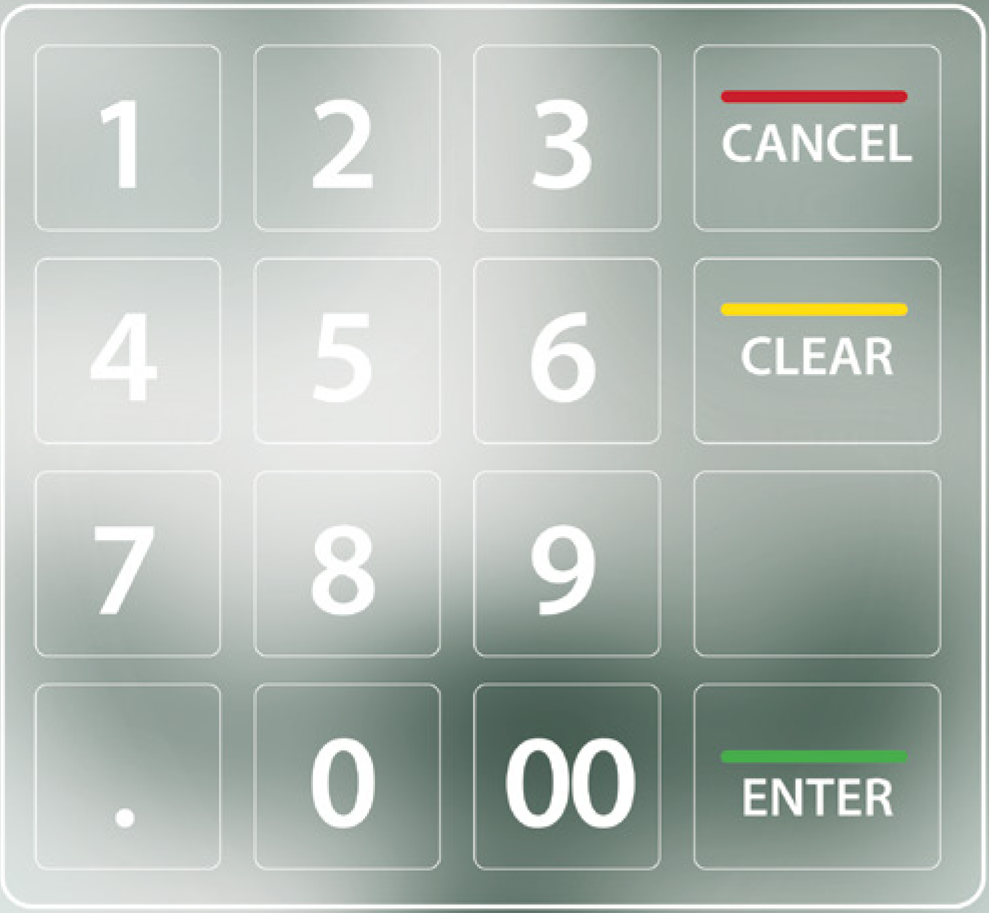
KASPERSKY LAB REPORT

Financial cyber threats in 2013



April 2014

KASPERSKY lab

▶ TABLE OF CONTENTS

▶ INTRODUCTION

Money and risks in a multi-device world

It has been quite a few years since cybercriminals started actively stealing money from user accounts at online stores, e-payment systems and online banking systems. However, for much of that time the financial fraudsters' sphere of activity was restricted by a number of factors, in particular the relatively limited scope of electronic payment tools.

In recent years, electronic money has been growing in importance. The convenience and universal accessibility of electronic payment systems and online banking services attract huge numbers of users, and in many countries banks and financial institutions are seriously considering the complete discontinuation of cash flow in favor of cash-free payments. A 2013 survey conducted by B2B International in cooperation with Kaspersky Lab also demonstrates the growing popularity of digital payments: 98% of those polled say they regularly use online banking or payment systems, or shop online.

This increasing popularity of cash-free transactions is accompanied by growing numbers of devices on which financial transactions can be made. As demonstrated by the same survey, PCs and laptops are still the "main" devices from which users access financial services: 87% of respondents said they conduct operations involving electronic money using a desktop or laptop computer. However, the share of mobile devices used for the same purposes is substantial: 22% and 27% of those polled respectively use tablets or smartphones for some financial operations.

Of course, these trends attracted unwanted attention. The dramatic growth in the number of users of all types of payment systems has attracted cybercriminals, and they are investing ever-growing resources into fraud schemes with which they can first gain access to users' financial data and then to their actual money. Although financial attacks are among the most complicated and expensive types of attacks, they are also highly lucrative because, once successful, they provide direct access to the victims' money. Once an online banking account is accessed, all that remains is to take the money and cash it in, whereas a malware writer or the owner of a botnet designed to launch DDoS attacks or send spam still has to find clients to buy their services.

For over 16 years, Kaspersky Lab has developed tools to protect against all types of cyber attacks, including financial attacks. The development of such technologies is impossible without routine detailed analysis of new malware samples, social engineering methods and other tools used by cybercriminals involved in financial fraud. One of the most general conclusions that can be drawn from this analysis is that, unlike many other types of attacks, financial malware attacks typically incorporate a highly diverse set of instruments – from phishing pages imitating the legitimate websites of financial institutions, to exploiting vulnerabilities in popular software and the writing of customized malicious programs.

Since financial cyber attacks are complex, an analysis of how they impact user security requires a comprehensive approach. That's why when preparing this report, Kaspersky Lab's experts considered Windows threats alongside threats targeting OS X and Android; "specialized" malware as well as other programs that are potentially capable of stealing financial data; and not only the spread of dangerous Trojans but also phishing attacks that can be an effective tool to coax valuable financial data from unwary users. In Kaspersky Lab's view, this comprehensive approach is the only way to achieve the goal of this study, which was to give the broadest possible picture of the cyber-threat landscape aimed at online finances, and to attempt to evaluate the magnitude of the danger that such cyber threats pose.

▶ METHODOLOGY OF THE REPORT

The study used de-personalized data obtained from Kaspersky Security Network.
The Kaspersky Security Network is a globally distributed cloud-based infrastructure designed for the real-time processing of data about threats that Kaspersky Lab users encounter. Kaspersky Security Network was created to ensure that information about the most recent threats is delivered to Kaspersky Lab product users as quickly as possible. With this network, an information for a new threat is added to databases within minutes of a previously unknown threat being discovered. KSN's other function is to collect depersonalized statistics about threats which land on user computers. It is each user's voluntary decision to provide their information to KSN. Data received in this way was used as the basis for this report.

The researchers studied data about the number of times Kaspersky Lab components successfully protected against phishing (under Microsoft Windows and Apple OS X), malware (under Windows) and mobile malware (under Google Android). In addition it looked at statistics about the number of users attacked. The research also analyzes information about the geographic spread of the attacks and their intensity.

The research covers the entire year of 2013; the data is analyzed in comparison to the equivalent data collected in 2012. The main subject of the research is the targets of phishing campaigns: the number of blocked attempts to download fake sites of payment systems, online banking systems, online stores and other targets associated with financial institutions. In addition, Kaspersky Lab's experts selected a few dozen malware samples created specifically to steal financial data, and analyzed how frequently they were observed "in the wild" during the research period.

As the crypto-currency Bitcoin became extremely popular in 2013, Kaspersky Lab's experts separated threats associated with the generation and stealing of this currency into a separate category, and followed their evolution.

According to the information collected from the protection sub-systems of Kaspersky Lab products, 2013 saw a dramatic increase in the number of finance-related attacks, be it phishing or attacks involving malware.

Below are the main findings of the research.

▶ MAIN FINDINGS

Phishing

- 31.45% of all phishing attacks in 2013 targeted financial institutions
- 22.2% of all attacks involved fake bank websites; the share of banking phishing doubled compared with 2012.
- 59.5% of banking phishing attacks exploited the names of just 25 international banks. The rest of the attacks used the names of 1000+ other banks.
- 38.92% of all instances that required intervention by Kaspersky security technologies on Mac computers were triggered by “financial” phishing sites.

PC Malware

- In 2013, of all Internet users who encountered some sort of malware attack, 6.2% encountered financial attacks involving malware. This was an increase of 1.3 percentage points compared to 2012.
- In 2013, the number of cyber attacks involving malware designed to steal financial data rose by 27.6% to reach 28,4 milion. The number of users attacked by this financial-targeting malware reached 3,8 million, which is an 18.6% increase year on year.
- Among all finance-related malware, tools associated with Bitcoin demonstrated the most dynamic development. However, malware for stealing money from bank accounts, such as ZeuS, still plays the leading role.

Mobile malware

- In Kaspersky Lab’s malware sample collection, the number of malicious Android applications designed to steal financial data rose almost fivefold in the second half of 2013, from 265 samples in June to 1321 in December.
- In 2013, Kaspersky Lab’s experts first discovered Android Trojans that were capable of stealing money from the bank accounts of attacked users.

Further on in the research text, we will discuss in more detail how attacks develop over time, look at their geographical distribution, and see the lists of their targets.

▶ PART 1

Phishing threats

Phishing, or creating fake copies of sites to obtain confidential user data, is a very common cyber threat. This is largely due to the fact that to deploy the simplest phishing campaign, cybercriminals do not need to have specific programming knowledge – it's enough to have certain skills in creating web pages. The main purpose of phishing is to convince the victims they are visiting a real site, not a fake one. These attempts are often successful so phishing campaigns are used both as the main tool to obtain sensitive user information and as part of a complex attack to lure users to a site from which malware will be downloaded on to their device.

According to our study, phishing pages are frequently used in cyber attacks aimed at stealing user financial data. However, before proceeding to the detailed analysis of these attacks it would be helpful to present the general picture of phishing threats in 2013.

Phishing: overall situation

Attacks and users

Kaspersky Lab protection products have four sub-systems to combat phishing attacks. Phishing databases (similar to the malicious file signature databases) are stored on user devices and contain a list of the most common phishing links active when the database was released. The second sub-system is an anti-phishing cloud database that Kaspersky Lab protection products consult if a user notices a suspicious link that has not yet been included in the local anti-phishing database. The cloud database is updated faster than the local ones and is designed to detect the very latest phishing attacks.

Kaspersky Lab products also integrate two automatic systems for detecting phishing links and pages: Mail anti-phishing and Web anti-phishing. Mail anti-phishing monitors the links in users' emails if they work with one of the popular email clients (Microsoft Outlook, etc.). Web anti-phishing checks everything that appears in the users' browsers, utilizing a set of heuristic rules, and is capable of detecting new phishing pages even if there is no information about them in any database.

For this report, Kaspersky Lab used just the data obtained from Web anti-phishing because this is generally only called upon when information about a new phishing page is missing from Kaspersky Lab's databases. Moreover, it makes it possible to determine the target of the phishing attack.

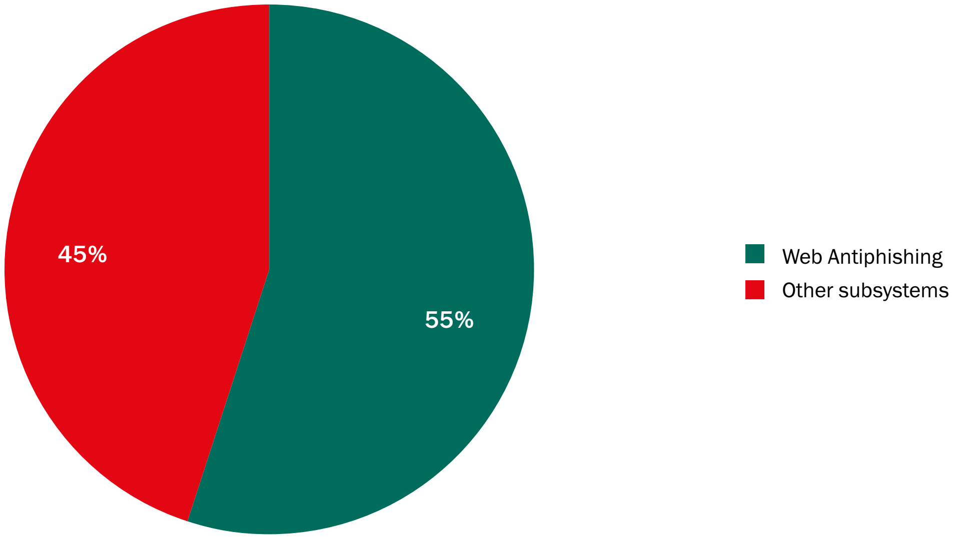
According to Kaspersky Lab, in 2013 about 39.6 million users faced phishing attacks, an increase of 2.32% from 2012.

Over 600 million notifications about the phishing links and pages encountered by our users arrived from all four Kaspersky Lab anti-phishing sub-systems. In 2012 this figure was almost the same. At the same time the number of attacks blocked by heuristic Web anti-phishing increased by 22.2% over the same period – from **270 million** in 2012 to about **330 million** in 2013. This may be due to the constant improvements made to the heuristic detection system.

Geography of attacks

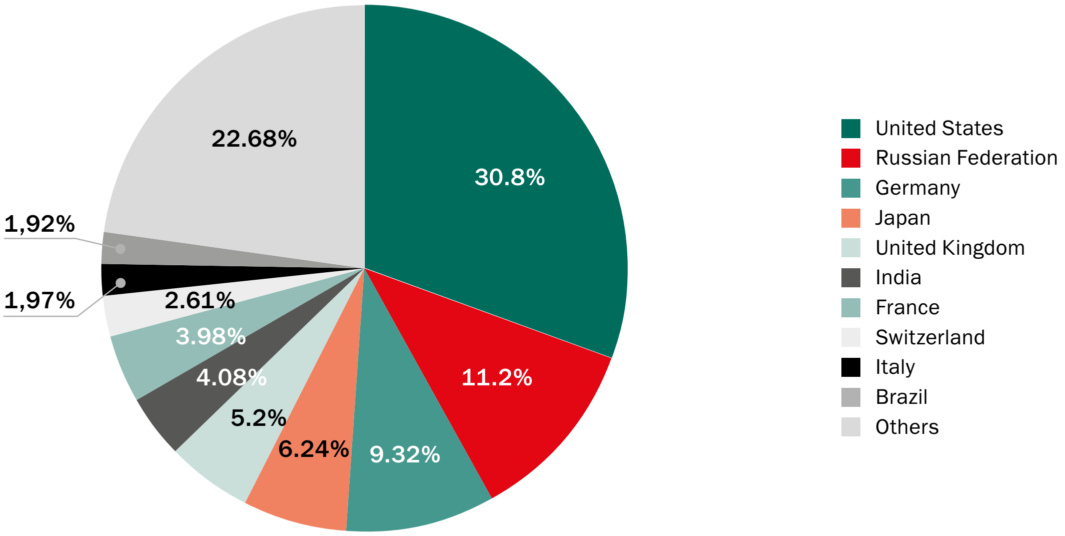
In 2013, the majority of phishing attacks blocked by Kaspersky Lab (30.8%) targeted users in the USA. Second came Russia (11.2%) followed by Germany (9.32%).

Web anti-phishing share in overall number of detects in 2013



Most frequently attacked countries in 2013

Here and below, the data is provided by Kaspersky Security Network



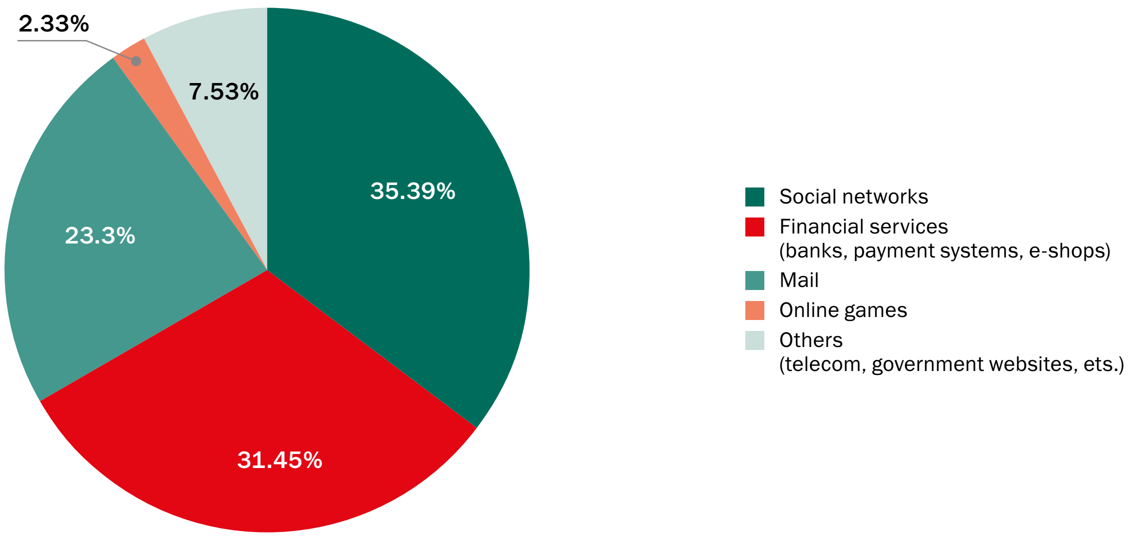
Compared to the previous year, in 2013 the list of the most frequently attacked countries saw significant changes. For example, the share of attacks on Russian users declined by 9.19 percentage points while the percentage of attacks on users in the USA increased considerably – from 17.56% in 2012 to 30.8% in 2013. The proportion of attacks on German users also grew by 3.49 pp, from 5.83% to 9.32%.

There could be several reasons for this geographical distribution. We have already seen a reduction in the amount of attacks in some countries and increases in other countries. The decline might be the result of such factors as enhancing measures to combat cybercrime, more complex domain name registration procedures, etc. The growth may be triggered by a «natural» increase in the total number of Internet users and individual Web resources: social networking sites, Internet stores, etc. The more often people download web pages, the more likely they are to encounter phishing pages.

Targets

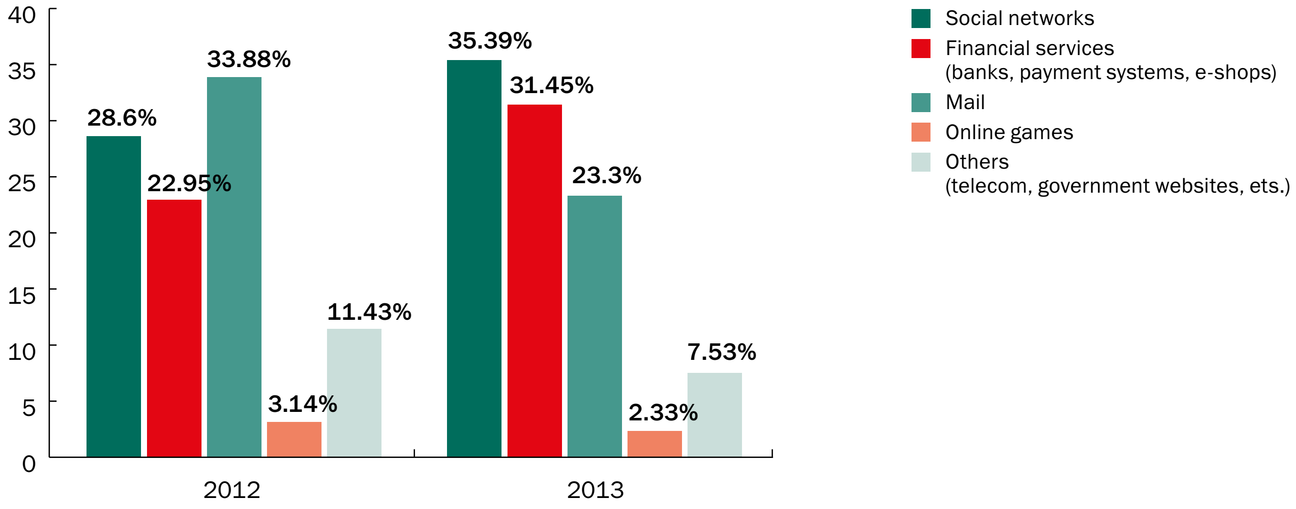
As seen from the chart below, the majority of attacks in 2013 mimicked social networking sites – about 35.4%. Financial and phishing targets – fake banking sites, payment systems and online stores – accounted for 31.45%. Mail services came third with 23.3% of attacks.

Phishing targets in 2013



Noticeably, in comparison with 2012, the distribution of targets by type changed significantly in 2013. The share of attacks using fake social networking pages increased by 6.79 pp and reached 35.39%, while the percentage of financial attacks grew by 8.5 pp and accounted for 31.45%. At the same time, the proportion of attacks exploiting fake websites of mail services decreased by 10.5 pp to 23.3% and online games dropped from 3.14% in 2012 to 2.33% in 2013.

Phishing targets in 2012 and 2013



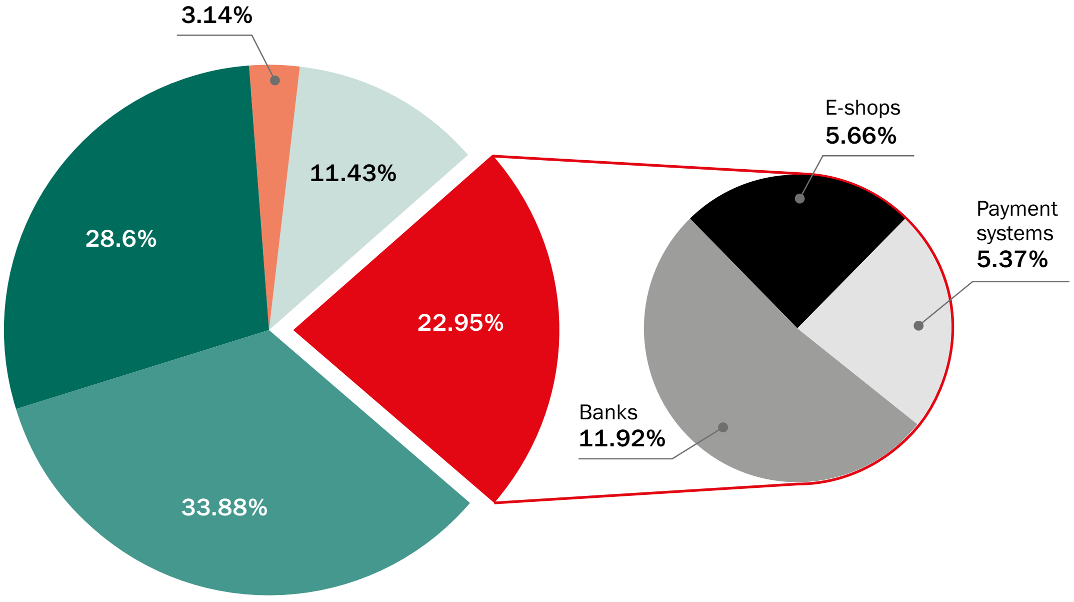
Financial attacks demonstrated the most notable growth in 2013 compared to 2012, which gives rise to a more detailed analysis of the dynamics of such attacks.

Phishing: financial attacks

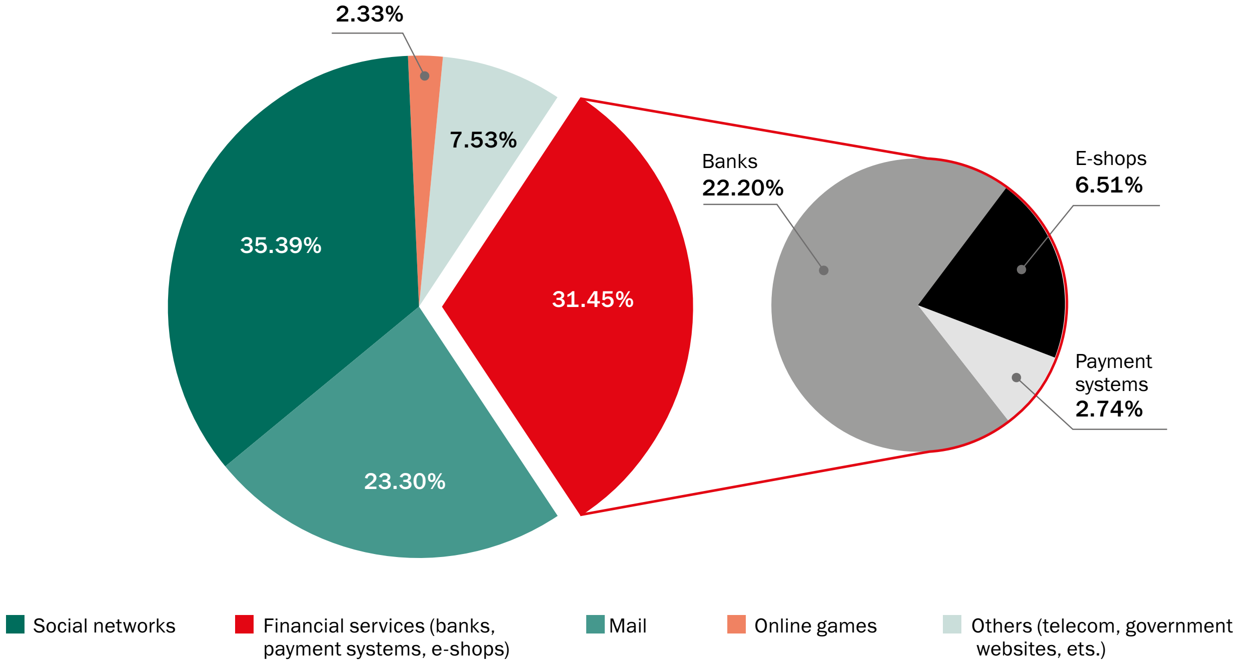
Worrying trend

In 2012, 22.95% of all phishing attacks targeted financial services of one kind or another: 11.92% of all attacks were performed using fake bank and online banking sites, 5.66% targeted online stores, and 5.37% targeted payment system sites.

Financial phishing in 2012



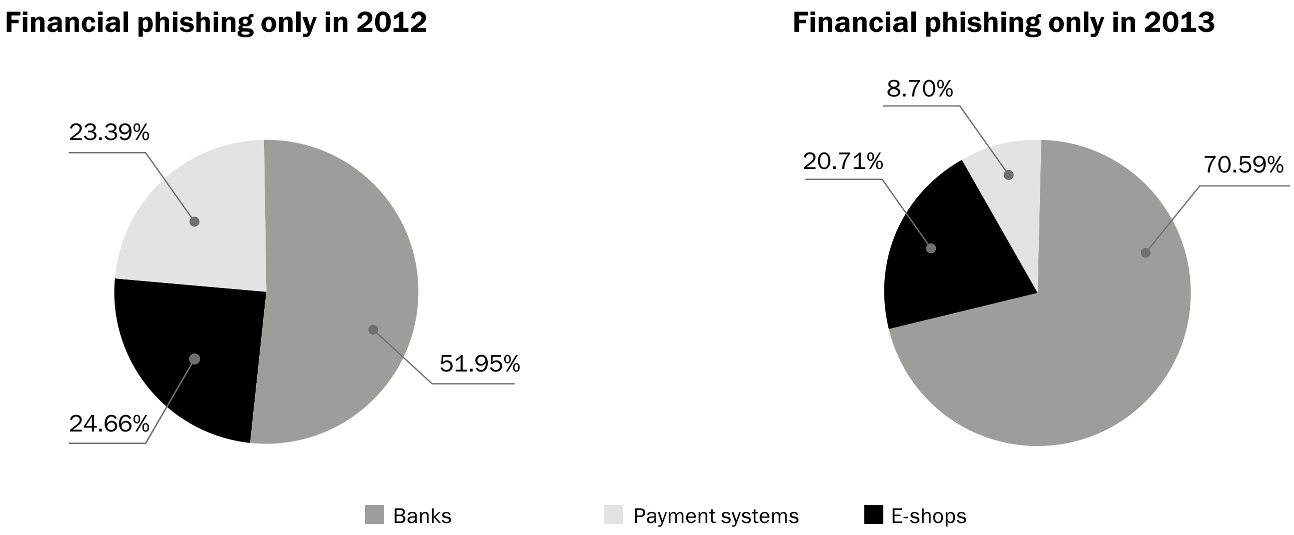
Financial phishing in 2013



However, in 2013 the distribution of attacks within the ‘Online Finance’ category changed dramatically. The percentage of phishing targeting banks almost doubled and reached 22.2%. The share of online stores increased insignificantly – from 5.66% to 6.51% – while the proportion of payment systems dropped by 2.63 pp. The conclusion here is obvious: the attackers are increasingly focusing on bank web services and this is one of the strongest trends in the area of phishing threats.

The trend is even more clear-cut when financial phishing is separated from the other categories. In 2013, fake bank pages made up 70.59% of all Kaspersky Lab Web anti-phishing detections in the Online Finance category, but one year earlier the share of bank phishing was only 51.95%.

The percentage of attacks on online stores decreased from 24.66% in 2012 to 20.71% in 2013 while the proportion of attacks on payment systems fell from 23.39% to 8.7%.


Financial phishing only in 2012

Financial phishing only in 2013

A closer look at financial phishing targets

Banks

Although Kaspersky Lab anti-phishing databases contain more than a thousand names of banks that have been attacked or are at risk of being attacked due to their popularity, the vast majority of all phishing attacks using fake bank pages exploited the names of just 25 organizations.

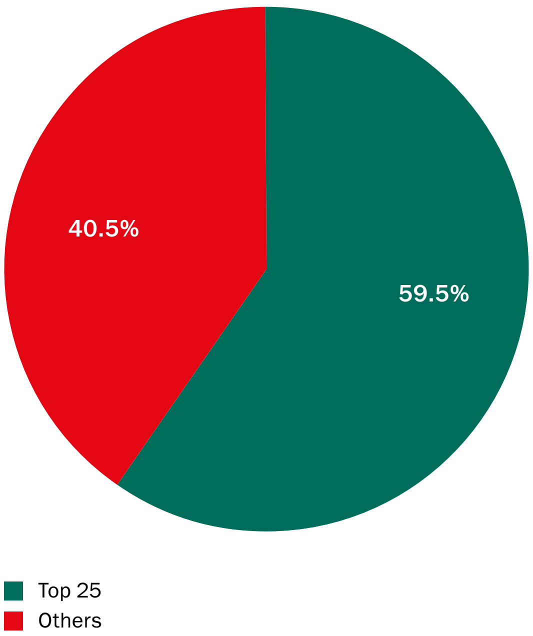
In 2013, these 25 banks attracted about 59.5% of all «bank» attacks. However, most of these organizations are the largest international banking brands, operating in dozens of countries worldwide. Widespread brand recognition is one of the main tools of the phishers: the more popular the brand, the easier it is for cybercriminals to use its name to lure users to a fake website.

Payment systems

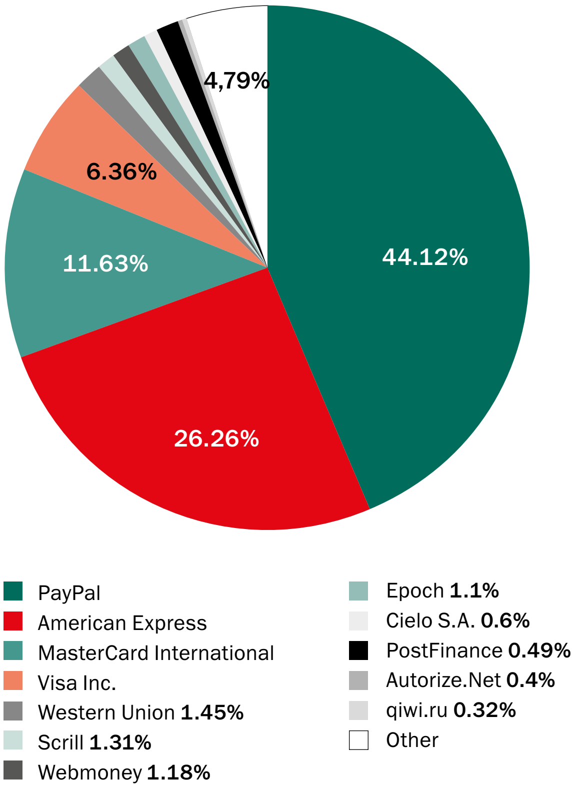
As with attacks on banks, the distribution of attacks on payment systems largely depends on brand awareness – almost 90% of phishing attacks in this category fell on one of five international brands: PayPal, American Express, MasterCard International, Visa or Western Union.

PayPal, being an extremely popular system for making online payments, is equally popular with hackers – the amount of attacks on this system reached 44.12%.

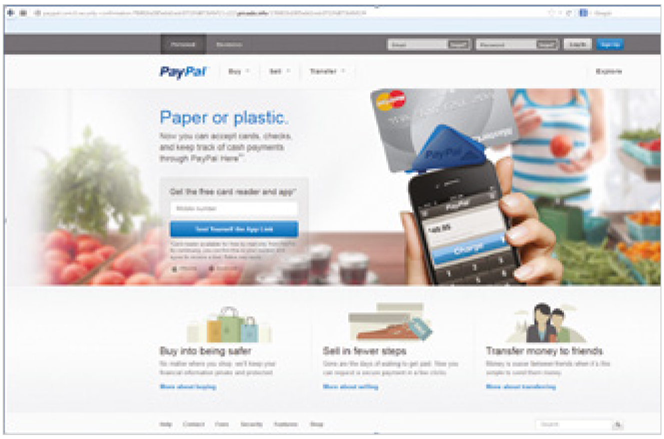
Attacks against banks in 2013



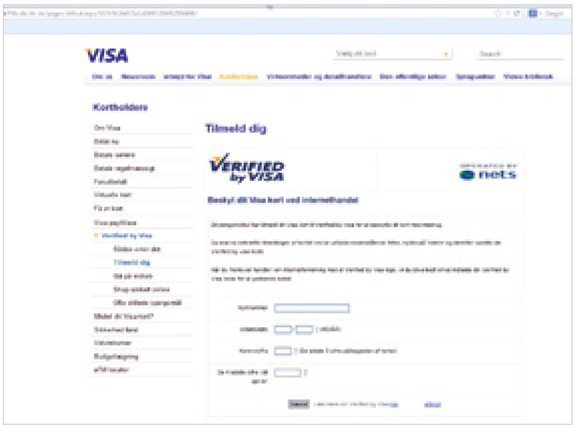
Attacks against payment systems in 2013



An example of a phishing page imitating the PayPal website



An example of a phishing page imitating the Visa website

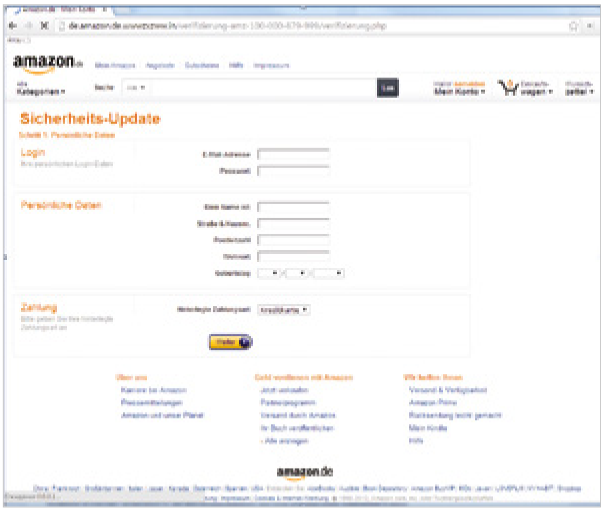


A significant proportion of attacks imitated American Express – 26.26%. MasterCard International and Visa Inc. pages are targeted much less often: these systems accounted for 11.63% and 6.36% of attacks respectively.

Online shops

For several years in a row Amazon.com (61.11% in 2013) has been the most popular cover for phishing attacks in the Online Stores category.

An example of a fake Amazon page targeting users in Germany



Sicherheits-Update

Login

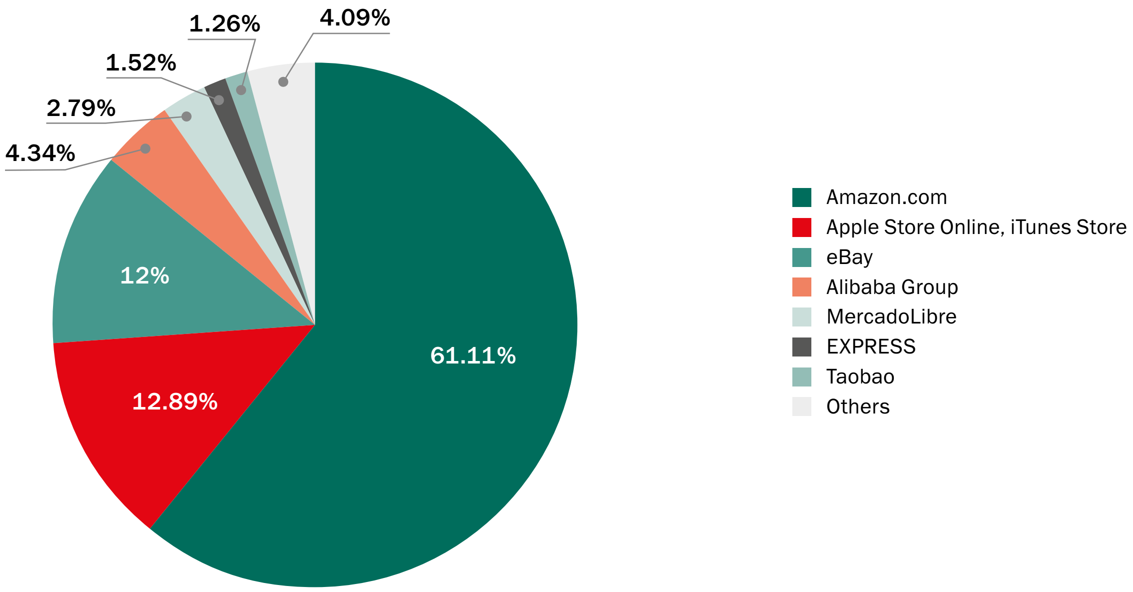
Persönliche Daten

Zahlung

As the world’s largest online store, offering a wide range of goods, Amazon is familiar to many users. Therefore, it is popular with fraudsters who create fake pages.

A significant proportion of attacks (12.89%) use the Apple brand name. Generally, the attackers try to imitate the pages of online stores selling Apple devices as well as App Store and iTunes Store.

Attacks against online shops in 2013



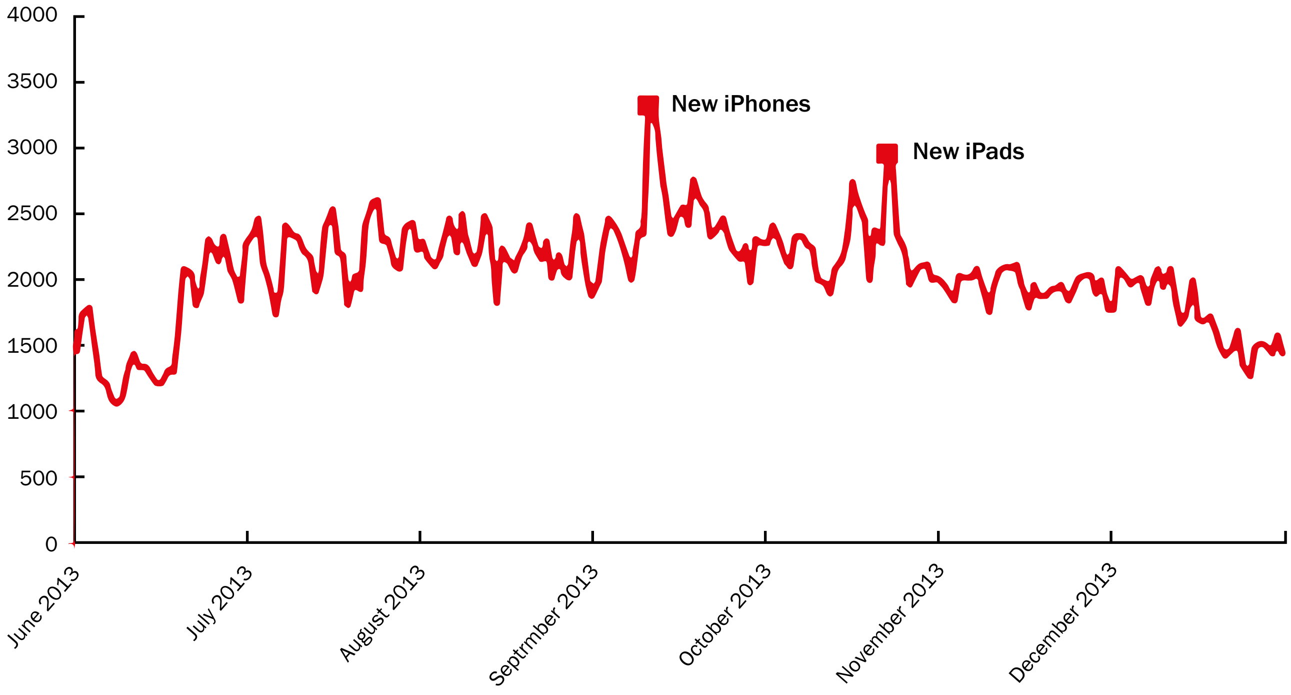
Among the traditional phisher targets is the Internet auction site eBay (12%), and the Chinese online store Alibaba (4.34%) is becoming increasingly attractive for scammers. In 2013 it was joined by another Chinese online store – Taobao (1.26%). Almost 3% of all attacks on online stores fell on MercadoLibre.com, a South American version of eBay. The diagram above illustrates the «international» character of financial phishing. As can be seen, the victims of attacks are not only English-speaking users but also people who speak Chinese, Spanish, Portuguese, and several other languages.

Deeper into the dynamics of attacks

The professional and marketing activities of the companies that are exploited in phishing schemes also affects the number of attacks.

This trend can be illustrated by the graph of attacks which exploited the Apple brand name.

Attacks exploiting the Apple brand name in the 2nd half of 2013



Over the year, the dynamics of Kaspersky Lab security technology detections of threats that exploit Apple's trademark had been a series of peaks and troughs ranging from 1 to 2,500 operations per day. However, as seen from the chart above, there were two noticeable peaks which coincided with the date iPhone 5s and 5c were announced on 10 September 2013 and the announcement of iPad Air and iPad Mini with retina-display on 22 October 2013.

The logic in this case is clear: Apple devices are always a hot topic for news and discussion on the Internet, particularly when a new product is about to be released. For the fraudsters, using «hot» keywords is the usual way of attracting audiences to fake sites and, as the graph shows, this method works.

Apple is not the only phisher target that shows a correlation between the number of attacks and the company's activities. Natural disasters and high-profile international events attract active coverage and discussion in the media and on the Internet, giving rise to the emergence of so-called thematic phishing and spam. Similarly, large-scale marketing campaigns held by a bank, an e-store or other commercial or financial organizations may become a pretext for phishing

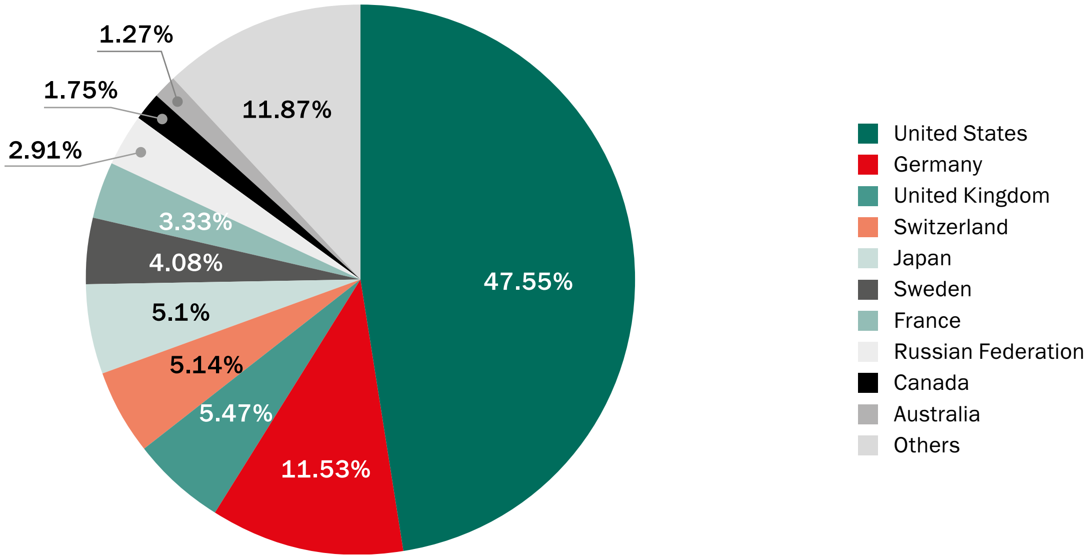
The logical conclusion for banks, payment systems and other financial institutions regularly conducting online marketing activities is simple: when initiating an advertising campaign to attract new business, don't forget to warn customers about potential cyber threats.

Phishing against OS X: first signs of a growing threat

The number of malicious attacks on the owners of computers running OS X has always been significantly lower than the number of attacks on Windows users. This can be easily explained: although Apple actively promotes its Mac computers and laptops all over the world, the number of users of these devices is a long way short of the number of computers running under Windows. Since criminals are keen to maximize their profits, they naturally pay more attention to Windows users. However, this statement is only valid when it comes to malware. The attacker does not need to do anything special to attack a Mac user via phishing: although Windows and OS X have fundamental differences which make it impossible to write «universal» malicious programs for both platforms, the users of both PCs and Mac download the same web pages and phishing threats which spread with the help of social engineering techniques are as dangerous for Mac users as they are for Windows users. The results of Kaspersky Lab's study confirm this fact.

However, it should be noted here that for technical reasons Kaspersky Lab only became capable of collecting relevant statistics from Mac users in November 2013 and all Mac-related information in this study was harvested in November and December 2013. Although the observation period is short, the data obtained provides some insight into the landscape of threats jeopardizing OS X users and helps to define differences compared with the overall picture.

Most frequently attacked countries: Mac users



In 2013, 7.8% of Kaspersky Lab anti-phishing detections protected Mac computers. Almost half of these attacks targeted US users (47.55%); 11.53% of attacks were registered in Germany and 5.47% in the UK. The list of the most frequently attacked countries also included Sweden and Australia.

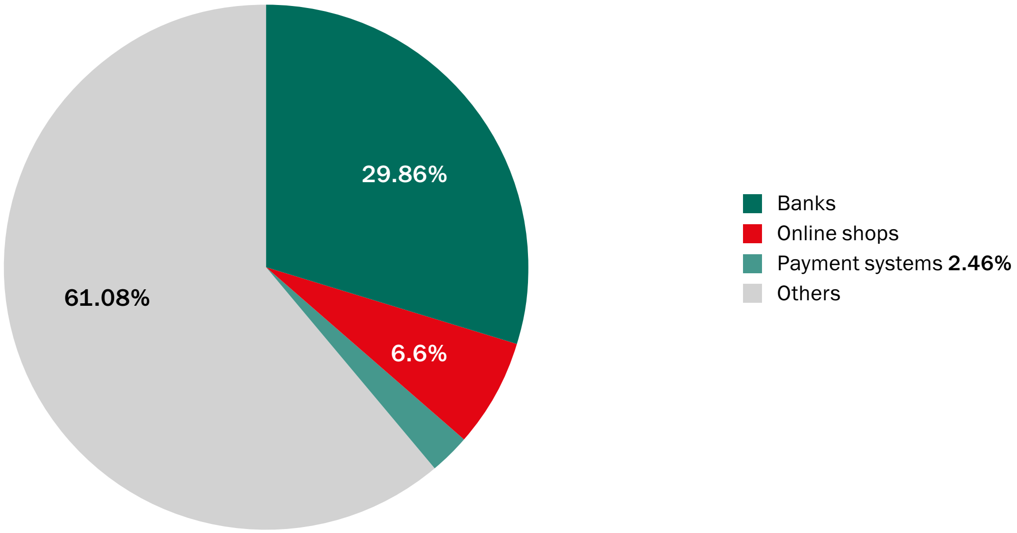
The differences in the distribution of attacks by country can be explained by the relative use of Apple computers in these countries. Traditionally, the USA and the developed European countries are the largest markets for Apple devices.

Targets

Mac owners faced phishing attacks as often as the users of computers running Windows, but their chances of becoming a victim of a financial attack are even greater.

Over the reporting period, about 38.92% of all Kaspersky Lab anti-phishing detections on Apple computers involved «financial» phishing pages. That is almost 7.5 percentage points more than the «financial» share of the total volume of attacks. 29.86% of the total number of attacks occurred when users were trying to enter fake bank sites; online stores and auctions accounted for 6.6%, while payment systems accounted for 2.46% of all anti-phishing detections.

Financial phishing: Mac



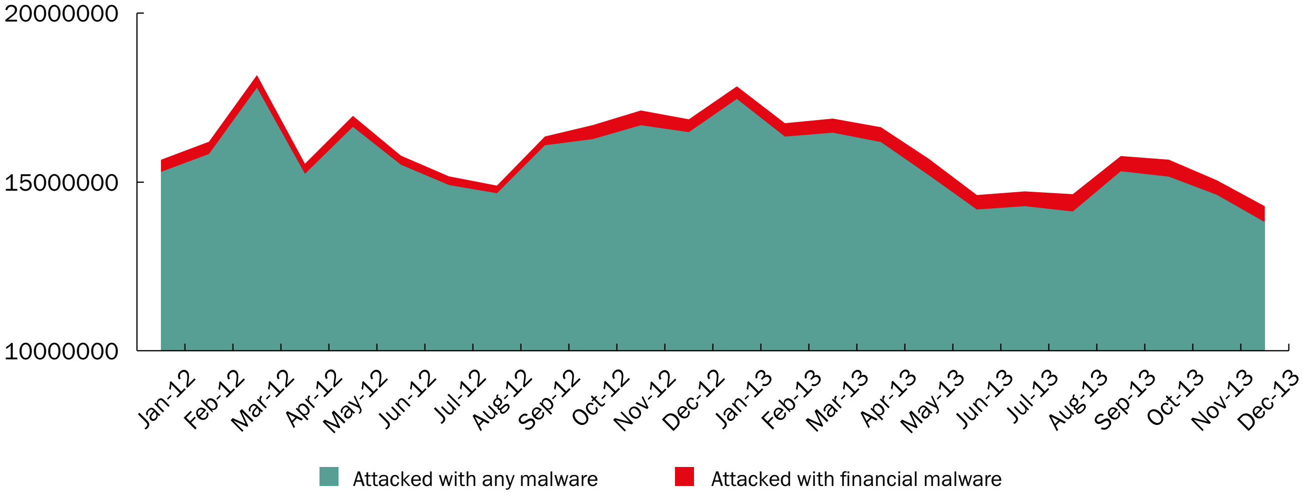
That was the view Kaspersky Lab's experts took on financial phishing in the year 2013. Although phishing is a fairly common threat, when it comes to financial cybercrime it forms a relatively small part of the overall landscape of financial cyber threats. The key role here is played by financial malware, dangerous software capable of obtaining user details to access online accounts and steal the victim's money. This will be discussed in the next part of the Kaspersky Lab report.

PART 2

Financial malware

Programs designed to steal e-money and financial data are among the most complicated types of malicious software out there today. They enable cybercriminals to quickly generate cash from their creation, so malicious users spare no effort or expense in developing financial Trojans and backdoors. Kaspersky Lab experts have noted that malware writers are even prepared to pay tens of thousands of dollars for information about new vulnerabilities – the first coder to get around a product's security systems leaves all the criminal competition in the dust.

In 2013, Kaspersky Lab detected 28.4 million attacks using financial malware, 27.6% more than the number of detections in 2012. The number of users targeted in attacks involving financial malware also rose 18.6% to 3.8 million.

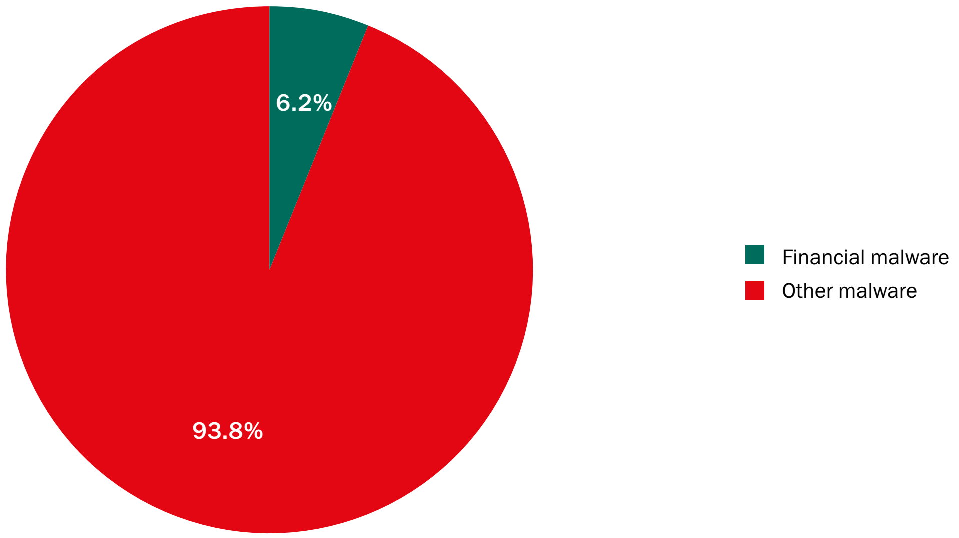


The number of users targeted by malware over the past year has dropped although the percentage of those who have encountered financial threats has been steadily rising over the past two years.

Malware designed to steal data and commit fraud was involved in a relatively small percentage of attacks (0.44% in 2013), although that is still 0.12 percentage points higher than the year before. However, when it comes to the number of affected users by financial cyber threats, the percentage is much more substantial: among the total number of users subjected to all types of malware attacks, 6.2% of those attacks involved some kind of financial threat – that's 1.3 percentage points higher than in 2012.

* The study factored in data about attacks using banking Trojans and keyloggers to steal from Bitcoin wallets and then download software to generate that crypto-currency

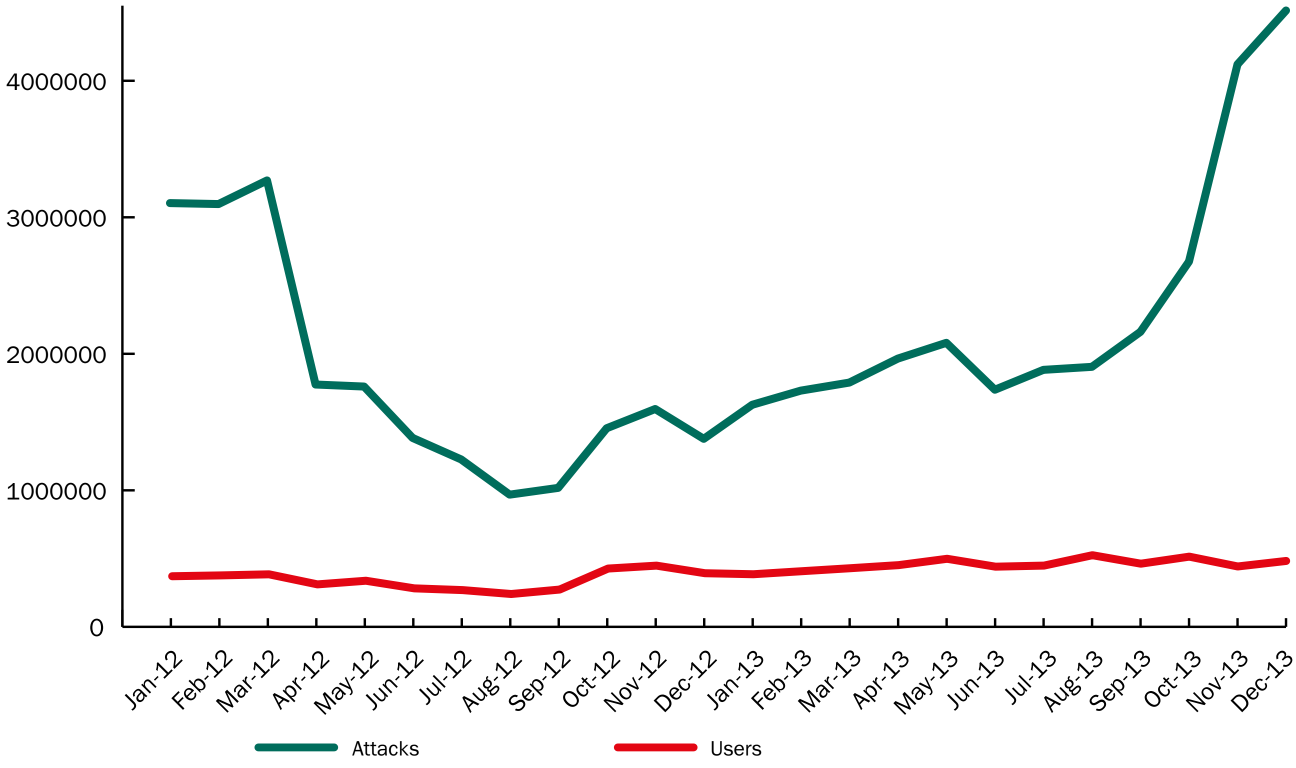
Users attacked in 2013



In 2013, financial malware affected 6.2% of the total number of users targeted in malware attacks.

There is a weak correlation between the number of attacks and the number of users targeted. In 2012-2013, the monthly number of attacks varied by tenths of percentages. In spring 2012, it dropped sharply and did not climb back up to its previous position until autumn 2013, although the number of users attacked did not undergo any significant fluctuations and more or less continued to grow on a monthly basis.

Financial malware: attacks and attacked users in 2012-2013



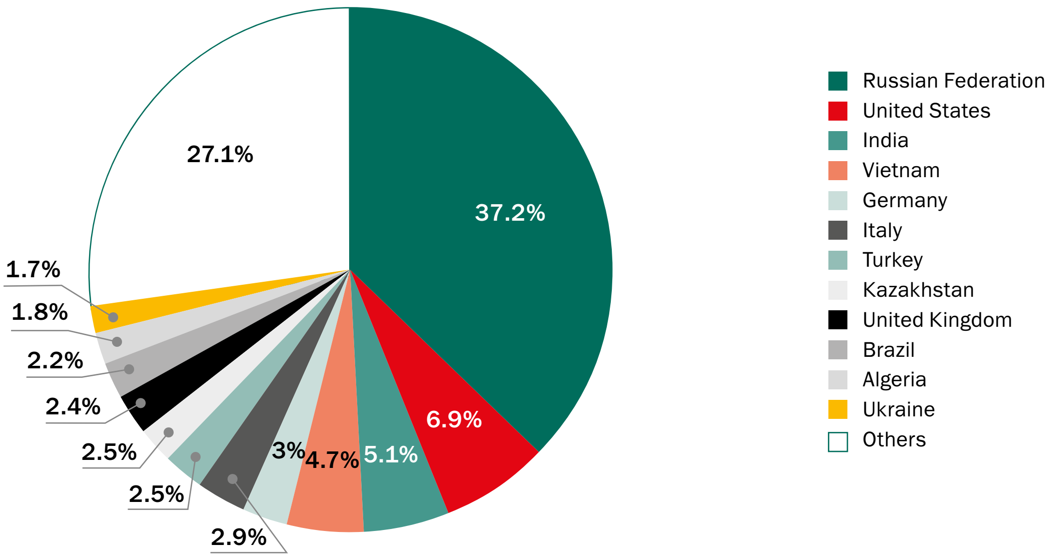
The number of users targeted in attacks involving financial malware increased over 2013.

The drop in the number of attacks observed in spring 2012 might be linked to the shutdown of several cybercriminal groups. In turn, the surge in attacks seen in the last six months of 2013 can be explained by several factors: malicious users discovered new vulnerabilities in Oracle Java, which made it possible for them to launch more attacks. Furthermore, following a rise in the Bitcoin exchange rate near the end of the year, we saw more programs designed to steal the crypto-currency from user e-wallets.

Threat borders: geography of attacks and attacked users

The country most frequently targeted by financial malware in 2012-2013 was Russia, with over 37% of all attacks. No other country had a percentage exceeding 10% over the reporting period.

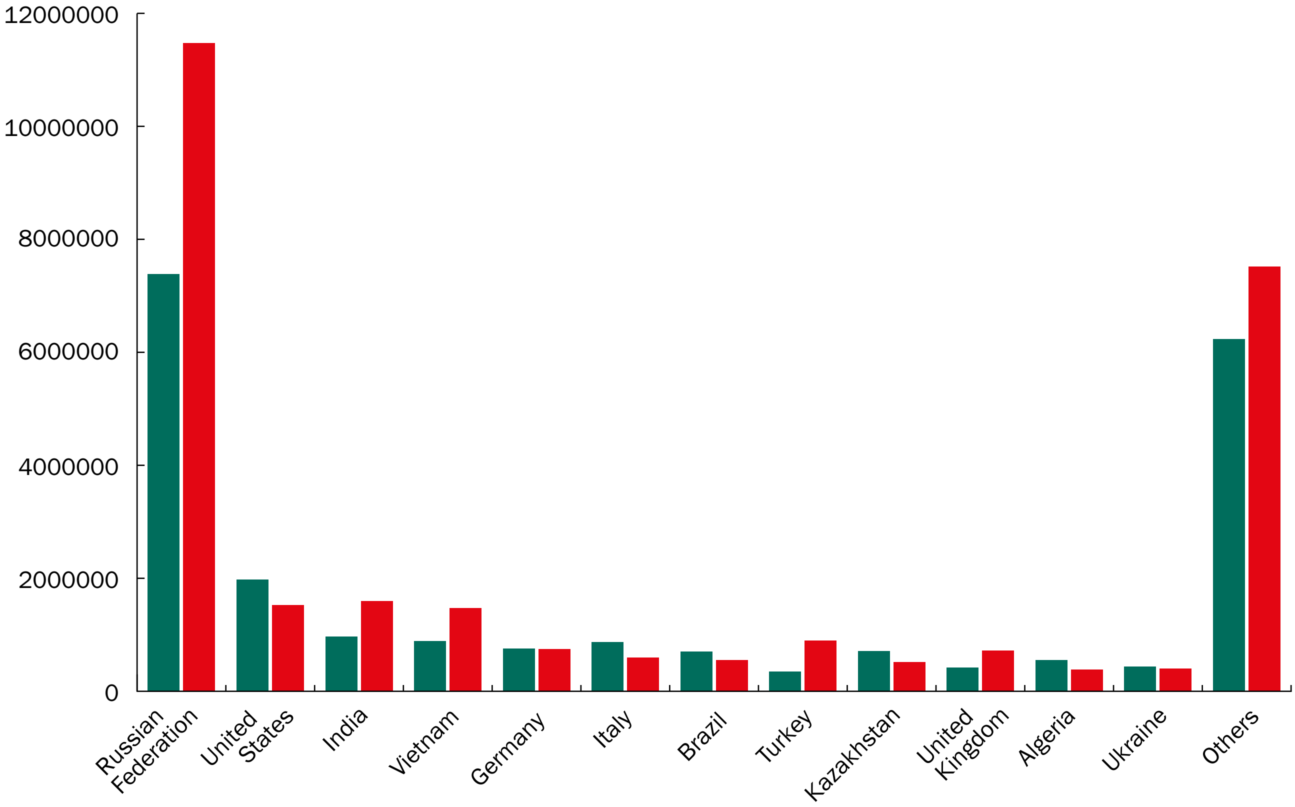
Most frequently targeted countries in 2012-2013



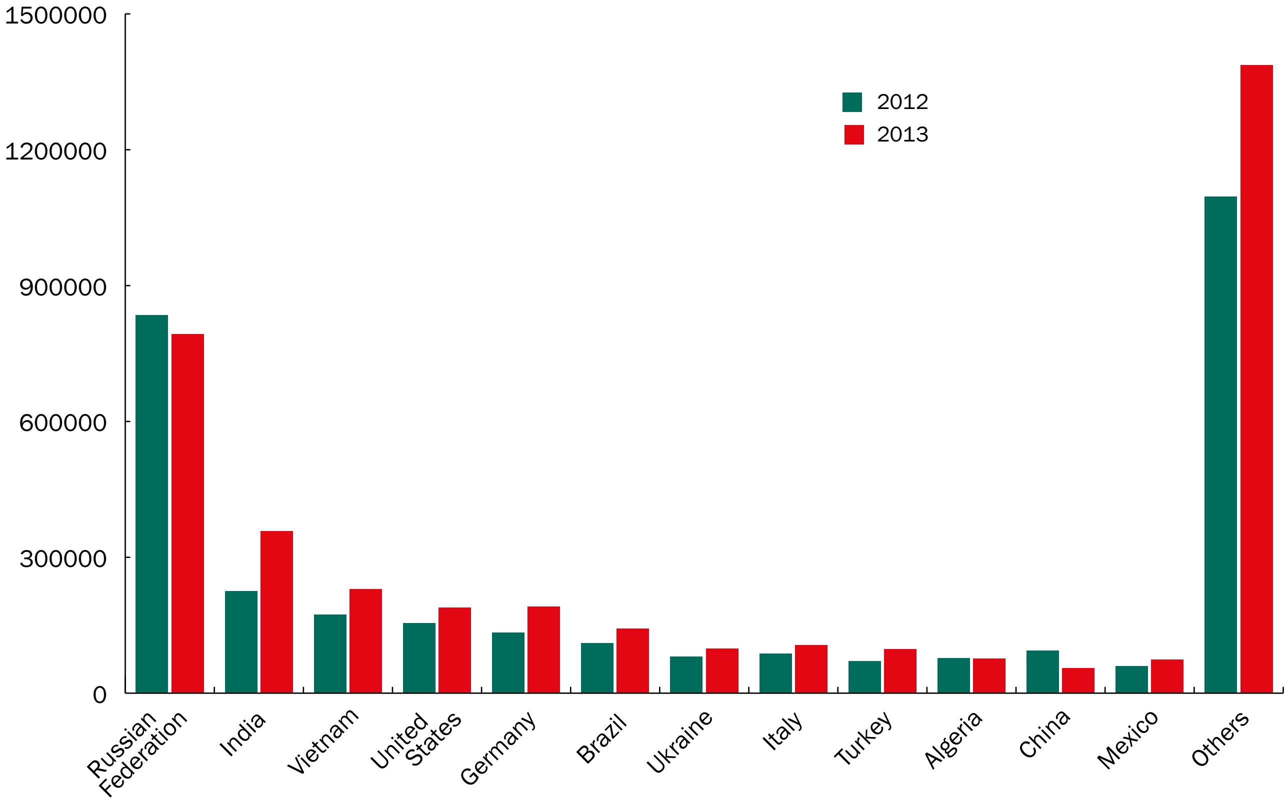
The Top 10 most frequently attacked countries were on the receiving end of 70% of all financial malware attacks over the past two years.

Russia was also the top country when it came to the number of attacks in one year. While the number of users targeted in Russia fell only slightly in 2013, most other countries in the Top 10 saw that number rise.

Financial malware attacks around the world



Users targeted by financial malware, by country



The number of users attacked by financial malware over one year increased in eight out of the Top 10 most frequently targeted countries.

Users in Russia faced the highest risk of becoming a victim of financial malware: in 2013, each individual targeted by cybercriminals specializing in financial malware was attacked 14.5 times on average – compare that to the average of just over eight times per year for residents of the United States.

Country	Number of attacks involving financial malware	Year-on-year change	Average number of attacks per user
Russian Federation	11,474,000+	55.28%	14.47
Turkey	899,000+	156.41%	9.22
United States	1,529,000+	–22.76%	8.08
Vietnam	1,473,000+	65.08%	6.43
Kazakhstan	517,000+	–26.88%	6.15
Italy	593,000+	–32.05%	5.61
India	1,600,000+	65.03%	4.47
Ukraine	401,000+	–7.54%	4.07
Germany	747,000+	–0.73%	3.9
Brazil	553,000+	–21.02%	3.87

The average number of attacks per resident targeted by financial malware in 2013.

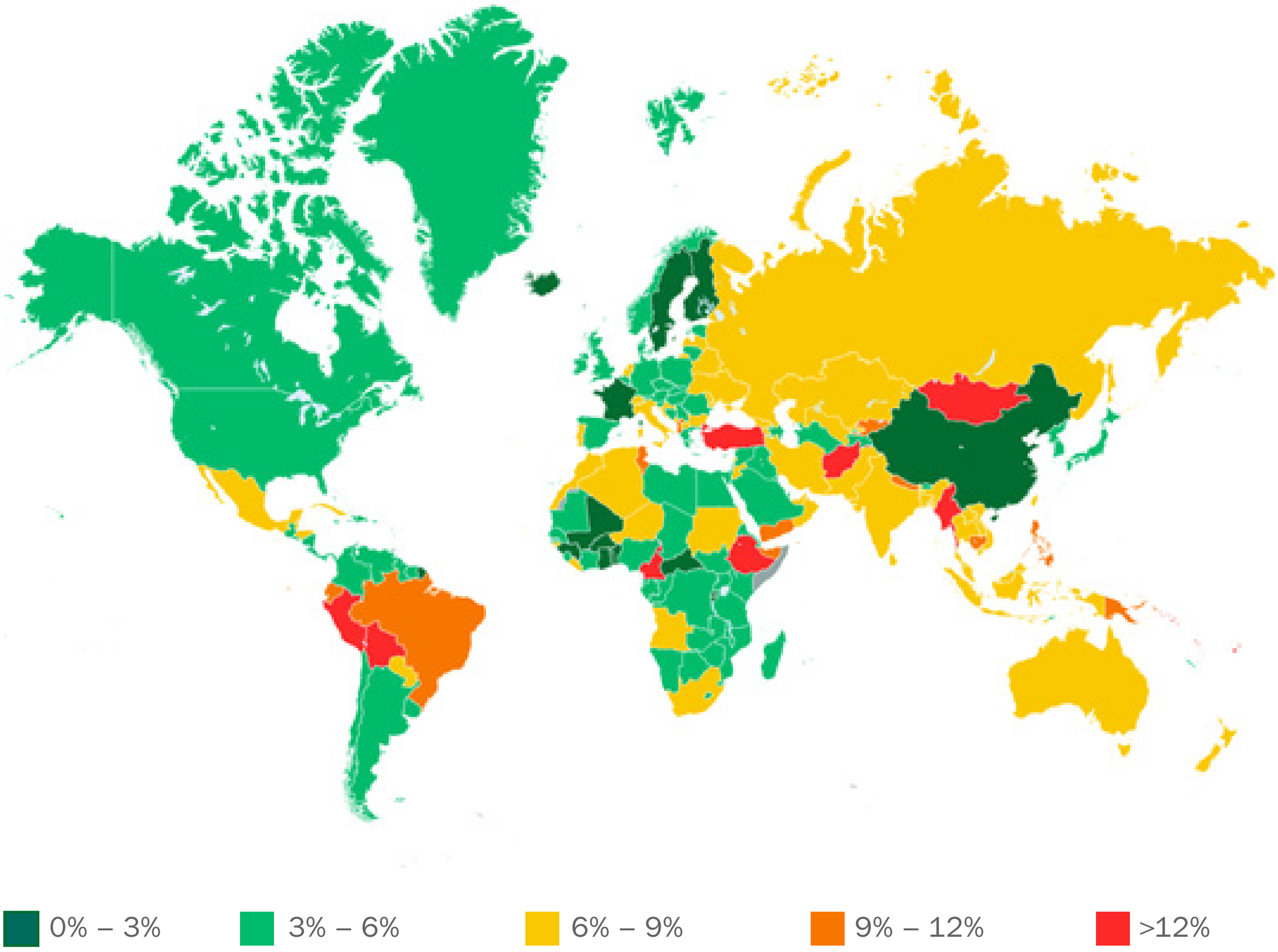
The Top 10 list of countries targeted by online financial threats was led by Turkey and Brazil. The percentage of users subjected to financial attacks in these countries was 12% and 10.5% respectively of the total number of users who encountered malicious programs in 2013. In Russia, that number was slightly over 6%, while just one in every 30 of the total number of users attacked in the US faced a specifically financial cyber threat.

Country	Users attacked by financial malware	Year-on-year change	% of users attacked by any type of malware
Turkey	97,000+	37.05%	12.01%
Brazil	143,000+	29.28%	10.48%
Kazakhstan	84,000+	5.11%	8.46%
Italy	105,000+	20.49%	8.39%
Vietnam	229,000+	31.77%	7.4%
India	358,000+	59.1%	6.79%
Russian Federation	792,000+	–4.99%	6.16%
Ukraine	98,000+	22.73%	6.08%
Germany	191,000+	43.22%	5.52%
United States	189,000+	22.30%	3.1%

Users attacked by financial malware in 2013 and their respective percentages of the residents of countries who were targeted by any type of malicious program.

If you look at a map of the world, it is clear that the percentages of financial attacks are relatively low in China, the US, Canada, and a number of European countries. The top countries in this category are located all around the world, and some of the most distinctive are Mongolia, Cameroon, Turkey, and Peru.

Percentage of users who encountered financial malware among the total number of users attacked by malware in 2013

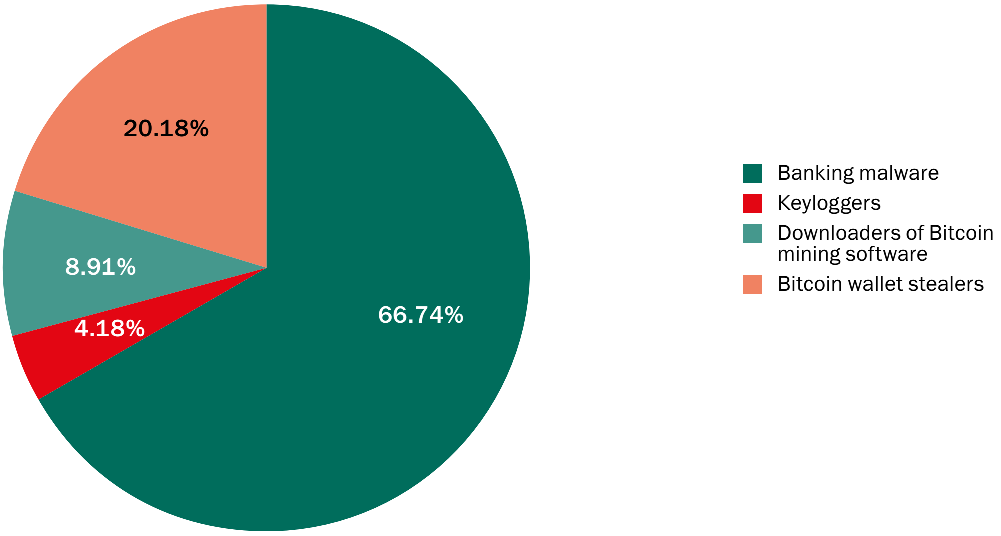


Know your enemy: financial malware species

In order to understand which malicious programs target users' financial assets and made up the landscape of threats over the past year, Kaspersky Lab experts put the tools used by cybercriminals into different categories. For the purposes of this study, the 30 most prevalent examples of malware used in financial attacks were examined. These were further divided into four groups, depending on a program's function and intended targets: banking malware, keyloggers, Bitcoin theft malware, and Bitcoin crypto-currency software installers.

The most diverse group of programs is the banking malware group, which includes Trojans and backdoors designed to steal cash from online accounts or to harvest data needed to steal cash. Some of the better known programs in this group are **Zbot**, **Carberp**, and **SpyEye**.

Attacks utilizing financial malware in 2013



Programs in the second category – keyloggers – are designed to steal confidential information, including financial data. Often, banking Trojans perform the same function, which can contribute to a decrease in the use of keyloggers as standalone tools. The most well-known among these are **KeyLogger** and **Ardamax**.

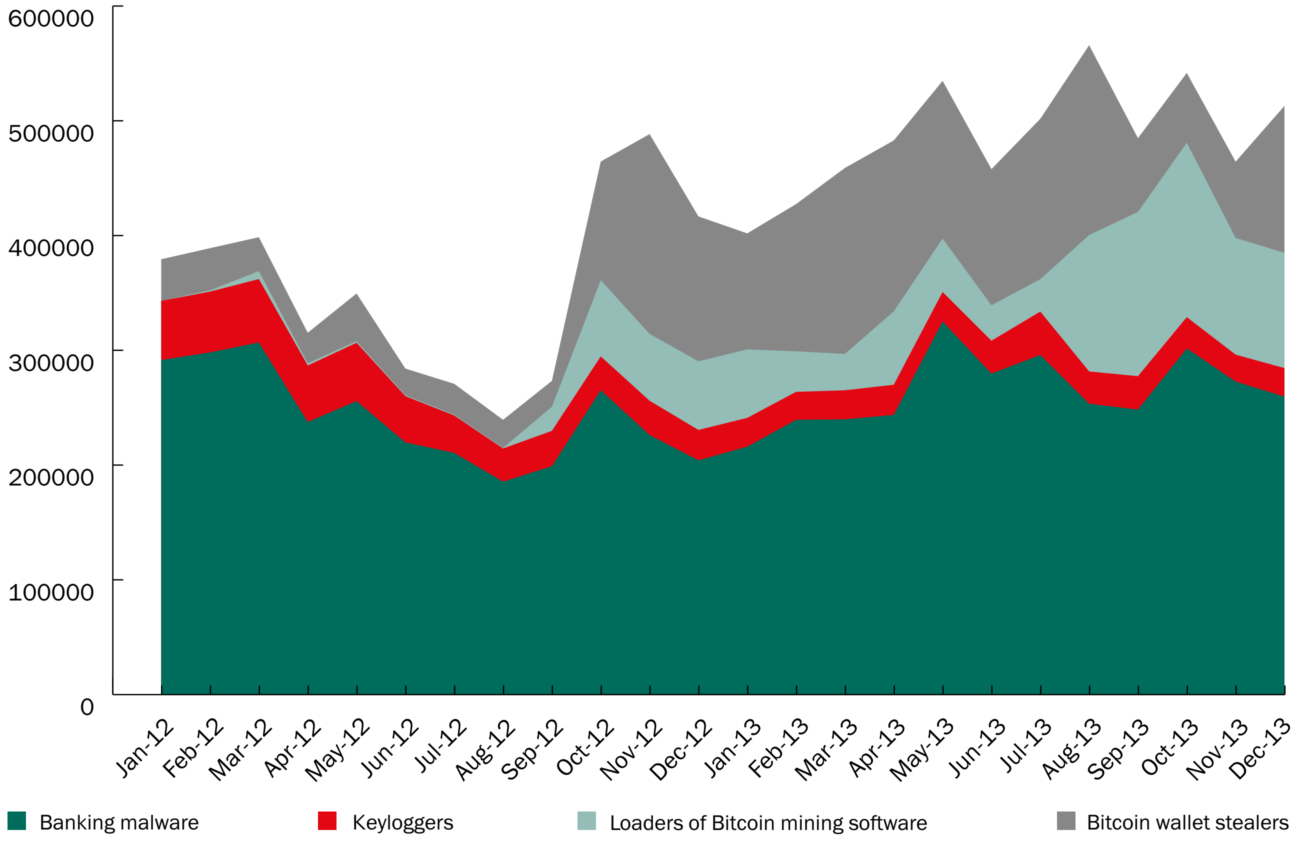
The last two malware groups are associated with the crypto-currency Bitcoin, which has become a sought-after prize for financial fraudsters over the past couple of years. These programs include tools used to steal Bitcoin wallets, and programs that secretly install applications on infected computers to obtain this currency, also known as mining software.

The first category includes malware that steals Bitcoin wallet files which store data about the bitcoins owned by a user. The second is slightly more difficult to define: in order to install the applications to generate Bitcoins (mining apps), one can use just about any kind of malicious program capable of downloading new programs to a computer without the user noticing, which is why for the purposes of this study, only the programs that have been noted in strict association with downloading and launching mining tools have been included.

It should be noted that this categorization is not 100% precise. For example, one and the same keylogger can be used both to harvest financial data and to steal online gaming account information. However, usually malicious programs tend to have a particular 'specialization' which defines its primary unlawful use and function, which allows us to associate each program with a particular category of cybercrime – financial crime, in this case.

Banking malware strikes

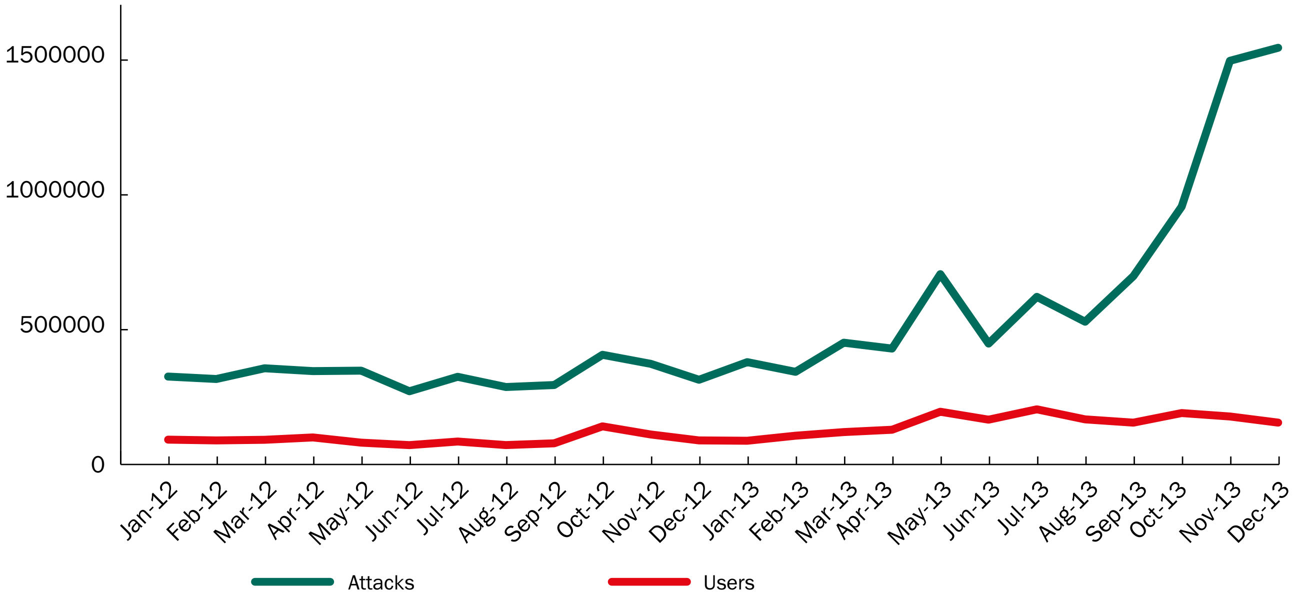
In 2013, banking malware – malicious programs that steal money from user accounts – played a leading role among financial cyber threats. Over the past year, at least 19 million cyber attacks were launched, representing two-thirds of all financial attacks involving malware.



By late 2013, the total percentage of users attacked each month by malicious users aiming to steal Bitcoins and install Bitcoin mining apps almost reached the same level as banking malware.

The most active malicious banking program – both in terms of the number of attacks and in terms of the number of targeted users – is the Trojan Zbot (aka ZeuS). The number of attacks that were traced back to this Trojan's modifications more than doubled over the course of the year, and the number of users attacked by the Trojan in the past year was greater than all the victims of the other Top 10 malicious banking programs put together.

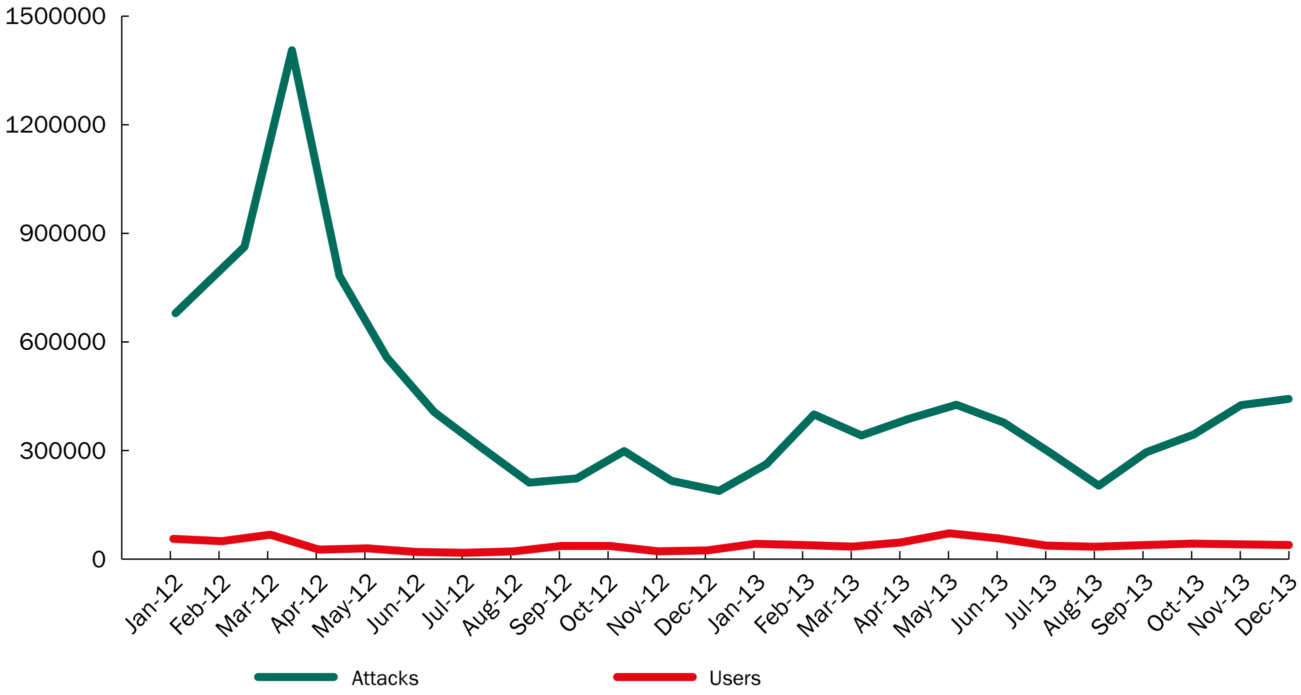
Zbot, 2012-2013



In 2011, Zbot's source code went public and was used to create (and is still being used to create) new variants of malicious programs, which is impacting attack statistics. Zbot is also known for having served as the foundation for the development of the Citadel platform – one of several attempts to migrate the principles of commercial software into the sphere of malicious program development. Citadel users could not only purchase a Trojan, they could also get tech support and prompt updates to prevent their programs from being detected by antivirus products. Citadel web resources also provided an organized social venue for hackers who could place orders for new functions. In early June 2013, Microsoft collaborated with the FBI and announced the shutdown of several large botnets that had been a part of Citadel; this was a major victory in the war against cybercrime. However, as we can see from Kaspersky Lab statistics, this did not have a huge impact on the proliferation of malicious programs designed to steal financial data.

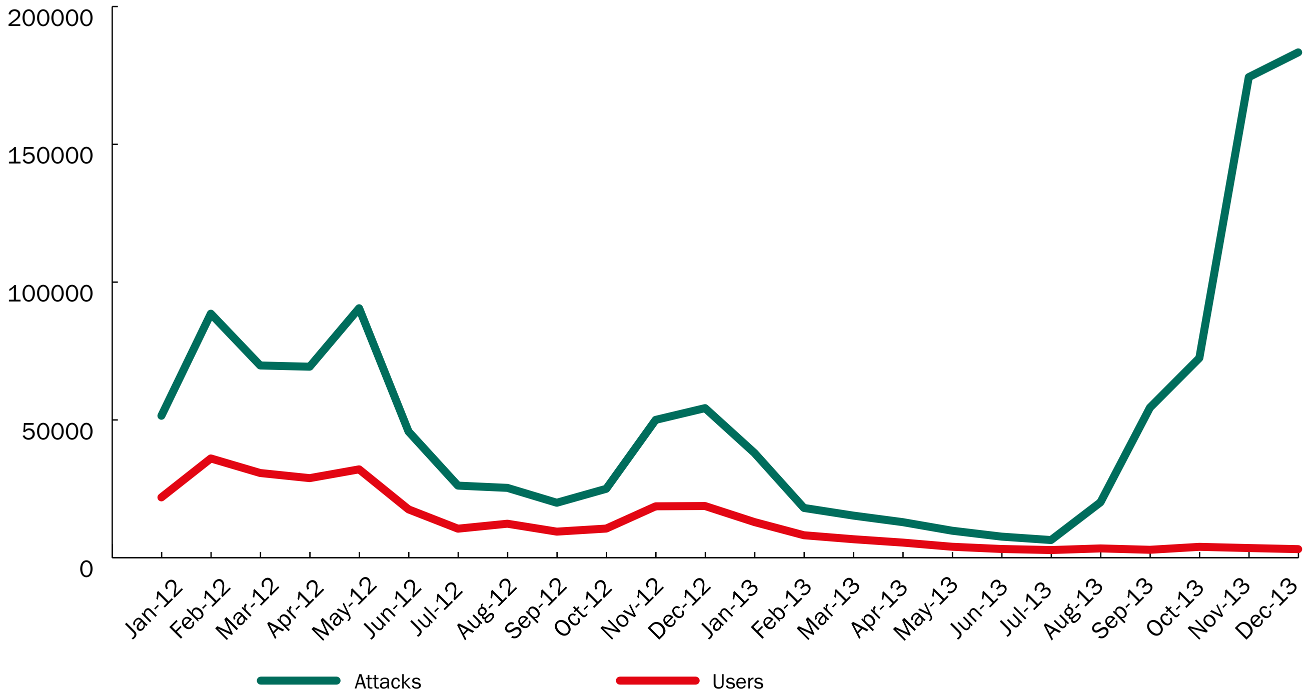
A sharp drop in the number of attacks using Qhost could potentially be related to the arrest of its creators, who in 2011 stole roughly $400,000 from the clients of one large Russian bank. The program's creators were sentenced in 2012, yet that did not stop the threat from spreading further. The relative simplicity of its settings and its ease of use means that this program continues to attract new malicious users.

Qhost, 2012-2013



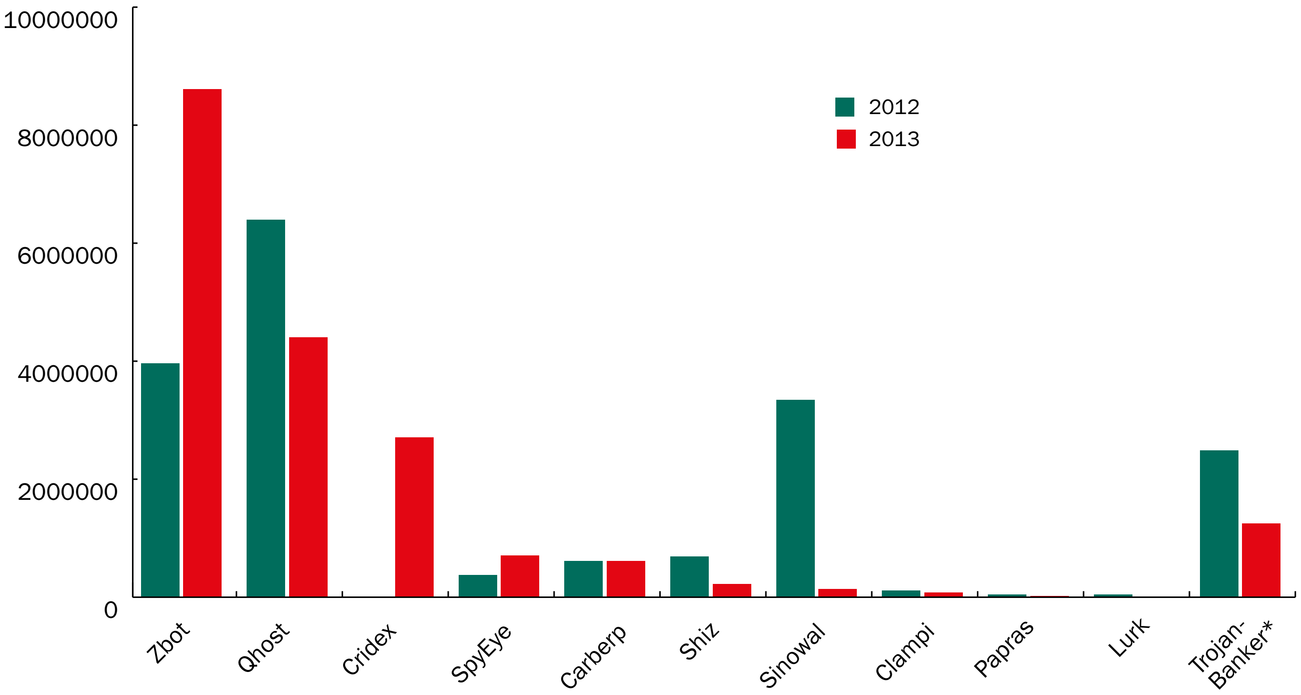
The number of attacks launched using the Carberp Trojan dropped during the first six months of 2013 after the springtime arrest of Trojan users – presumably, these included the program's creators. However, in summer, the number of Carberp attacks began to rise significantly, bringing 2013's end-of-year numbers up to the same level as those for 2012. Among other things, this is related to the open-source publication of the malware's source code, leading to a surge in the development of new versions of the Trojan. All the same, the number of users targeted by these modifications still decreased substantially during the past year.

Carberp, 2012-2013



The general trend is clear: after a bit of a downswing during the last six months of 2012, the scammers responsible for financial cyber attacks in 2013 resumed higher levels of activity as we can see by the increased number of attacks and the higher number of targeted users.

Attacks using banking malware in 2012-2013



* Trojan-Banker is the universal entry in Kaspersky Lab's database to detect financial malware

Bitcoin: money for nothing?

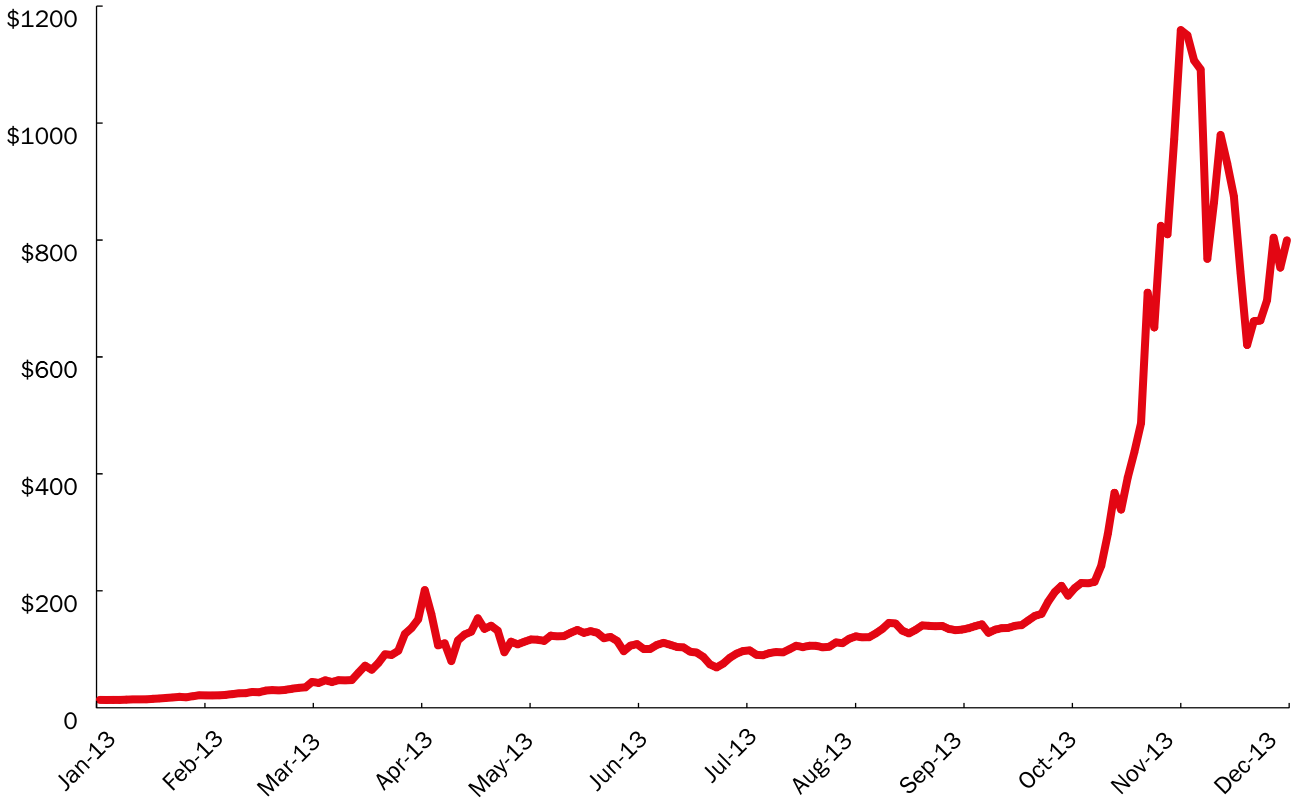
Bitcoin is an electronic crypto-currency that is not regulated by any government, but is in circulation thanks to its general use. A dedicated network supporting Bitcoin was launched in 2009. It was initially used by people with close ties to the IT industry, but gradually became more widely known. It began to gain popularity as a currency when it became a payment option on several major websites specializing in black market or otherwise illicit trade. These sites chose Bitcoin as it allows users to maintain anonymity.

One variation of a Bitcoin banknote

In theory, anyone who wants to can earn Bitcoins using their computers – this process is called mining. Mining essentially involves solving a series of cryptographic tasks that maintain the Bitcoin network.

Many of those who are considered “Bitcoin-rich” earned their Bitcoin estates back when the crypto-currency was just getting established, and before it was accepted as a liquid cash fund. However, as the currency became more common, it became more difficult to earn Bitcoins through computer performance – this is one of the peculiarities of the system, in addition to the ultimate volume of Bitcoins that will be released into circulation. At this time, the complexity of the requisite computations has increased so much that Bitcoin mining on typical computers has become unprofitable – even potentially loss-making and challenging to just break even when you factor in electricity costs.

The Bitcoin exchange rate



The Bitcoin exchange rate in early 2013 was at $13.60, and by December it had reached a historic high of over $1200.

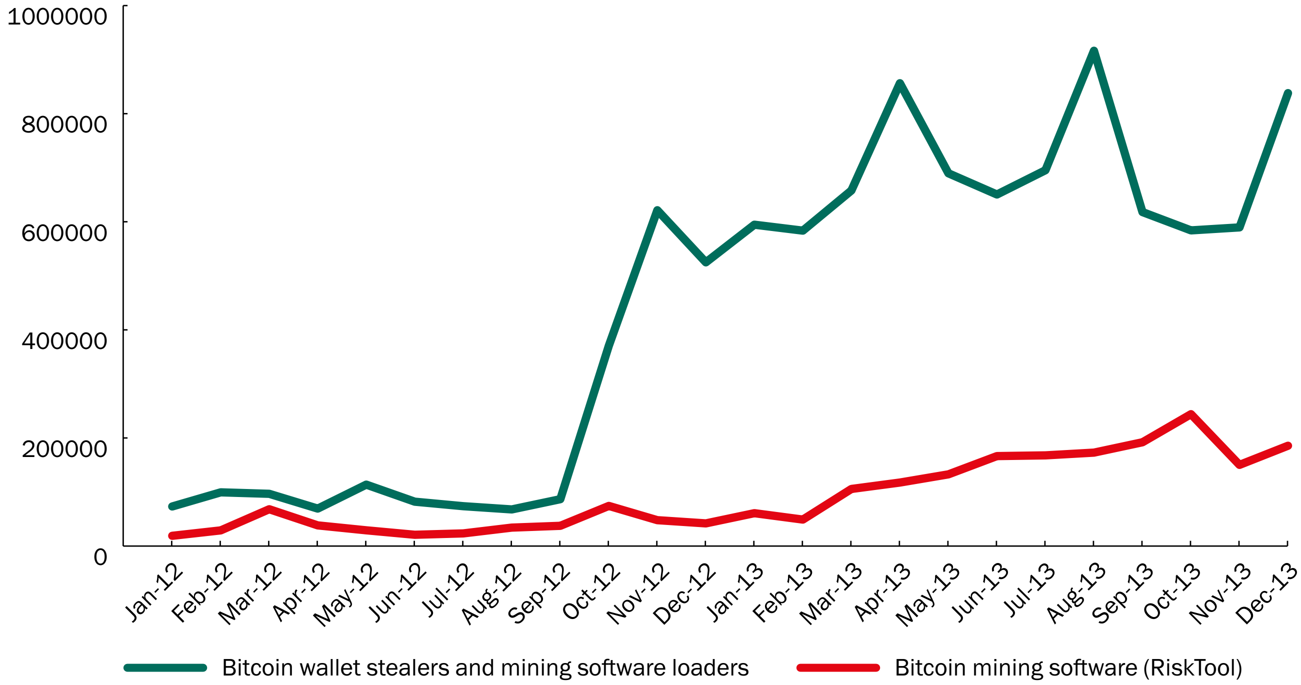
Over the course of the year, the Bitcoin exchange rate skyrocketed, exceeding $1200 at the close of December. This surge was followed by a decline, including due to the cautious stance among the central banks of a number of countries with regard to this currency. The People's Bank of China banned the use of Bitcoin exchanges, which cut the currency down by approximately one-third. At the same time, other countries have taken a supportive approach to Bitcoin. In particular, Germany's Ministry of Finance officially recognized the crypto-currency as a form of payment, and in Canada and the U.S., ATMs are being set up allowing Bitcoins to be transformed into cash funds.

In a word, in just a few years Bitcoin has moved from being a niche Internet phenomenon supported by a small group of enthusiasts to something close to a fully-fledged currency unit that holds actual value and is now hugely sought-after. It makes sense, then, that Bitcoin would naturally draw the attention of malicious users. From the moment that Bitcoin trading was launched on Internet exchanges for real money, more and more sellers began to accept this currency as payment, and cybercriminals became more interested.

Bitcoin is stored on computers in a special wallet file (wallet.dat, or something similar, depending on the app used). If that file is not encrypted and malicious users are able to steal it, then they could transfer all of the funds held therein to their own wallets. The Bitcoin network allows any participant to gain access to the transaction history for any user – that means it's possible to identify the wallet(s) to which stolen funds were transferred.

In addition to Bitcoin thefts, cybercriminals can also use their victims' computers to mine Bitcoins, in the same way that they use their victims' computers to send out spam and perform other malicious operations. There are also well known blackmailer programs that demand a ransom paid in Bitcoin in exchange for deciphering user data.

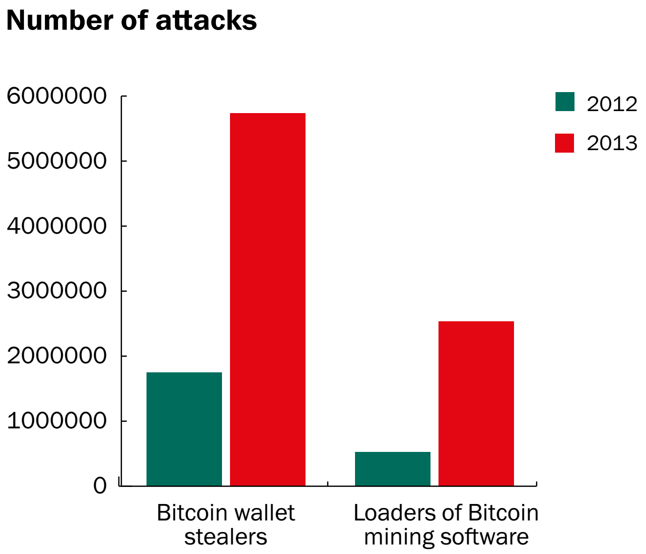
The chart below shows the dynamics of attacks using malicious tools designed to steal Bitcoin wallets, as well as malware that can load mining software on victim computers. In addition, there have also been instances where Bitcoin mining software was detected on a computer and where the owner of the computer could have intentionally installed that software, or it could have gotten on the user's computer without him knowing. Kaspersky Lab products put these apps into the RiskTool category – that means that this type of app could potentially harbor a malicious function and the user is notified of such.

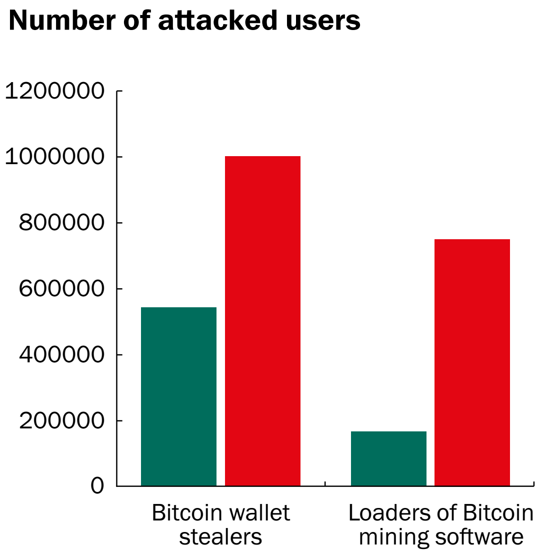


As you can see from the chart, the number of Kaspersky Lab product detections of Bitcoin theft programs and Bitcoin mining loaders began to rise during the second half of 2012. The dynamics became even more interesting in 2013. For example, one of the two most significant peaks of Kaspersky Lab detections related to Bitcoin took place in April – it was approximately at that time when Bitcoin's exchange jumped up to over $230. Clearly, the surge in the exchange rate provoked malicious users to more actively spread malware designed to steal or mine Bitcoins.

Incidentally, in April, the currency's price plunged down to $83. This crash was followed by a recovery up to $149 in late April and stabilization in May. From May until August, Bitcoin held up within a range of $90-100, and in August it began a steady upward surge. This process was only weakly correlated with the situation on the malicious front, although it is possible that it was the stabilization of the Bitcoin exchange rate that essentially provoked a new rush of attacks in August. Another sharp jump in the number of attacks took place in December, when the Bitcoin exchange rate first plummeted from $1,000 down to $584, and then later soared back up to $804 by the end of the month.

Since April, the number of Kaspersky Lab product detections of software used to generate Bitcoin has increased steadily. This growth continued right up through to October, until the number of detections began to decline in November.





Overall in 2013, both the number of detections registered by Kaspersky Lab products and the number of users coming into contact with malicious or potentially malicious software related to Bitcoin rose dramatically in comparison with 2012. It is also remarkable that starting roughly in October 2013, the number of detections of malicious programs loading Bitcoin mining apps began to drop while, in contrast, the number of detections of Bitcoin wallet theft apps began to rise. This could be the result of the above-mentioned idiosyncrasy of the Bitcoin system, where the more 'coins' that are generated, the more difficult it is to generate new ones. This could also drive malicious users to focus on searching for and stealing Bitcoin wallets holding already-generated crypto-currency.

Malicious programs designed to steal financial data are, of course, one of the most dangerous types of cyber threats today. The scale of the threat continues to expand, so we see an enormous amount of potential victims of attacks involving these types of malicious programs – just about everyone who owns a bank card and accesses the Internet from a computer with weak security could fall victim to cybercriminals. However, computers and notebooks are far from the only devices used to conduct financial transactions. Just about every modern individual owns a smartphone or a tablet these days, and for malicious users, these mobile devices offer yet another way to sneak into the pockets of people who use online financial services.

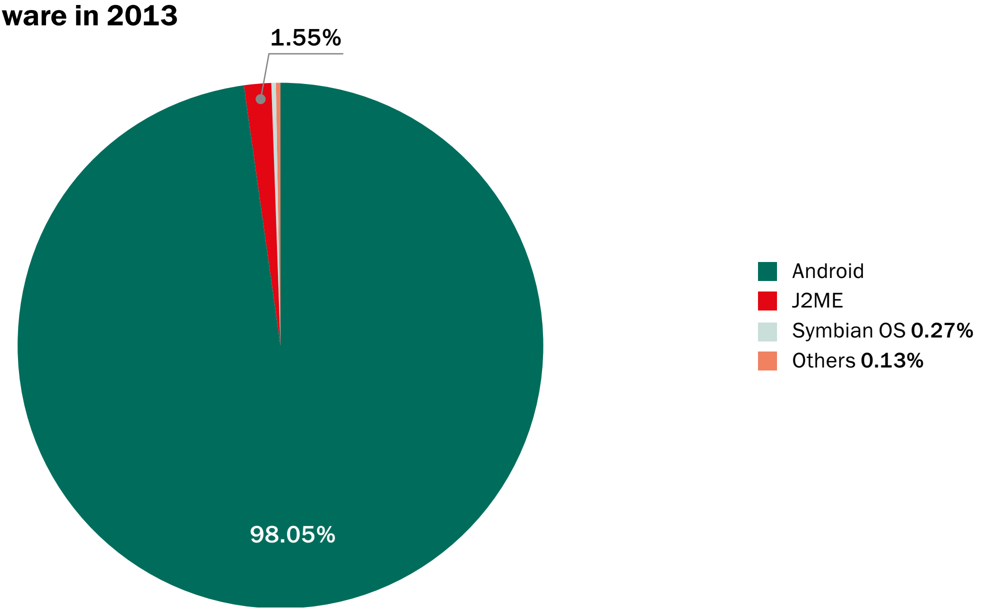
PART 3

Mobile banking threats

For a long time mobile devices were untouched by cybercriminals. To a large extent this was because the first generations of mobile devices had limited functionality and writing software for them was difficult. However, everything changed with the arrival of smartphones and tablets – versatile devices with Internet connectivity and publicly accessible application development tools. For several years now Kaspersky Lab experts have been recording an annual increase in the number of malicious programs targeting mobile devices, particularly those running Android.

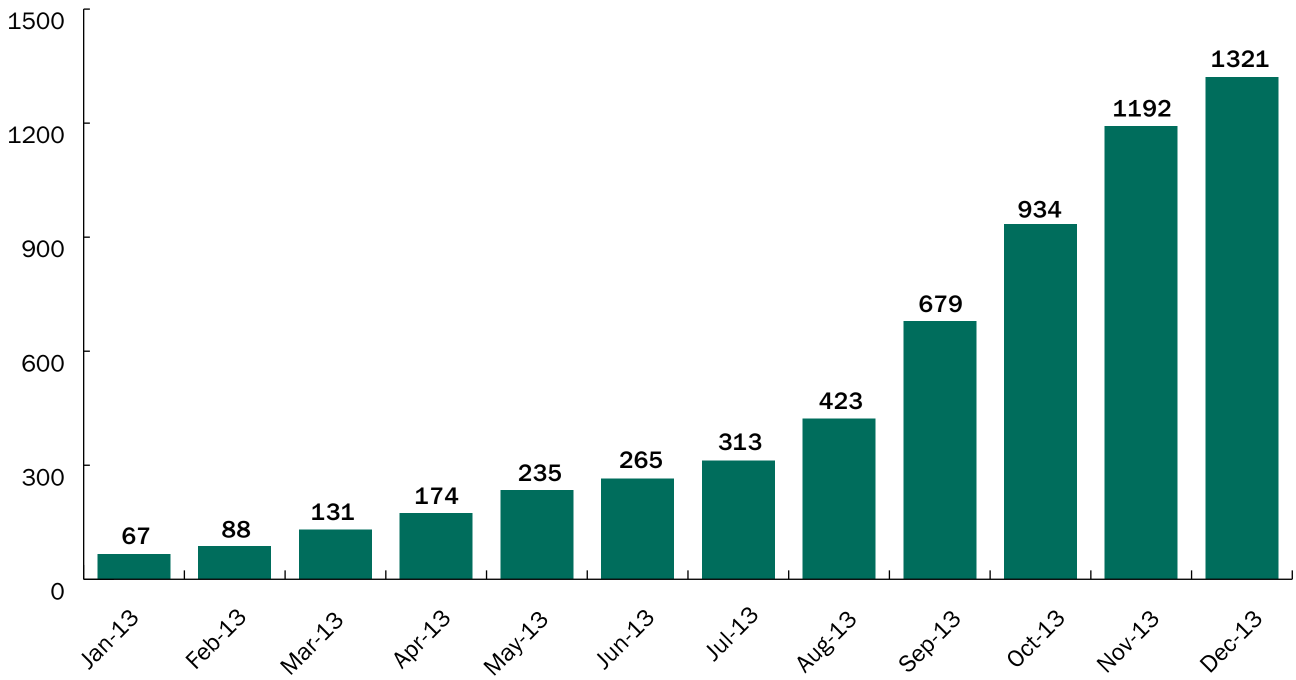
In 2013, Android was the main target for malicious attacks, with 98.1% of all mobile malware detected in 2013 targeting this platform. This is an indication of both the operating system's popularity and the vulnerability of its architecture.

Mobile malware in 2013



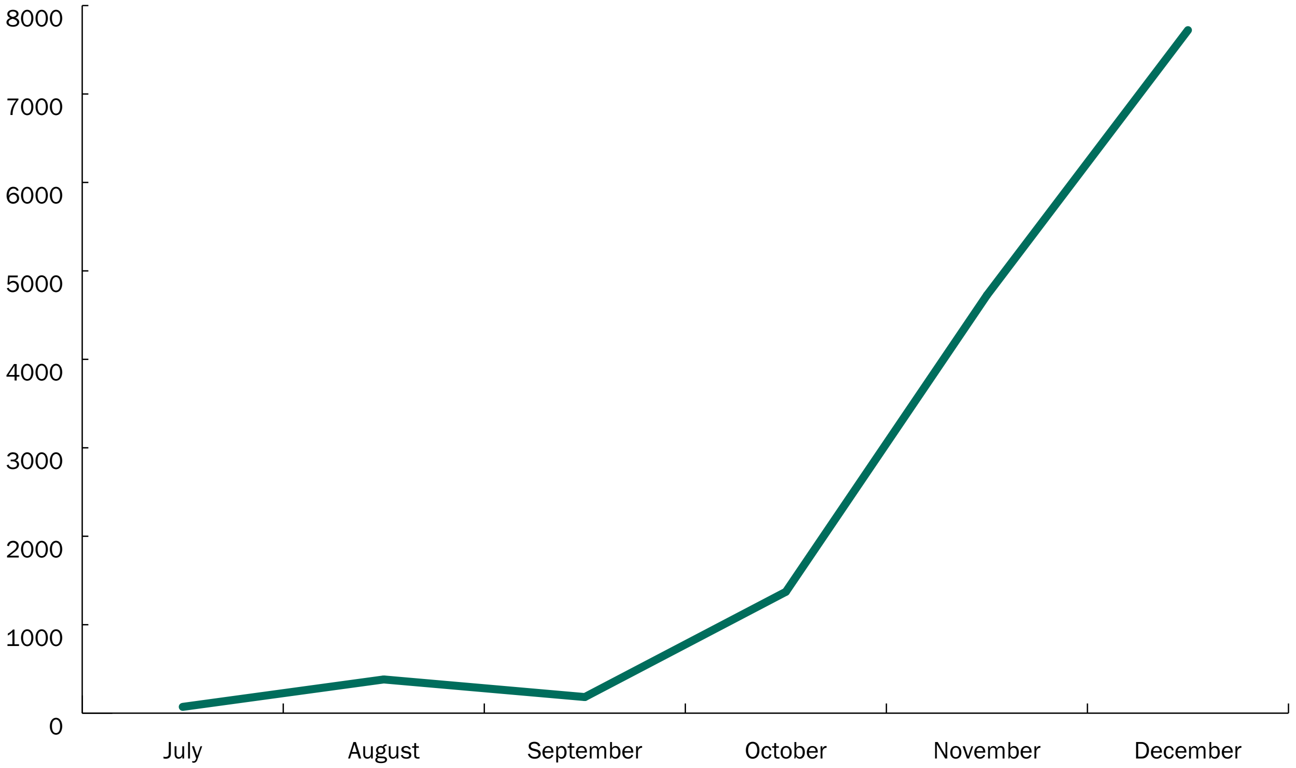
Most malicious programs for mobile devices, including many backdoors and some malware in the Trojan category, are designed to steal money from users. But one of 2013's most dangerous trends in mobile malware was the growing number of programs designed to steal online banking credentials in order to gain access to people's money.

The number of mobile banking Trojans in Kaspersky Lab’s collection in 2013



The number of these malicious programs began to grow rapidly in July and exceeded 1,300 unique samples by December. The number of attacks recorded by Kaspersky Lab began to rise at about the same time.

Attacks with mobile banking malware in 2nd half of 2013

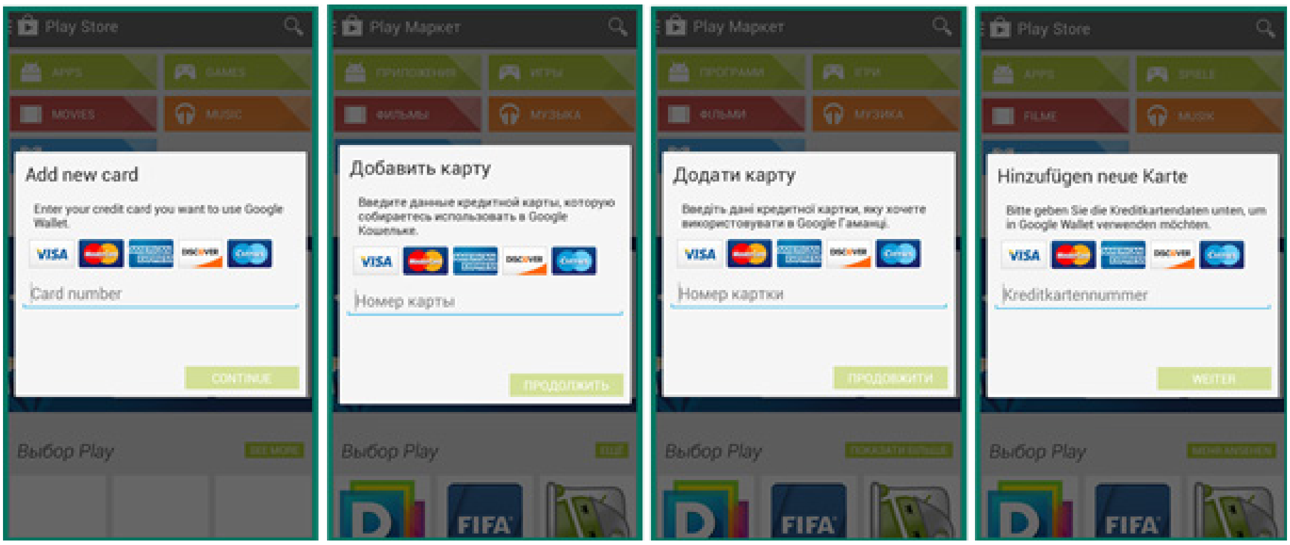


Mobile malware targeting online banking customers is nothing new. For example, ZitMo (the mobile 'twin' of Zeus, the infamous Win32 banking Trojan) has been on record since 2010, but until lately it was not known to have been used in mass attacks. That was partly due to its limited functionality: ZitMo could only work in conjunction with the 'desktop' version of Zeus. The 'partner' program intercepts the victim's online banking credentials, and then it is up to ZitMo to obtain the one-time passwords used in online banking systems to authorize transactions and send them to cybercriminals, who will use the data to steal money from the victims' bank accounts.

This fraudulent scheme was also used in 2013: by that time the main competitors of Zeus – SpyEye (SpitMo) and Carberp (CitMo) – had also got themselves 'little brothers'. However, they are not known to have caused a significant number of attacks. The black market for cyberthreats came up with more 'autonomous' Trojan programs, which were able to work without 'desktop' counterparts.

One example is the Svpeng Trojan, which was discovered by Kaspersky Lab experts in July 2013. The Trojan takes advantage of the way some of the Russian mobile banking systems work to steal money from victims' bank accounts.

The customers of some large banks in Russia can top up mobile phone accounts by transferring money from their bank cards. It's all done by text message, sent to a specific number maintained by the bank. Svpeng sends messages to the SMS services of two of these banks. This enables the owner of Svpeng to find out whether any cards issued by these banks are associated with the infected smartphone's number and to get balance information if an account exists. After this, the cybercriminal can instruct Svpeng to transfer money from the victim's bank account to the mobile phone account associated with it.



Add new card

Enter your credit card you want to use Google Wallet.

Card number

Добавить карту

Введите данные кредитной карты, которую собираетесь использовать в Google Кошельке.

Номер карты

Додати карту

Введіть дані кредитної картки, яку хочете використовувати в Google Гаманці.

Номер картки

Hinzufügen neue Karte

Bitte geben Sie die Kreditkartendaten unten, um in Google Wallet verwenden möchten.

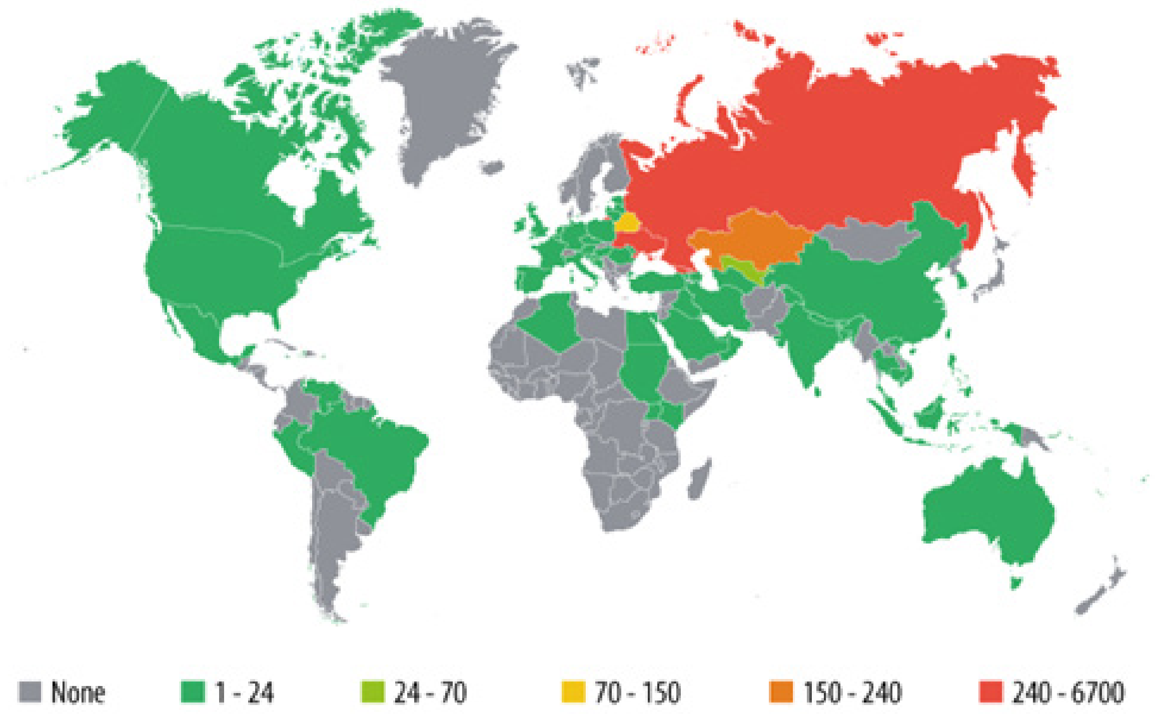
Kreditkartennummer

Svpeng fake authorization interface

Money can be subsequently 'bled' from the mobile account in different ways – e.g., by transferring it to an online wallet using the user's account control page on the mobile phone operator's website or simply by sending messages to premium numbers. Svpeng also has an additional function to steal the user's online banking credentials.

Two more examples of dangerous banking Trojans discovered by Kaspersky Lab experts are Perkele and Wroba. The former is similar to ZitMo – its main function is to intercept one-time passwords (transaction authorization numbers). The latter searches infected mobile devices for online banking applications and removes any applications found, replacing them with fake copies, which are then used to collect the user's credentials and send them to the cybercriminals.

Although most of the attacks involving mobile banking Trojans that were detected by Kaspersky Lab took place within the territory of Russia and neighboring countries, Perkele targeted users of some European banks and Wroba targeted users from South Korea.



Geographical distribution of attacks involving malicious mobile banking applications for Android in 2013

In absolute terms, the number of attacks that were detected by Kaspersky Lab products, involved financial malware and targeted mobile users has been relatively low up to now, but their number has been rising – a clear trend which has now been observed for more than six months. It means that users of mobile devices, particularly those running the Android platform, should be extremely careful when it comes to the security of their financial data.

Users of iOS-based devices should not be complacent, either. Although there has not so far been a spate of malware designed to steal sensitive data from iPhone and iPad owners, operating system errors making such malware possible keep appearing. One very recent example is an error found by researchers in late February 2014, which can enable attackers to record the characters entered by the user on the device's on-screen keyboard. Cybercriminals could take advantage of the vulnerability to steal the user's online banking credentials, among other sensitive data.

Conclusion: watch your digital wallet

The study has clearly demonstrated that users' electronic money is under constant threat. Whenever users work with their accounts via online banking or pay for their purchases in online stores, cybercriminals are there hunting for their money.

All types of financial threats demonstrated a significant growth in 2013. The proportion of phishing attacks involving bank brands doubled and that of malware-based financial attacks was a third greater than the year before. There were no 'newcomers' in the financial malware segment which could have an impact comparable to that of Zbot and Qhost.

Those two and other infamous Trojans were responsible for the majority of attacks during the past year. However, cybercriminals have once again demonstrated that they are keen to follow any changes in market conditions: the dramatic growth in attacks designed to steal Bitcoins, which began in late 2012, continued in 2013.

Kaspersky Lab experts offer the following advice on enhancing protection against financial cyberthreats.

For business

- Business bears a significant part of the responsibility for users' security. Financial companies should tell users about the threats posed by cybercriminals and provide advice on the ways to avoid losing money to cyber attacks.
- Banks and payment systems should offer their customers comprehensive protection against cybercriminals. One solution that can be used for this is the Kaspersky Fraud Prevention platform, which offers multi-tier protection against fraud.

For home users and online banking users

- Malware writers often rely on vulnerabilities in popular software. This is why only the latest versions of applications should be used and operating system updates should be installed as soon as they come out.
- Observing universal online security rules helps to minimize the risk associated with financial attacks. Users should choose strong passwords that are unique for each service, be careful when using public Wi-Fi networks, avoid saving sensitive information in the browser, etc.
- It is essential to use reliable anti-malware products that have demonstrated their effectiveness in independent tests. In addition, some security products, such as Kaspersky Internet Security, have built-in tools enabling users to work with online financial services securely.
- If you use a smartphone or tablet to access online banking, a payment system or for online shopping, be sure to protect the device with a reliable security solution, such as Kaspersky Internet Security for Android, which includes advanced tools providing protection against malware, phishing and device loss or theft.

For crypto-currency holders

Since Bitcoin and other similar crypto-currencies, such as Litecoin, Dogecoin and many others, have not been around for very long, many users are unfamiliar with the finer aspects of working with such systems, which is why Kaspersky Lab experts have prepared advice on using crypto-currencies securely:

- Avoid using online services to store your savings; use dedicated wallet applications instead.
- Break up your savings into several wallets – this will help to minimize losses in the event that one of the wallets is stolen.
- Store the wallets where you hold your long-term savings on encrypted media. Alternatively, you can use wallets printed on paper.

KASPERSKY lab