications of Android malicious applications, as detected by Kaspersky Lab in August 2013 – July 2014.

This number rose by a factor of nearly 3.4 over the year, from 120,500 malware modifications in August 2013 to 410,800 in July 2014.

For the study period the top 10 most widespread malware are mostly malicious programs from the Trojan-SMS type – these accounted for 57.08% of all attacks. Following that, RiskTool programs, accounting for 12.52% detections, are in second position. These are nominally legitimate programs that can also be used for malicious purposes, such as sending SMS with a visual notification of the user, transmitting geo-data etc. Aggressive advertising software (adware) came in third (7.37%.)

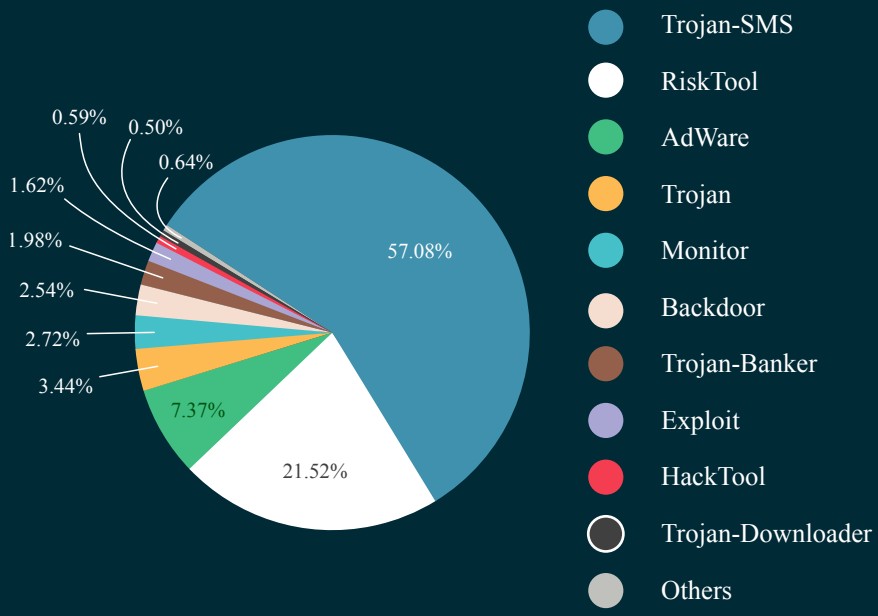


Figure 8. Distribution of attacks by malware types: Top 10 most active malware types. August 2013 – July 2014.

These overall statistics are affected by the large number of Russian users and the popularity of SMS payments in Russia. To eliminate any possible "Russian" bias, we also looked at the cyber-threat landscape described without data collected from users in Russia.

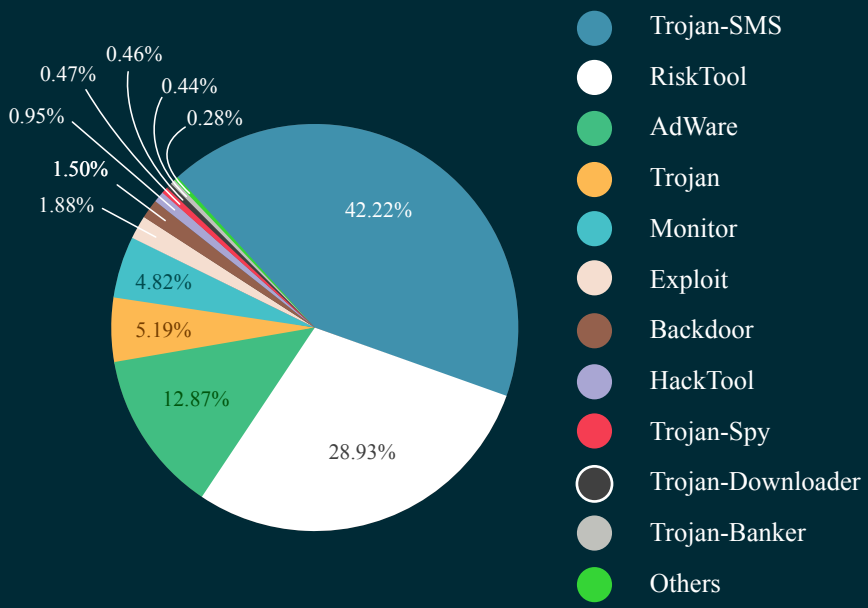


Figure 9. Distribution of attacks by malware types, excluding data from Russian users. August 2013 – July 2014.

As can be seen in the diagram, the numbers have changed. However, the overall situation remains broadly similar: Trojan SMS is still the most widespread type of malware. Below is a graph showing the Top 10 countries with the largest numbers of reported attacks involving Trojan SMS malware:

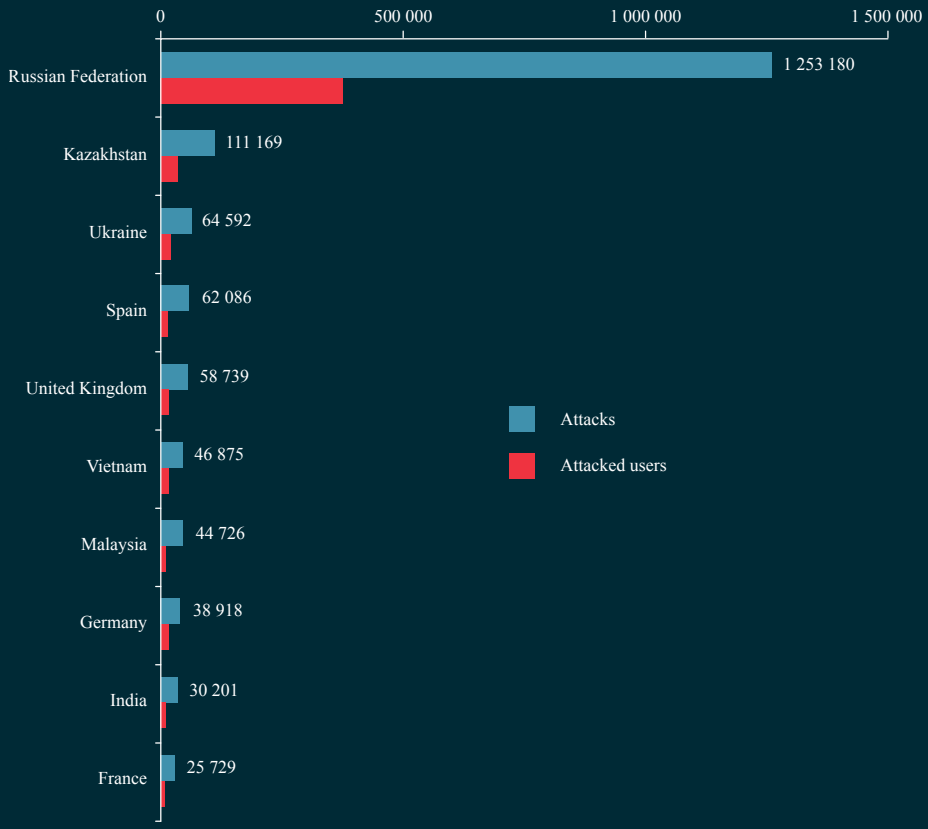


Figure 10. Top 10 countries with the largest numbers of reported attacks involving Trojan-SMS malware. August 2013 – July 2014

Attacks involving Trojan-SMS malware are most frequent in Russia. Residents of Kazakhstan, Ukraine, the UK, Spain, Vietnam, Malaysia, Germany, India, France and other countries also encounter attacks involving this type of malware.

Malware created with the sole aim of stealing money from victims (i.e. Trojan-SMS and Trojan-Banker malware types) accounted for **59.06% of attacks** and was reported on the

devices of **49.28%** of users during the study period. In absolute numbers that represents half a million users who agreed to have their statistics on detected threats sent to KSN.

It is hardly surprising that cybercriminals actively use financial Trojans. As reported in a B2B International report, 53% of polled smartphone and tablet users say they use the devices to pay online. In other words, theoretically cybercriminals can potentially make money on every second user of a mobile device. Statistics show that approximately every second user is indeed attacked by cybercriminals.

Legitimate surveillance

Approximately 2.72% of all detections, or 92,600 detections, involved "Monitor" class programs. In Kaspersky Lab's classification, this stands for conditionally legitimate applications designed to conduct surveillance over smartphone users. These applications can track the user's location, read his/her messages, and access other personal information. The manufacturers of such software advertise it as a useful tool to help look after children and the elderly, but Kaspersky Lab classifies it as potentially insecure. A total of 41,400 users encountered such applications in the 12-month period. On average, each of these users encountered such programs twice.

Interestingly, the geographical distribution of these programs is noticeably different from the overall global distribution of malware detections.

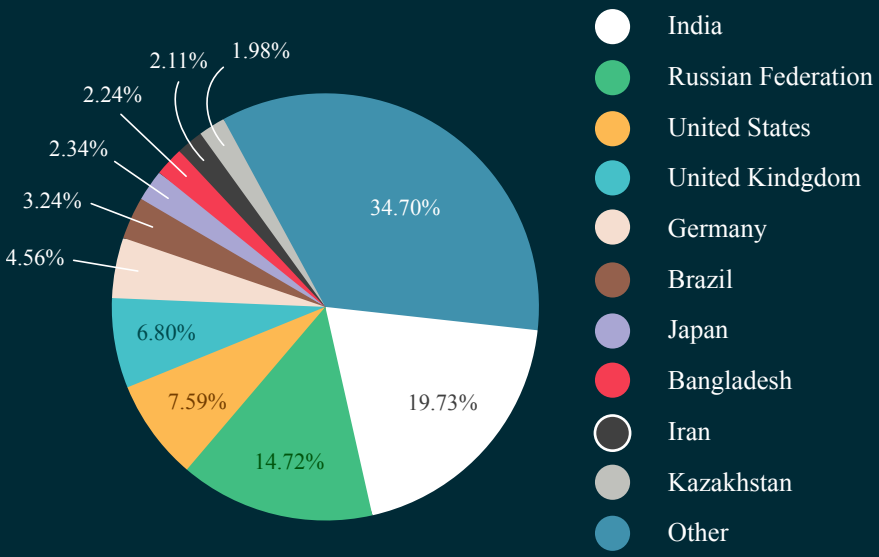


Figure 11. The geographical distribution of detected "legitimate" spyware in the "Monitor" class. August 2013 – July 2014.

India is in first position with 19.73% of all detections. Russia is in second place with 14.72% of all detections (even though it is the leader of the general threat ranking). Users in the USA also quite often encounter these applications (7.59% detections); followed by the UK (6.8%) and Germany (4.56%). Kaspersky Lab experts have no reason to assume all these detection cases are attempts to secretly install these programs on a device protected by a Kaspersky Lab product. However, this scenario is possible, so Kaspersky Lab security products detect Monitor-class programs as potentially dangerous.

Part 3: Trojan-SMS and the 'Legitimate' Business of Affiliate Programs

During the reporting period, 452 different modifications of 62 different Trojans capable of using SMS messaging were detected.

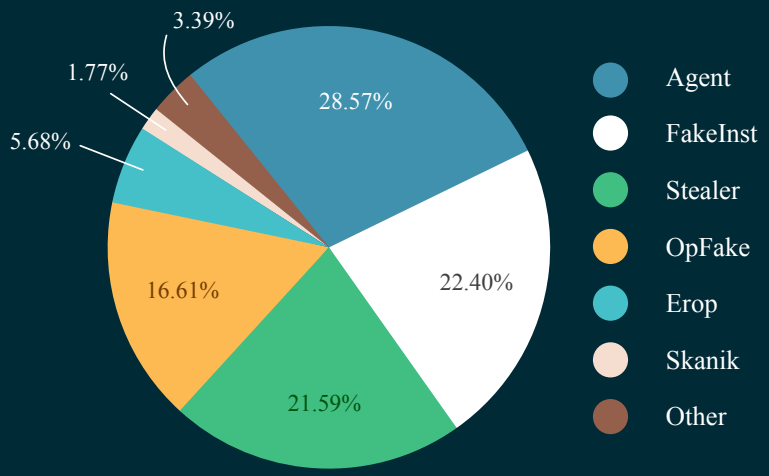


Figure 12: Distribution of attacks involving the most widespread SMS Trojans during the period from August 2013 to July 2014

Malware from the Agent family had the largest proportion of detection (28.57%), followed by FakeInst (22.4%) in second place and Stealer (21.59%) in third.

According to Kaspersky Lab experts, affiliate programs are one of the most common ways of delivering malicious code.

A typical setup for a malicious affiliate program is as follows: a group of cybercriminals creates an affiliate website and invite Internet users to become their accomplices and make money by

distributing a malicious program. A unique modification of the malware and a landing page from which it will be downloaded to victims' devices is created for each user who agrees to take part. After that, participants of the affiliate program buy Internet traffic from third parties or bring in users by redirecting requests from compromised websites, displaying banners on popular Web resources or creating their own sites and promoting them using search-engine optimization. The objective is to have as many Android users as possible visit the page hosting the malicious application. After each successful installation, the newly-infected device starts sending SMS messages to premium numbers, making money for the cybercriminals. Part of that money is paid to the affiliate partners. Criminal groups that sell traffic usually resort to various social engineering techniques, attracting users with pornography, free games, etc.

According to Kaspersky Lab experts, about 38% of users who end up on these landing pages will download malicious apps from them. About 5% of users go on to install these applications. Cybercriminals can earn millions of dollars in net profits from this activity.

During the study period, Kaspersky Lab experts observed at least four large active affiliate programs, accounting for about one quarter of all attacks recorded over that time. All of these affiliate programs were primarily active in Russia and countries of the former Soviet Union, but each program used a different family of SMS Trojans.

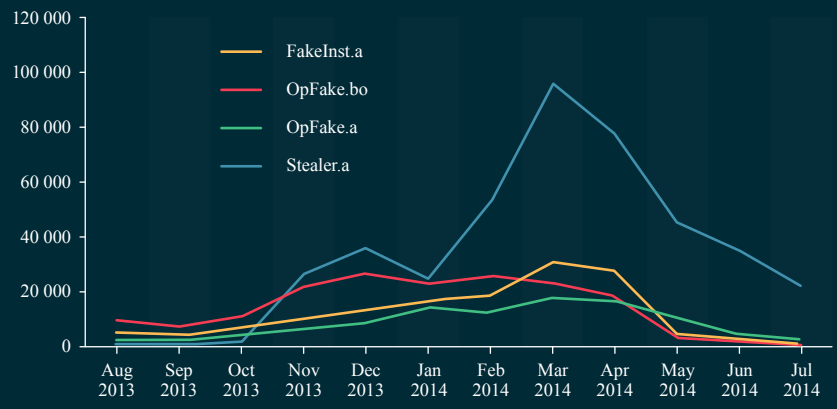


Figure 13: Activity of four affiliate programs distributing Android malware from August 2013 to July 2014

In the beginning of the period under consideration, there were three 'leaders' in this market: Fakeinst.am, Opfake.bo and Opfake.a, of which Opfake.bo was the most active and successful. However, the situation changed radically in October 2013 with the appearance of a new player – Stealer.a. It was different from competing malware in that it had more extensive functionality and spread very actively. By November 2013 it was the most frequently detected affiliate program and remained at the top throughout the rest of the research period.

2014: bad news for malicious affiliate programs

The abovementioned attacks conducted using SMS Trojans were different from typical malicious campaigns targeting PCs in one important respect. Legitimate legal entities, mostly registered in Russia, were involved in distributing Android Trojans and profited from the consequences of infecting smartphones. The business model of affiliate programs that distribute applications and premium content is not illegal, but there is indirect evidence that the companies behind some of the affiliate programs described above worked with cybercriminals as well as those who distribute legitimate content and apps.

This situation continued for a long time, because neither the heavy penalties issued by mobile-phone operators for mounting fraud campaigns nor criminal liability for distributing malware managed to stop cybercriminals or the organizations that worked with them. However, everything changed in early 2014: shortly before changes in legislation aiming, among other things, to curtail SMS fraud came into effect, mobile-phone operators adopted an Advice of Charge (AoC) mechanism. Every time a customer (or an SMS Trojan) attempts to send a message to a premium number, the operator notifies the customer how much the service will cost and requests additional confirmation from the user.

Early in the year the mechanism was applied to selected types of premium SMS services and as of May 1, 2014 a new law made it obligatory for mobile-phone operators to notify their customers of any attempts to start any mobile subscription. This coincided with a radical fall in the number of attacks involving SMS Trojans.

The major surge in the number of attacks, particularly those involving Stealer.a, could have been an attempt to make as much money as possible before AoC was universally adopted.

Kaspersky Lab experts observed that in spring 2014 the three affiliate programs which distributed Fakeinst.am, Opfake.bo and Opfake.a stopped active operation. Kaspersky Lab experts have no reason to believe that the three affiliate programs have run out of steam completely, but they lack their earlier vigor and the reduced number of attacks involving SMS Trojans is a good, albeit indirect, indication of this.

The most active program of the four – the one distributing Stealer.a – has also lost a lot of ground in terms of the number of attacks, but users often still come across versions of this malicious app.

Curiously, although all these affiliate programs were set up and maintained by Russian-speaking cybercriminals and their scams mostly targeted users from Russia and the former Soviet Union, parts of Europe saw fewer attacks involving SMS Trojans in spring, too.

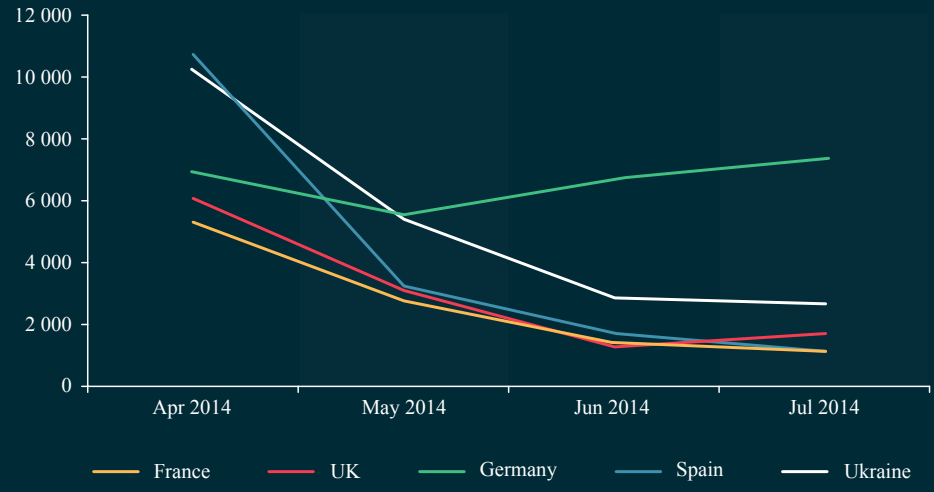


Figure 14: Changes in the number of attacks involving Trojan-SMS in European countries where Kaspersky Lab products detected this type of malware from April to June 2014

The diagram above shows data about attacks involving Trojan-SMS in the European countries in the Top 10 for attacks using Trojan-SMS. The diagram shows that four of the five countries which ranked among those attacked most often have seen the number of attacks fall.

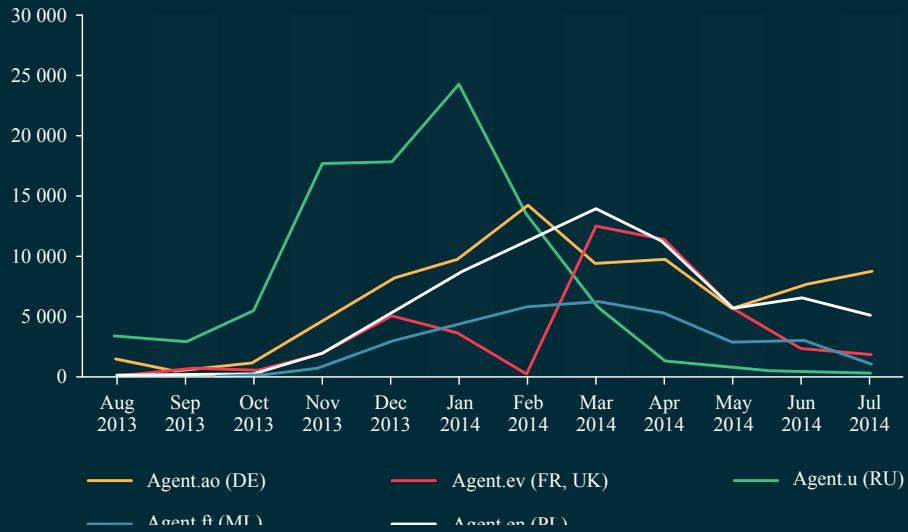


Figure 15: Attacks involving Agent family Trojans from August 2013 to July 2014

Towards the end of the period there was also a slight growth in the number of attacks in Germany by Agent.ao malware, which was distributed by an affiliate program primarily targeting that country. All other affiliate programs which had been active in Europe and Asia were noticeably less active.

In other words, the number of attacks was falling almost everywhere in the post-Soviet space, in Europe and in Asia.

This may be due to two reasons. First, cybercriminals wind down their activity during the vacation season, which begins in spring. Additionally, the Russian legislative developments described above may also have contributed to the decline. Kaspersky Lab experts have frequently observed that Russian-speaking developers of Android malware have global ambitions and adapt their malware, including Trojan-SMS, to attack markets where languages other than Russian are spoken. However, the number of detections recorded outside the post-Soviet space has always been significantly smaller than in Russia and its neighbors – in other words, it is unlikely that most distant targets brought much money to the owners of affiliate

programs based in Russia. So when the main 'players' in a Russian segment of Android malware wound down their activity, this naturally resulted in the closure of their foreign 'projects'.

Admittedly, Kaspersky Lab experts do not have the solid evidence needed to confirm this theory, though if it is it would be an example of how anti-fraud measures in one country can have a beneficial effect – albeit a small one – elsewhere in the world.

Mobile banking Trojans: dangerous trends

A total of 67,500 attacks involving Trojan-Banker malware against 37.7 thousand users were recorded in the analysis period. Trojan-Banker is a type of malware designed to steal online banking credentials. The total number of banking Trojans targeting mobile devices grew from 423 in August of 2013 to 5,967 in July 2014. That is a **more than 14-fold increase!**

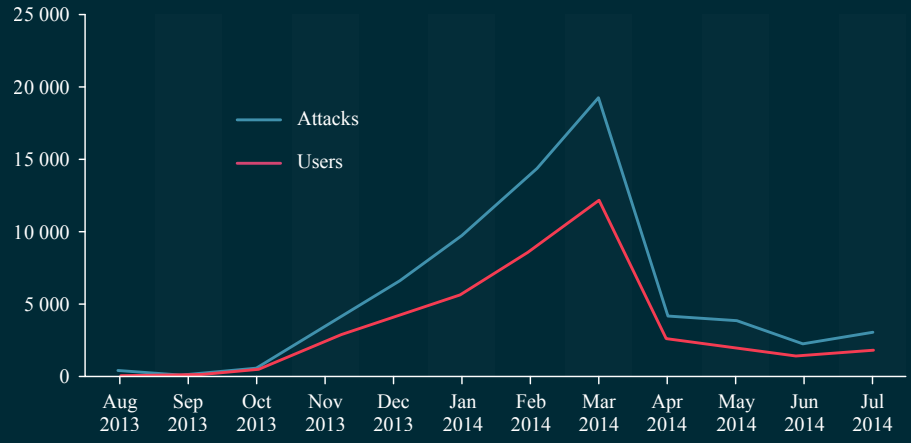


Figure 16: Changes in the number of attacks and users attacked by Trojan-Banker malware from August 2013 to July 2014.

However, even though there were more malware variants, the decline in the use of Trojan-SMS malware also affected Trojan-Bankers. This was primarily because one of the banking Trojans was distributed using the same affiliate networks as Trojan-SMS malware.

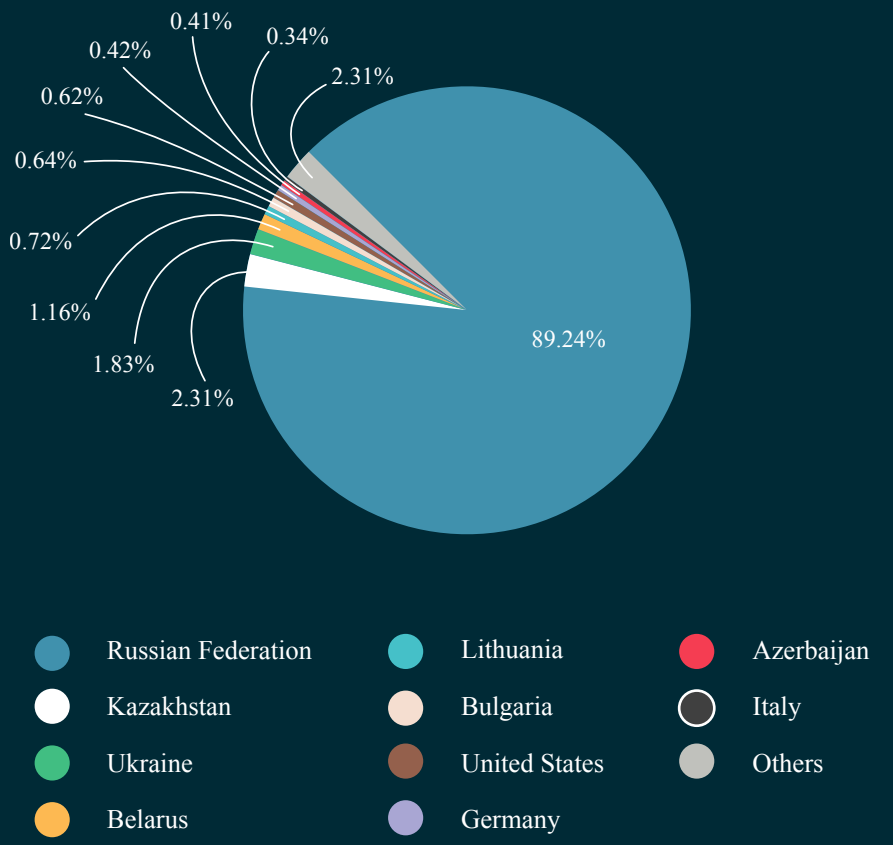


Figure 17: Geographical distribution of users affected by Trojan-Banker on Android from August 2013 to July 2014.

The overall downward trend was sparked by the Faketoken Trojan-Banker, which could steal one-time passwords sent to confirm bank transactions and operated in conjunction with 'desktop' banking Trojans.

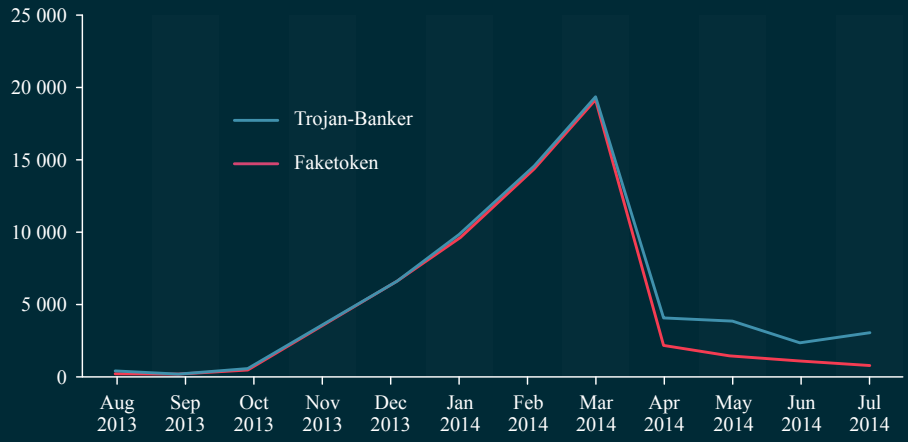


Figure 18: Attacks involving Faketoken, compared to all attacks involving mobile banking Trojans from August 2013 to July 2014

As the diagram above shows, from August to March Faketoken was virtually the only widespread mobile banking Trojan. However Faketoken was distributed by one of the affiliate networks that wound down in April 2014 and from that time it too began to dwindle. Subsequently the overall number of mobile banker detections remained at a higher level than Faketoken and showed a small increase in overall attack numbers.

This rising trend was led by two other programs targeting online banking users – Svpeng and Marcher.

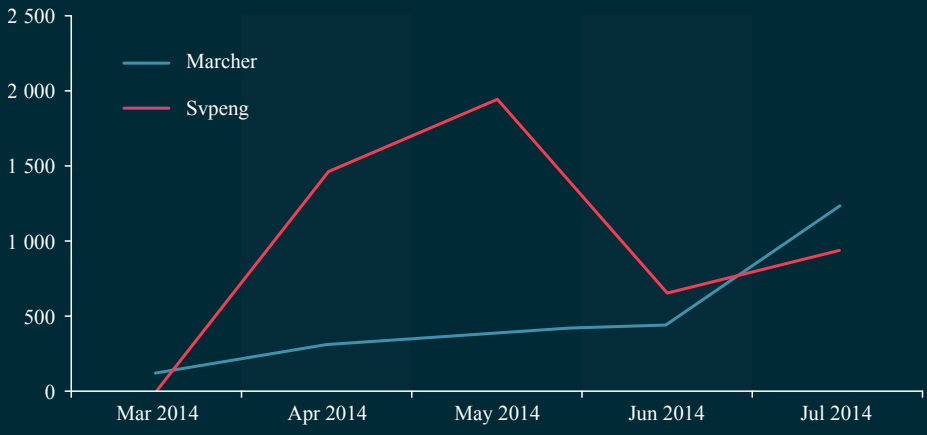


Figure 19: Changes in the number of attacks involving Marcher and Svpeng banking Trojans from March to July 2014

As the diagram shows, the number of attacks involving Svpeng fell from late May to late June; however, in June Kaspersky Lab experts discovered a new Svpeng variant. Previously it was a mostly 'Russian-speaking' and exclusively 'banking' Trojan, but in its new variant Svpeng acquired ransomware Trojan functionality. It displayed messages saying the phone was blocked and demanding several hundred dollars to unblock it. Analysis of the content used by the malware has demonstrated that US users were its main targets.

As for Marcher, at first glance it seems to be just one more 'Russian' banking Trojan –98.84% of users affected by it live in Russia. However, when Kaspersky Lab experts analyzed the Trojan's code they found that the objectives pursued by the Trojan are not quite so obvious.

After infecting a device, the malware tracks the launch of just two apps. If the user starts Google Play, Marcher displays a false window requesting credit card data.

Initially, Marcher was only able to attack Google Play users, but in March 2014 Kaspersky Lab experts discovered a variant that targeted the mobile client of a large German bank's online banking system. If the user launches the bank's mobile banking client, another fake window displays fields for user credentials for the online banking system.

Although so far users of Kaspersky Lab mobile products in Germany have not encountered this threat, this situation may change in the future. Kaspersky Lab experts will track the evolution of this and other dangerous Android threats.

Other Threats: Bitcoin Miners and Ransomware

Bitcoin Mining Malware on Mobile – notable mention

In April 2014, Google Play removed a new category of malware applications that were directly aiming at mining crypto-currencies. "BadLepricon" malware, one of the first to be detected was masquerading as a fully operational live wallpaper application. Infected mobile devices were overheating once the hidden process of crypto-mining currencies was triggered. Even though the processing power of a single mobile device was quite minimal and not really an effective miner, it is estimated that a massive infection of devices could contribute to big profits for the actors managing the malware.

There have been further reports and detections from the Anti-Virus community, some of which indicated that similar malware applications were released on the Google Play market and had over one million downloads, raising serious questions on the profitability of that model. Even though the malware does not target personal information, this type of malware still falls in the category of unauthorized access to a personal device, which makes it illegal to use an individual's machine without the owner's prior consent. It is expected that further variants of crypto-mining malware will emerge in the coming months, possibly focusing on mining altcoins or the family of clonecoins, which are easier to mine than bitcoins at this stage.

Cryptoransomware finds its way to Android

Cryptoransomware refers to a class of malware that infects a machine then encrypts targeted files with specific extensions and demands payment before providing the key to decrypt the files. Cryptoransomware found its way to Android OS in 2014 after gaining a reputation as a growing problem for Internet security companies and law enforcement in general.

Simplelocker A, a piece of cryptoransomware tailored for Android, was the focus of research by INTERPOL. This variant uses AES-256 to encrypt the data within specific

file extensions hosted on the SD card of a mobile device, making it impossible to access the files. More interestingly, the malware itself communicates with its C&C servers by routing to an onion on the Tor Network for further anonymity. Simplelocker.A has been mainly targeting Russian speaking countries. However, security experts believe that it is only a proof of concept with a far more developed, mature and complicated version expected to surface soon in Google Play.

Conclusions and Recommendations

The data analyzed in this study shows that mobile cybercrime is an extremely widespread phenomenon across the globe. It's important to remember that the study only reflects data on users protected against mobile malware and can only give a general idea of the extent to which different threats are widespread and dangerous.

One thing that is certain is that the number of threats is growing and the damage that can be caused by them, potentially, runs to millions of dollars.

Another conclusion is that the cybercriminals involved in distributing malware which targets mobile device users commit their crimes outside the borders of the countries where they live.

It is obvious that the problem needs to be addressed by IT security experts and law enforcement agencies in the countries where the perpetrators presumably reside, not only in those countries where their crimes are perpetrated. Security solutions can simply block the threats on user devices, but the criminals will simply find other victims who are not so well protected. The only thing that can stop them is the involvement of law enforcement organizations.

To avoid falling victim to cybercriminals involved in distributing mobile malware, Kaspersky Lab and INTERPOL experts recommend the following security measures:

For individual users:

- Protect your Android devices with secure passwords to prevent attackers from accessing personal data by stealing your device and brute-forcing the password.

- Unblocking the option that enables apps from third-party sources to be installed on the device is not a good idea. As a rule, Google Play, which is the main distribution channel for Android apps, carefully verifies the software it distributes. Even if you

need to use a third-party application for some reason, be sure to block this option again after installing the app.

- Antivirus software developers often create applications designed to test devices for unclosed vulnerabilities. Such applications are regularly updated to include data on newly-discovered vulnerabilities. We recommend using these apps once in a while.

- Use a security solution on your device and make sure it scans files as they are downloaded and protects the device from other types of Internet attacks. Although Android malware has not so far been as widespread as malicious software targeting PCs this thought is unlikely to comfort you if you fall victim to mobile malware.

- When conducting banking transactions, be sure to use two-factor authentication. Ideally, temporary codes used to access your bank account should be sent to a different phone from the one from which you connect to online banking. Using simple devices with no smartphone features for this purpose is recommended, since this minimizes the chances of these devices being infected with a banking Trojan. And, generally, it is a good idea to use two-factor authentication wherever possible.

- You should use encryption if you have any valuable information (financial, personal or work-related) on your device. Then, even if your device is stolen, the attackers won't be able to access your data.

- If you believe that you may have fallen victim to or witnessed a cybercrime, do not hesitate to contact law enforcement as soon as possible. In most countries, creating and distributing malware or stealing personal information is a crime that is investigated by dedicated law enforcement agencies.

For corporations:

- The Bring Your Own Device approach, which allows employees to use their personal devices for work, can expose your company to virtually all 'consumer' IT security risks: sensitive corporate data stored on an employee's personal phone could be a valuable find for cybercriminals. A security solution with Mobile Device Management capabilities, including encryption and remotely wiping data from smartphones, will help you to keep your sensitive business-related information secure.

- If your employees are not aware of simple IT security rules, this is likely to cause security incidents. This is why, in an environment where nearly all the employees have Internet-enabled devices, training people to handle their mobile devices appropriately will be a worthwhile investment.

  Be sure to contact law enforcement and expert organizations in the event of an IT security incident. Many companies keep information about incidents secret for fear of reputational losses and do not initiate investigations into cybercriminal activities. However, a cybercriminal who escapes prosecution is free to come back and cause even greater damage in future.

For law enforcement and regulatory agencies

- There are many highly-qualified experts in digital forensics and malware analysis, whose participation in cybercrime investigations could speed up the process of collecting evidence and searching for suspects and make it more effective.

- Today, cybercriminals launch attacks against people in other countries without fear, taking advantage of the many jurisdictional issues that beset international multi-jurisdictional investigations. The more effectively cyber police forces of different countries work together, the harder it will be for cybercriminals to avoid liability.


INTERPOL


KASPERSKY