KASPERSKY LAB REPORT

Financial cyberthreats in 2014

#KLReport

February 2015

CONTENTS

Executive Summary and Main Findings 3

Financial Phishing 5

- Financial phishing in detail 6
- Banks 7
- Mac OS X financial phishing 8

Financial Malware 9

- Dynamics of attacks 11
- Banking malware 12
- Zbot decrease 12
- Other financial threats: Keyloggers and Bitcoin malware 14

Geography of financial attacks 17

Android financial threats 21

Conclusions and Recommendations 26

- Home users 26
- Businesses 27

Methodology 28

Note on Responsible Distribution of Information 29

EXECUTIVE SUMMARY AND MAIN FINDINGS

In 2013, Kaspersky Lab registered a sudden surge in the number of attacks targeting users' financial information and money. This trend and other aspects of the 2013 financial cyberthreats landscape were discussed in detail in Kaspersky Lab's "Financial Cyber-threats in 2013" report.

In 2014, the situation changed considerably:

Financial phishing attacks

- Financial phishing attacks, including phishing against banks, payment systems and e-shops accounted for **28.73%** of all phishing attacks (a decrease of 2.72 percentage points compared with 2013).
- Banking phishing accounted for **16.27%** of all attacks (a decrease of 5.93 percentage points compared with 2013).
- The share of phishing utilizing payment system brands increased 2.4 percentage points (from 2.74% in 2013 to **5.14%** in 2014).
- Phishing against e-shops increased slightly by 0.81 percentage points (from 6.51% in 2013 to 7.32% in 2014).

Financial malware attacks

- In 2014, Kaspersky Lab products detected **22.9** million attacks utilizing financial malware, targeting **2.7** million users. This represents a year-on-year decrease of 19.23% for attacks and 29.77% for the number of users.
- Among the total number of users subjected to any type of malware attacks, **4.86%** encountered attacks involving some kind of financial threat – that's 1.34 percentage points lower than in 2013.
- Although the total number of financial attacks decreased, the share of malware attacks targeting online banking credentials rose 8.89 percentage points to comprise **75.63%** of all financial malware attacks in 2014.
- The number of attacks with Bitcoin-mining malware tripled: from **360,065** attacks in 2013 to **1,204,987** in 2014.

Android financial malware attacks

- **48.15%** of attacks on users of Android-based devices that were blocked by Kaspersky Lab products utilized malware targeting financial data (Trojan-SMS and Trojan-Banker).
- Compared with 2013, the number of financial attacks against Android users grew **3.25** times (from **711,993** in 2013 to **2,317,194** attacks in 2014) and the number of users targeted rose **3.64** times (from **212,890** users in 2013 to **775,887** users in 2014).

The overall number of attacks and affected users decreased by more than 20%, as did the amount of financial phishing. There are several possible reasons for this. First of all, law enforcement agencies around the world actively prosecuted cybercriminals who were spreading financial malware and phishing. In particular, during the summer, law enforcement agencies in the US and the UK stopped the activities of two dangerous malicious campaigns – **Gameover / Zeus** and **Shylock**.

The second reason for the decline in the number of attacks might be a shift in the cybercriminals' focus – instead of attacking end-users they started to pursue organizations that work with financial information and payment tools. Throughout the year there were frequent reports of malicious attacks on large stores, hotel chains and fast food restaurants that between them serve millions of customers a day. In each case the fraudsters used **malicious software** that could steal bank card data directly from the memory of the POS terminals used by the organization under attack. Banks also **became** a "new" cybercriminal target and in 2014 Kaspersky Lab investigated several attacks targeting banks rather than their users' accounts. Neither of these "new" types of attack prompted a rash of new AV detections, simply because there were so few organizations involved compared with the number of private users running antivirus solutions, so it was difficult to compare the number of attacks. Nevertheless, with the damage from such attacks amounting to millions of dollars, these threats can hardly be dismissed.

A third possible reason for the reduced number of cyberattacks lies in a general trend **observed** by Kaspersky Lab specialists in 2014. According to the company's experts, cybercriminals became less interested in "mass" malicious attacks on users, preferring fewer, more "targeted" attacks. This can be seen from the increased levels of targeted phishing: fraudsters only went after a specific group of users (for example, online banking users) rather than spreading mass mailings that contained malicious links.

This tactic suggests that a selective malicious mailing was considered less likely to be detected by IT security specialists so that the lifespan of malicious links and malware samples would be extended – the fewer malicious messages sent out, the fewer chances that security researchers would notice the malicious campaign. The trick is not always successful, but one consequence of its use was a decline in the absolute number of registered cyberattacks.

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

FINANCIAL PHISHING

Financial phishing attacks, including phishing against banks, payment systems and e-shops accounted for **28.73%** of all phishing attacks detected in 2014 by the Heuristic anti-phishing component of Kaspersky Lab products. Each attack was an attempt to download a phishing page into the browser of the user. The source carrying the link could be an email message, or a message from an instant message services or a social network etc.

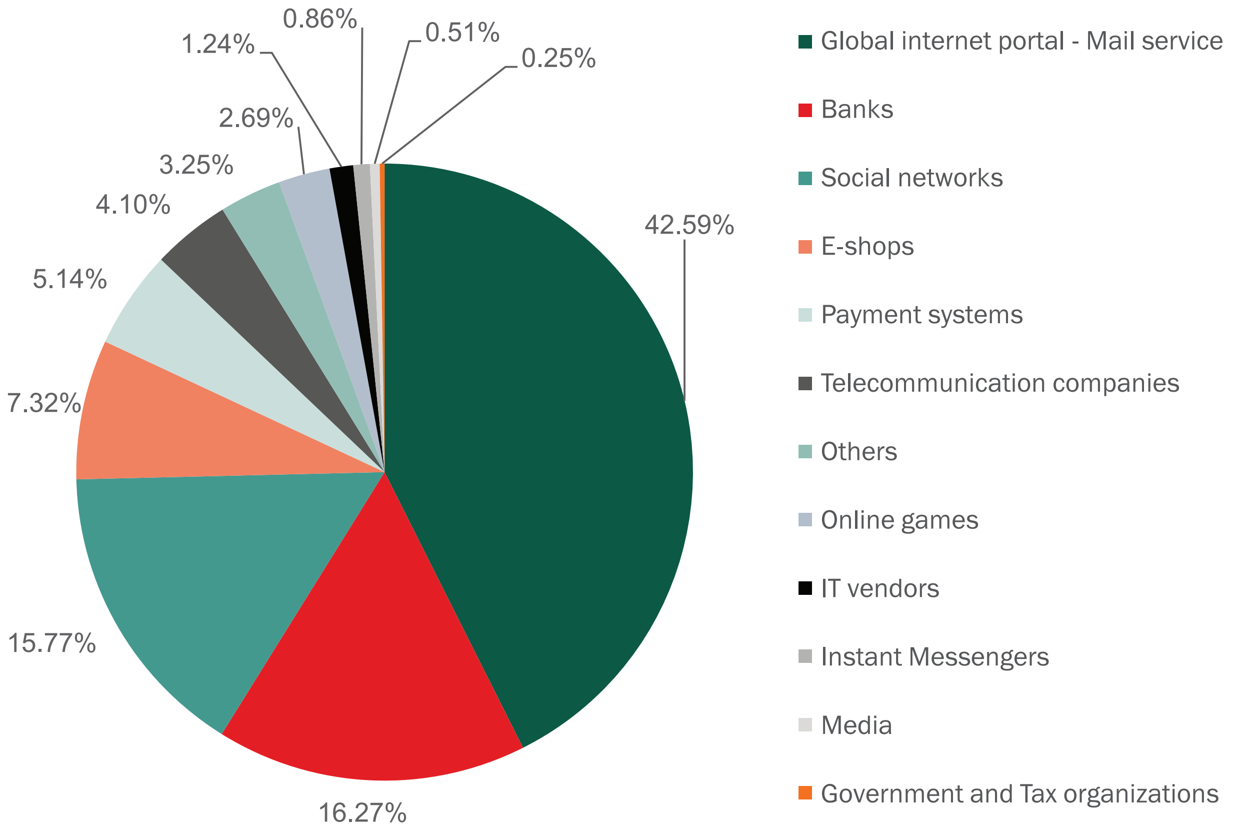

Fig. 1. Distribution of phishing attacks in 2014

The share of financial phishing decreased by 2.72 percentage points compared with 2013. The overall share of phishing against banks decreased 5.93 percentage points (from 22.2% in 2013 to 16.27% in 2014). The share of phishing against e-shops increased slightly by 0.81 percentage points (from 6.51% in 2013 to 7.32% in 2014), while the share of phishing against payment systems increased by 2.4 percentage points (from 2.74% in 2013 to 5.14% in 2014). According to Kaspersky Lab experts, the fall in the number of banking attacks was due to the countermeasures implemented by many banking organizations that had previously been heavily attacked. These measures included educational campaigns among clients and implementing anti-spam and anti-fraud solutions to make it much harder for fraudsters to run a successful phishing campaign. That had the effect, however, of making fraudsters pay more attention to other targets: payment systems and e-commerce organizations.

Type of phishing	Share in 2013	Share in 2014
Total share of financial phishing	31.45%	28.73%
Financial phishing/Banks	22.2%	16.27%
Financial phishing/E-commerce	6.51%	7.32%
Financial phishing/Payment systems	2.74%	5.14%

Table 1. Changes in the share of different types of financial phishing in 2013 and 2014

Financial phishing in detail

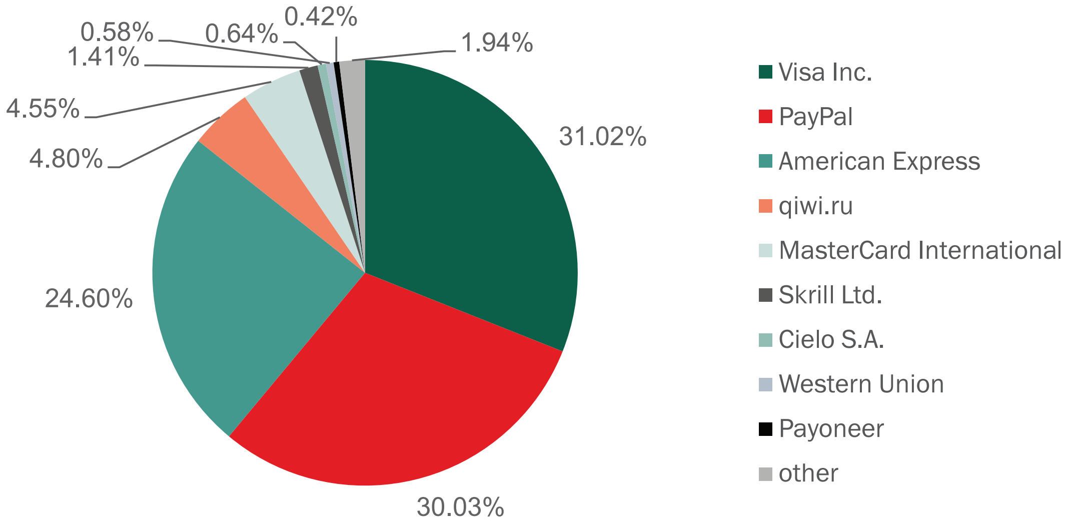

Fig. 2. Distribution of phishing attacks against payment systems in 2014

Phishing attacks against users of Visa cards jumped from 6.36% in 2013 to 31.02% in 2014. The longtime leader of the category, PayPal, is now in second place representing 30.03% of all phishing attacks against users of payment systems successfully blocked by Kaspersky Lab products in 2014. The share of attacks against users of PayPal decreased by 14.09 percentage points: from 44.12% in 2013 to 30.03% in 2014. It is important to note that Visa became the leader mostly because of the significant drop in attacks against users of PayPal, with the number of attacks mentioning Visa remaining more or less the same as in the previous year.

According to the statement provided to Kaspersky Lab by PayPal and the company's security partner, Agari, the significant decrease in the volume of attacks against users of the famous payment system might be due to the implementation of DMARC[1] policy by PayPal and global mail providers. This policy allows for the blocking of messages sent from unauthorized domains, thereby preventing the distribution of phishing emails. PayPal and Agari estimate that over 85% of consumer mailboxes in the US are protected by DMARC, as are over 65% of mailboxes across the world. The effectiveness of DMARC depends very much on how many e-mail providers are following the policy. The number of such providers increased in the last year and that has led to the corresponding result: a decrease in the share of attacks.

[1] Domain-based Message Authentication, Reporting and Conformance or DMARC is a method of email authentication that is a way to mitigate email abuse. Source: http://en.wikipedia.org/wiki/DMARC

In general, the situation for the most frequently attacked brands is the same as it was in 2013. MasterCard, Skrill, Cielo and Western Union are still among the most regularly attacked brands. PostFinance, WebMoney and Epoch have left the list, and have been replaced by Qiwi and Payoneer systems.

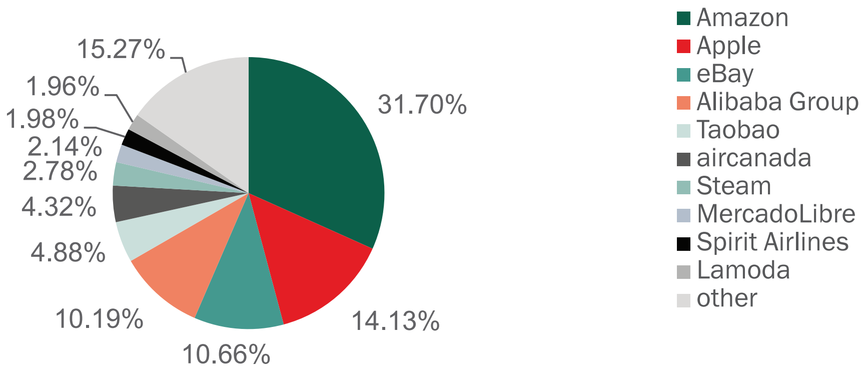

Fig. 3. Distribution of phishing attacks against e-shops in 2014

The e-commerce brand used most often by fraudsters is still Amazon – 31.7% of phishing attacks against e-shops used this retailer. However, this total is around half that of 2013 (29.41 percentage points lower), when 61.11% of all attacks on e-shops were against users of Amazon.

The share of attacks against users of Apple (Store, iTunes Store etc.) increased by 1.24 percentage points, from 12.89% in 2013 to 14.13% in 2014. Fraudsters continued to exploit the popularity of Apple products. In most cases they tried to fake the iTunes authorization page in order to steal users' credentials and credit card numbers.

Banks

In 2014 more than half of all attacks against banks utilized the names of just 13 of the biggest and most well known international financial organizations. The remaining 49.49% were distributed between more than 1,000 different banking brands. In 2013 a near-identical share of attacks was distributed between 25 banking brands. This change shows a kind of consolidation in the fraudsters' efforts. Fraudsters preferred to reduce the list of targets and concentrate on several of the most popular brands to increase their chances of success.

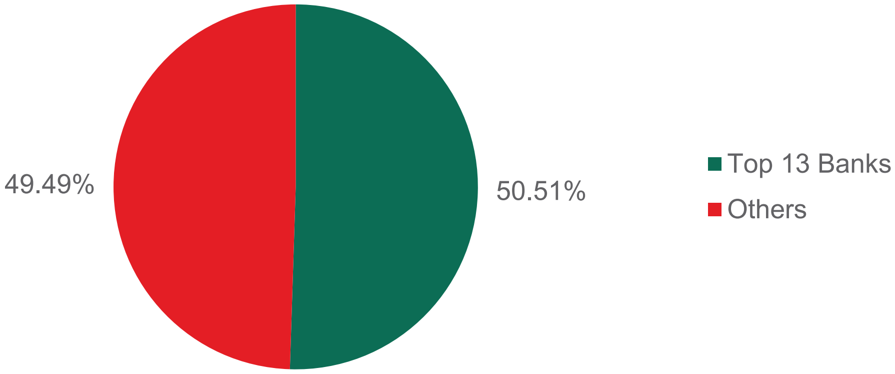

Fig. 4. Distribution of phishing attacks against banks in 2014

Mac OS X financial phishing

Over the reporting period, about 48.53% of all Kaspersky Lab anti-phishing detections on Apple computers involved «financial» phishing pages (Banks + Payment systems + E-shop). That is 9.61 percentage points more than in 2013.

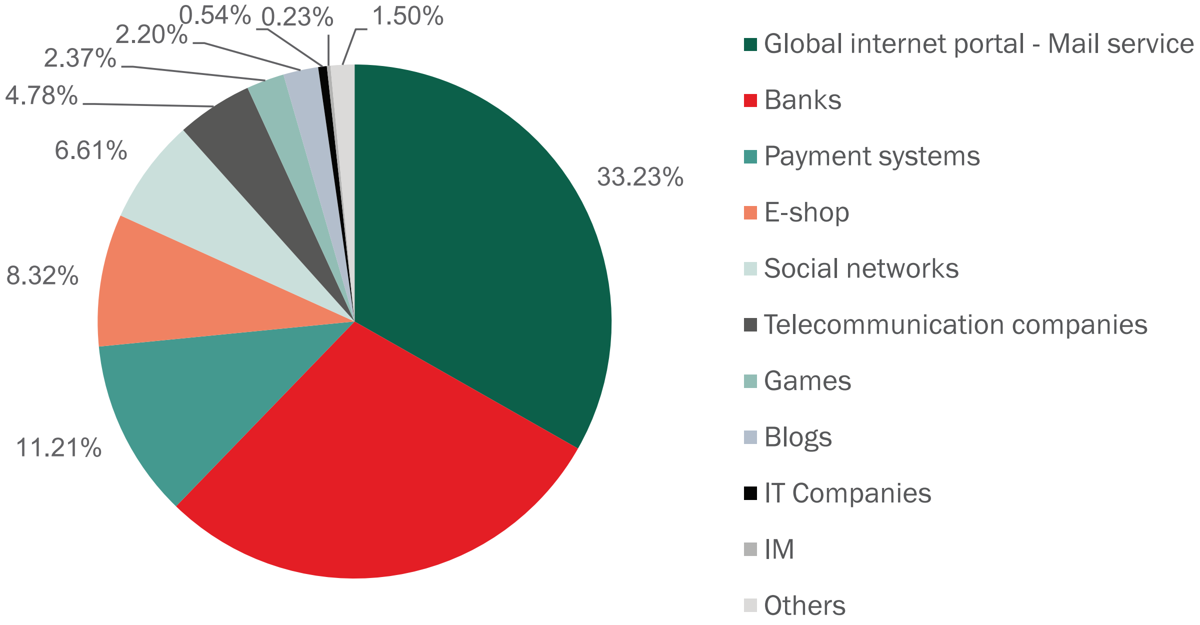

Fig. 5. Distribution of phishing attacks against Mac OS X users in 2014

The share of banking phishing reduced by 0.86 percentage points, and attacks against e-shops accounted for 8.23% (6.6% in 2013). The share of attacks against payment systems blocked on OS X computers increased by more than any other category – 8.75 percentage points, from 2.46% of attacks in 2013 to 11.21% of attacks in 2014. In other words, the KSN statistics show that in 2014 Mac owners faced phishing attacks as often as the users of computers running Windows.

FINANCIAL MALWARE

Among the total number of users subjected to any type of malware attack, 4.86% encountered attacks involving some kind of financial threat – that's 1.34 percentage points lower than in 2013 and a little more than it was in 2012 (4.78%).

In total, the number of attacks reached 22,947,229. That is 19.23% less than in 2013 (when there were 28,411,384 attacks). The number of users attacked was 2,698,509 – 29.77% lower than a year before (when 3,842,246 users were hit).

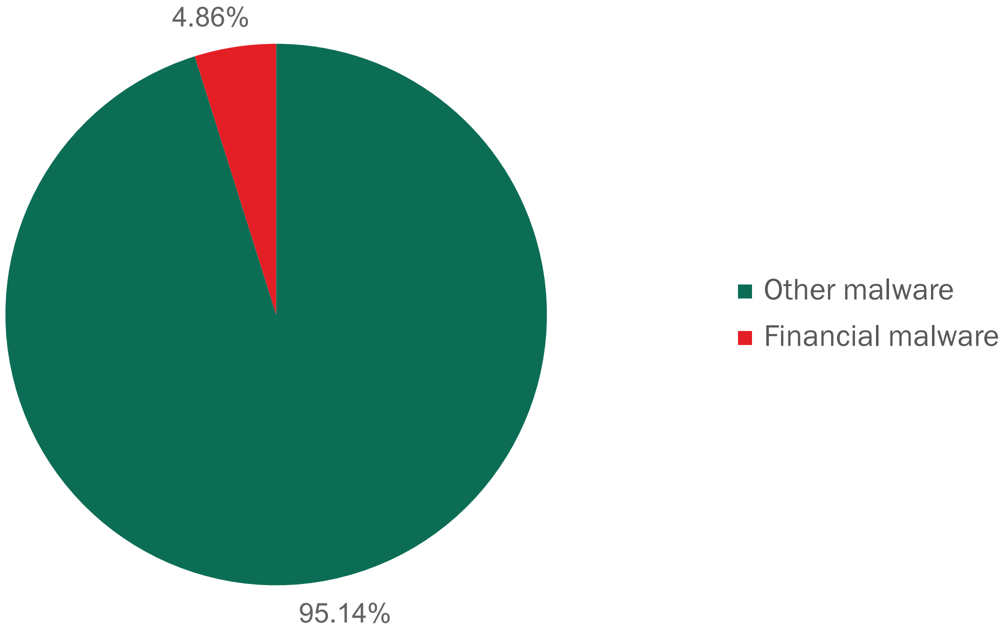

Fig. 6. Share of users attacked with financial malware in 2014

This could be explained by the tendency of cybercriminals to shift from mass to more precise and targeted attacks, a trend observed by Kaspersky Lab researchers in 2014. The idea behind this tactic is fairly simple: the wider a malicious campaign, the sooner security solutions start detecting the malware used in the campaign. In an attempt to avoid this criminals try to choose targets more carefully. The tactic is not necessary successful, but it affects the number of detections registered by security solutions.

Moreover, although the actual number of attacks and attacked users declined, the intensity of the attacks actually increased. On average, each user attacked with financial malware in 2014 was hit 8.5 times, while a year before it was 7.2 attacks per user, and in 2012 it was 6.9 attacks per user.

What's even more interesting is that the intensity of general malicious attacks (involving all types of malware) dropped from 106 attacks per user in 2013 to 81.8 attacks per user in 2014.

Types of financial malware

While the number of actual financial malware attacks decreased in 2014, the share of banking malware rose by 8.89 percentage points to 75.63% of all financial malware attacks.. At the same time, the shares of other types of financial malware decreased slightly.

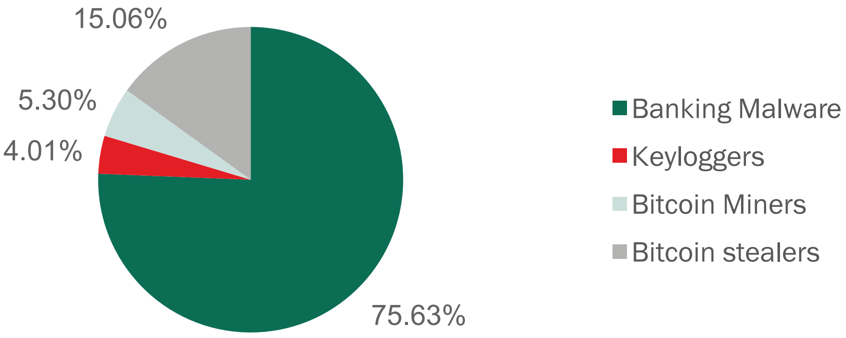

Fig. 7. Distribution of attacks with different types of financial malware in 2014

In 2013 it was…

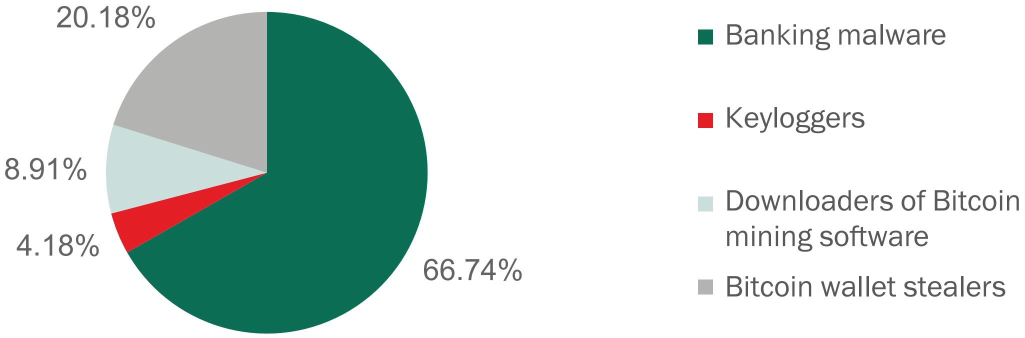

Fig. 8. Distribution of attacks with different types of financial malware in 2013

Dynamics of attacks

As can be seen on the graph below, the period July 2013 to December 2013 saw a dramatic increase in the number of attacks.

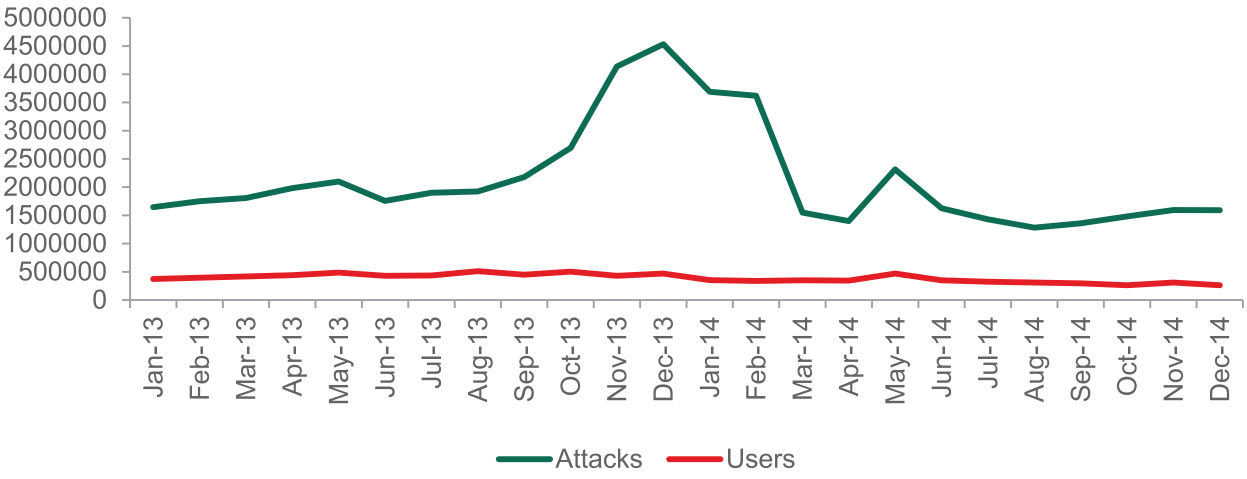

Fig. 9. Attacks with financial malware in 2013 and 2014

This increase was due to number of reasons described in last year's Financial Cyberthreats in 2013 report. Mostly, it was the result of work by the criminals behind Zbot, Carberp, Cridex, and several other malicious programs aimed at stealing credentials from online banking and other financial services accounts.

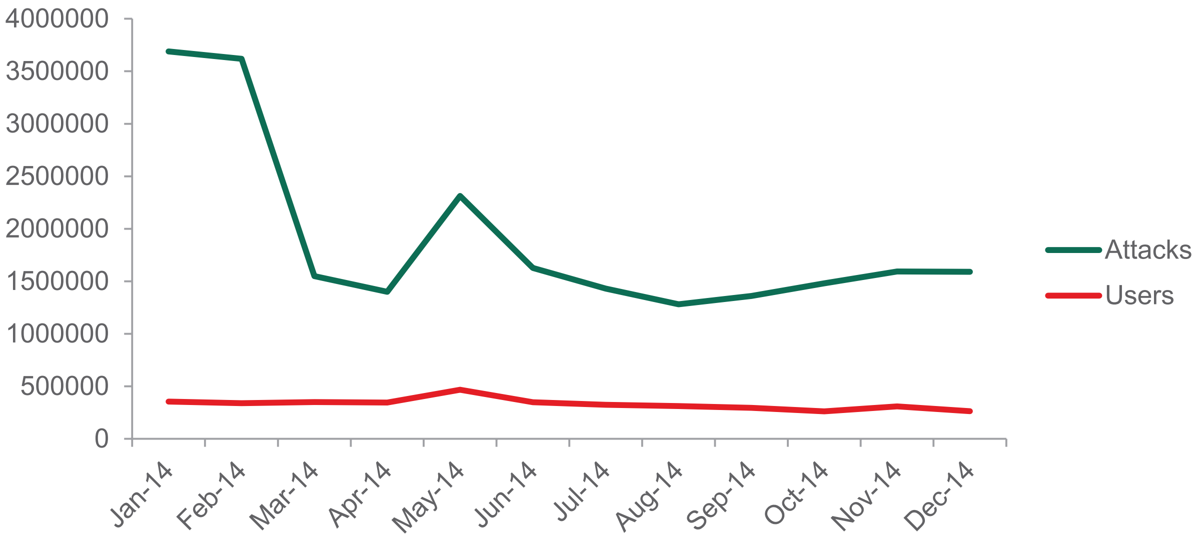

Fig. 10. Attacks with financial malware in 2014

Interestingly, the decrease in the number of attacks and attacked users observed in 2014 was the result of a fall in activity by almost the same list of malware families.

Banking malware

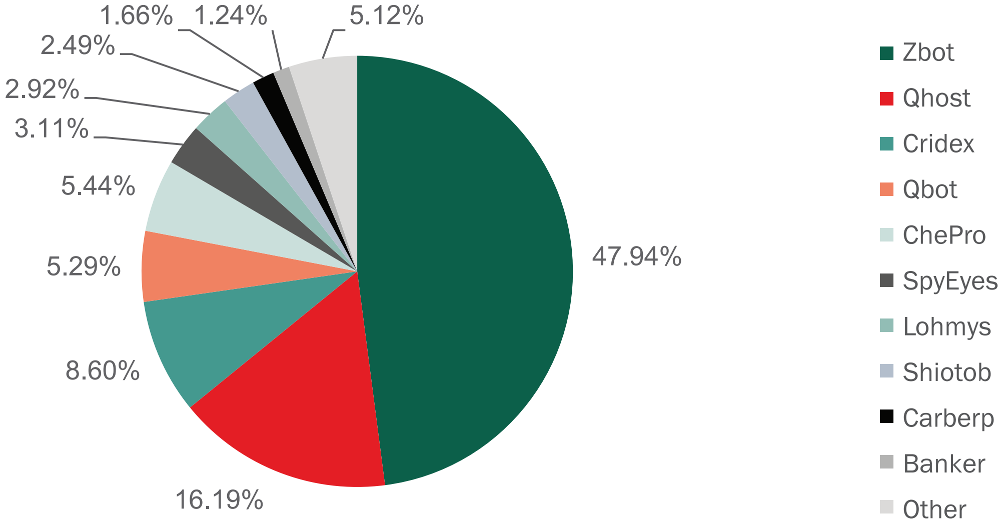

Fig 11. Top 10 of the most often used banking malware families

As can be seen on the pie chart above, only 10 families of malware are responsible for more than 94% of all banking malware attacks. It comes as no surprise that the top position again goes to the infamous Zbot – the most widespread and one of the most dangerous banking malware families.

Zbot decrease

But during the year we also saw signs of a decrease in Zbot influence on the financial threat landscape. Although this family was responsible for 47.94% of all banking malware attacks throughout the year, as the months went by Zbot's share (as well as the shares of several other “Big” threats) decreased significantly: from 34.86% in January, to 26.02% in December 2014.

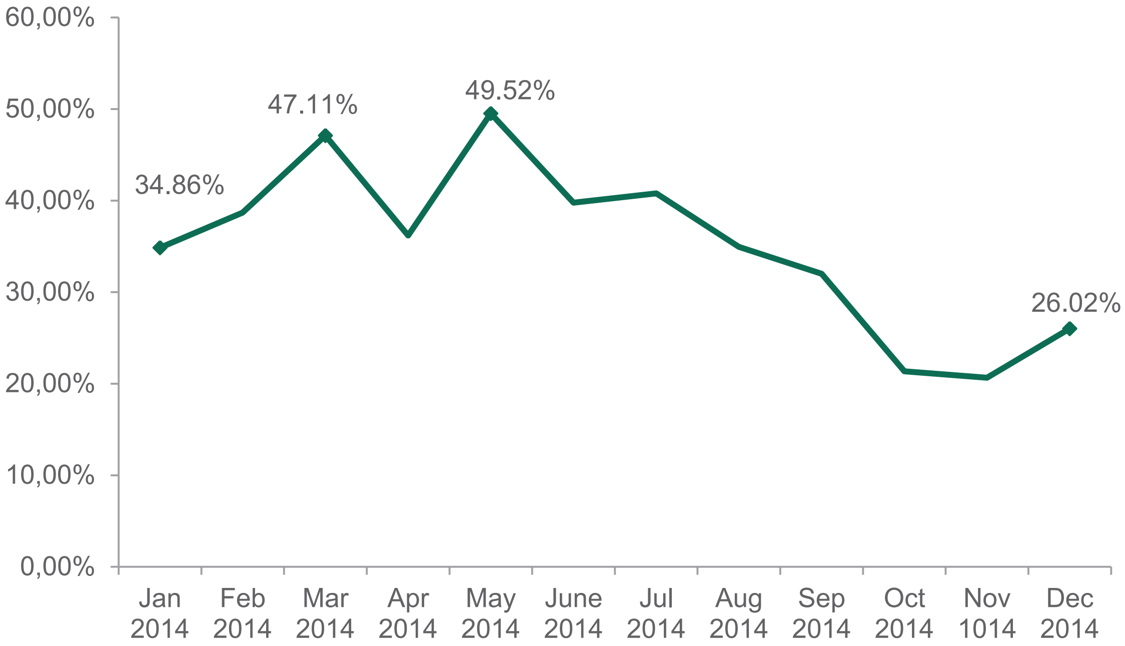

Fig. 12. Share of attacks with Zbot during the year

The change in the absolute number of attacks with Zbot is a good illustration of this process.

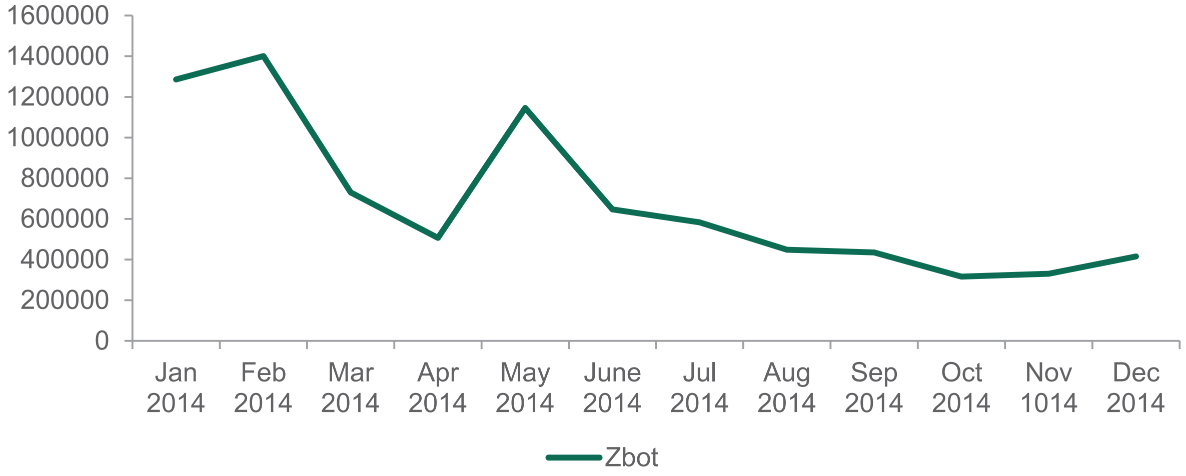

Fig. 13. Attacks with Zbot malware family during 2014

A noticeable and long-lasting period of decline started in June. At the beginning of that month the FBI and the US Department of Justice announced the shutdown of the ZeuS\Gameover botnet, one of the biggest botnets utilizing Zeus-malware. We believe that the decrease was provoked by this event.

The number of attacks utilizing Cridex worm, SpyEye Trojan, Carberp and several other malicious families also decreased, which also had a noticeable impact on the overall number of attacks and attacked users.

However, 2014 also saw the appearance of several new threats, which grew to become fairly prevalent.

In particular these were the ChePro and Lohmys Trojans.

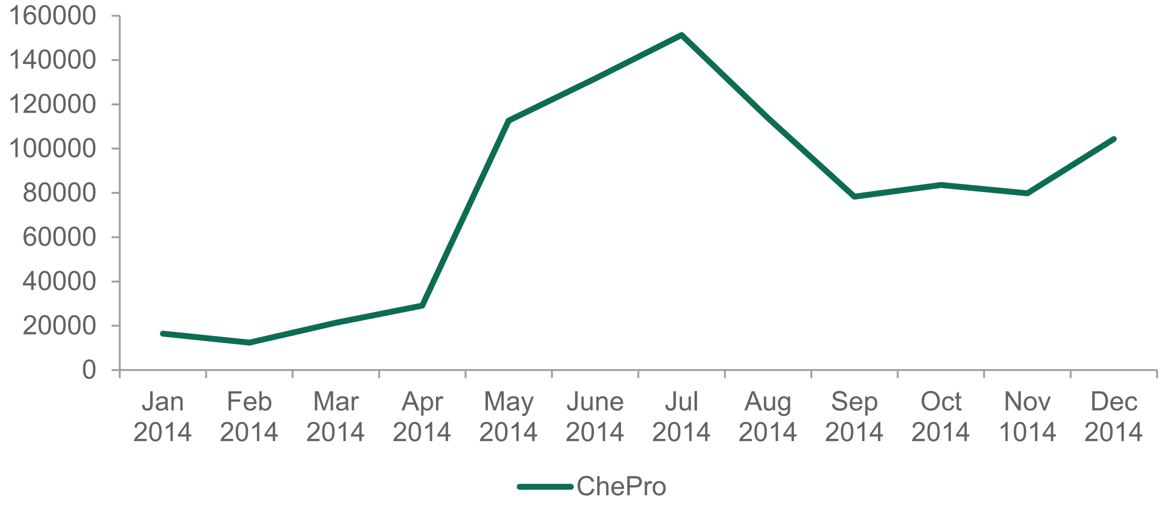

Fig. 14. Attacks with ChePro malware family in 2014

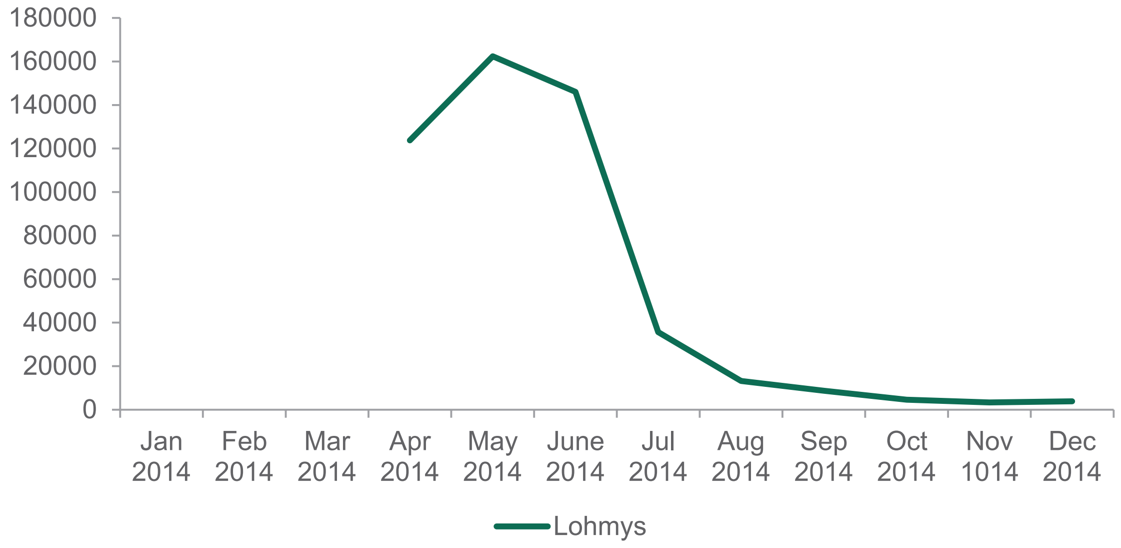

Fig. 15. Attacks with Lohmys malware family in 2014

Interestingly, although both these Trojans generated enough attacks to rank in the Global Top 10 of banking malware, they're hardly "global" in terms of geographical prevalence. Both families mostly targeted users in Brazil (more about that in Geography chapter).

Other financial threats: Keyloggers and Bitcoin malware

The timeline of Keylogger attacks demonstrated a steady decrease compared with 2013. This could reflect falling demand among cybercriminals for standalone keylogging functionality as they adopted more complicated all-in-one malware (like banking Trojans), which includes the capability to log keyboard strokes.

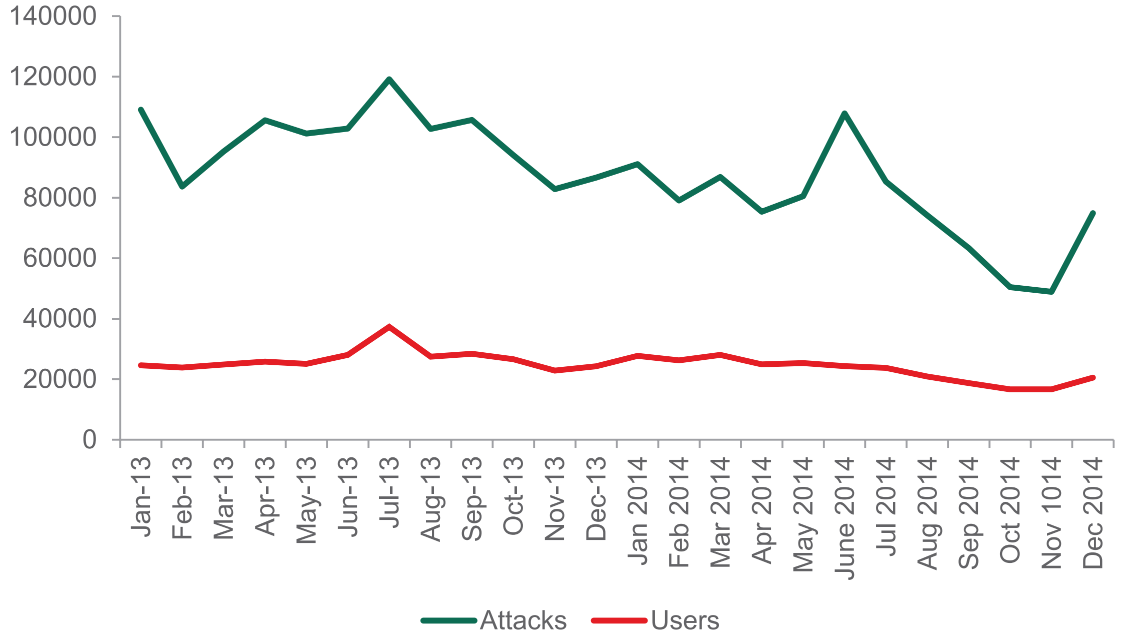

Fig. 16. Attacks with Keyloggers during 2013 and 2014

When it comes to Bitcoin malware, the situation is a little bit different. In 2014 the exchange rate for Bitcoins showed a drop from 772,530 USD on January 1st to 314,440 USD on December 31st.

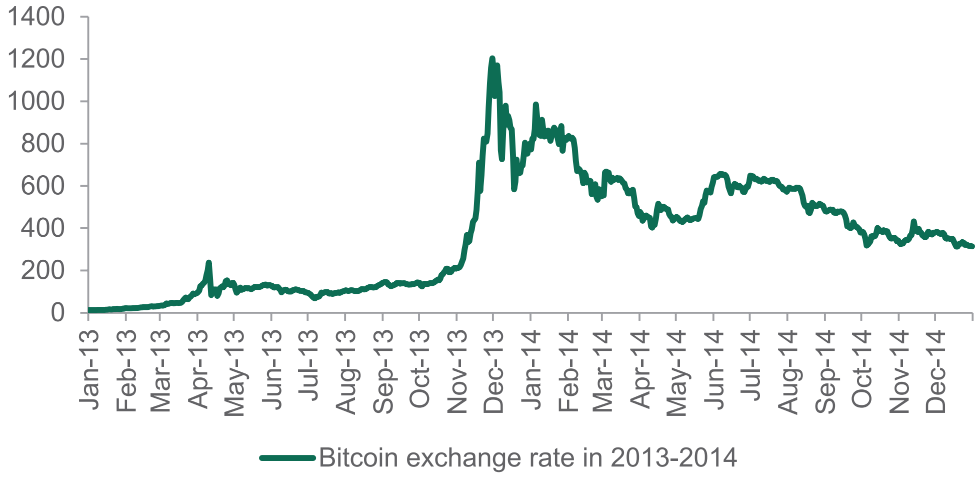

Fig. 17. Bitcoin exchange rate in 2013-2014

However, this did not reduce the efforts of cybercriminals to propagate Bitcoin-themed malware. Kaspersky Lab detected two types of such malicious programs. The first one was malware capable of installing the Bitcoin-mining software.

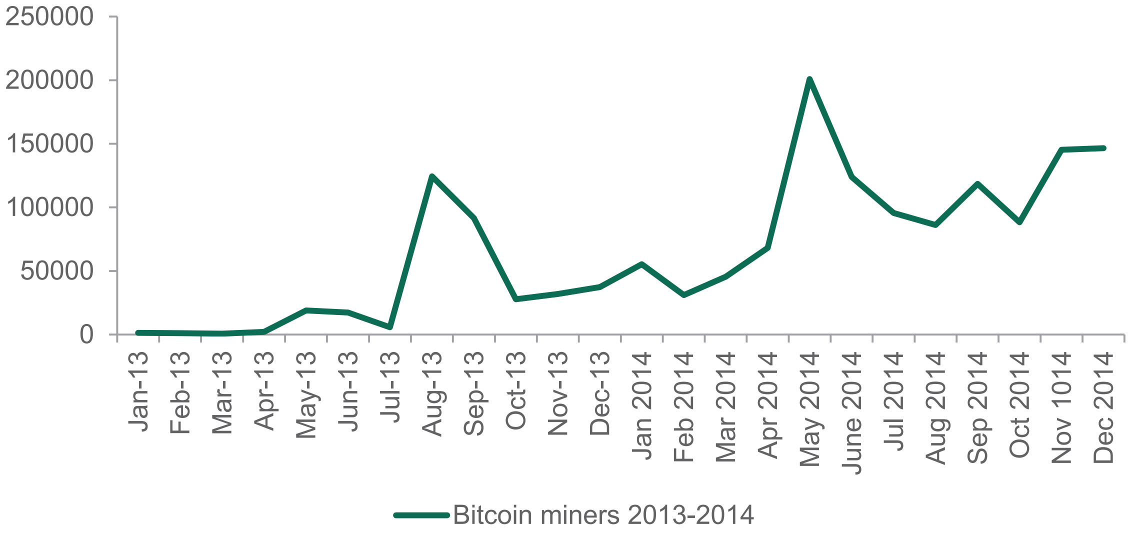

Fig. 18. Attacks with malware capable of installing Bitcoin mining software in 2013 and 2014

The number of attacks with Bitcoin-mining malware tripled: from 360,065 attacks in 2013 to 1,204,987 in 2014. It appears that criminals still found a reason to infect users' PCs with Bitcoin-mining software, despite the fact that the technical restrictions of the whole Bitcoin currency generation process make it really hard to generate a considerable amount of crypto money in a limited amount of time and with limited CPU resources. Another interesting thing is that criminals started to distribute the malware when the exchange rate was relatively high, but it took some time to become widespread.

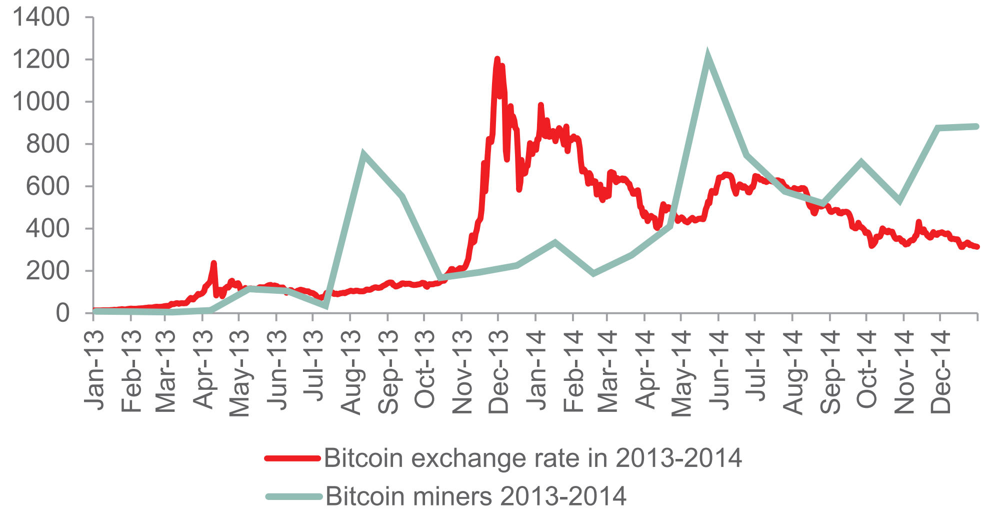

Fig. 18.1. Bitcoin exchange rate in 2013-2014 & Attacks with Bitcoin miners in 2013-2014

The second type of Bitcoin malware is malicious programs capable of stealing Bitcoin wallets.

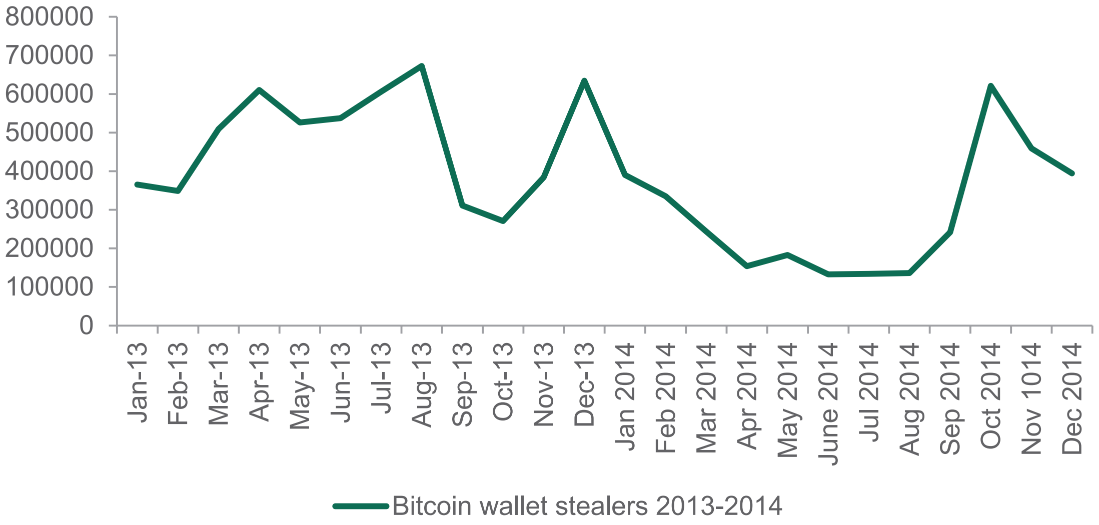

Fig. 19. Attacks with malware capable of stealing Bitcoin wallets in 2013 and 2014

The number of attacks containing Bitcoin wallet stealers decreased by 40.7% from 5,775,942 attacks in 2013 to 3,424,558 attacks in 2014. During the year the number of detections was fairly low; however Kaspersky Lab observed that between August and October there were a rising number of attacks carrying malware of this type. It is hard to determine the reason behind the ups and downs in the number of attacks with Bitcoin wallet stealers, but it is clear that Bitcoin wallets are of interest to cybercriminals who “generate” a continuous stream of no less than 100 000 attacks a month.

GEOGRAPHY OF FINANCIAL ATTACKS

In 2014, the Russian share of attacks decreased significantly – from 45.93%of attacks in 2013 to 29.97% – a fall of 15.96 percentage points; but that wasn't enough to move it from the top spot on the chart. Brazil jumped from 8th to 2nd place, Turkey moved from 5th to 3rd place and the US moved from 2nd place to 6th.

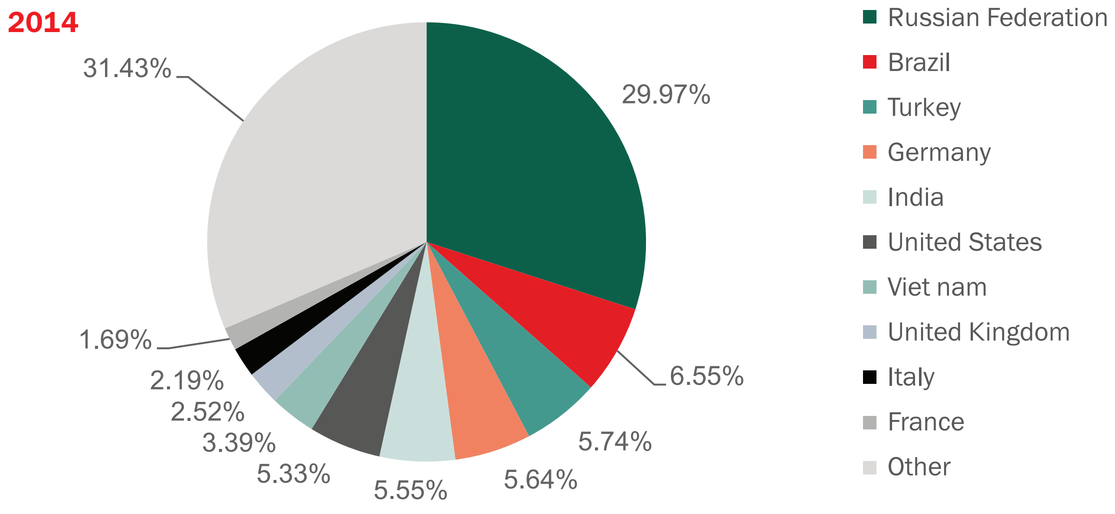

Fig. 20. Geographical distribution of attacks by financial malware in 2014[2]

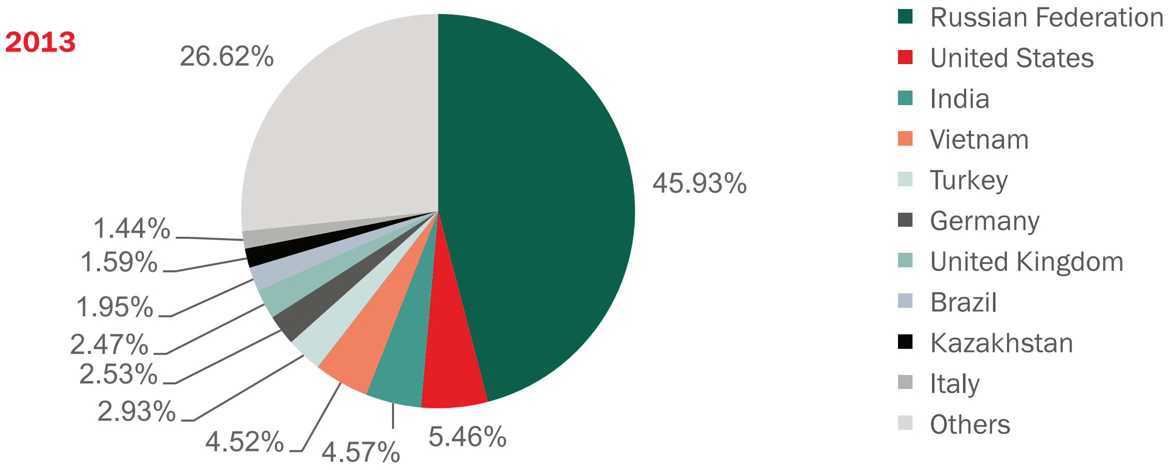

Fig. 21. Geographical distribution of attacks by financial malware in 2013

[2] 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

However, when we look at the number of users attacked by financial malware as a share of the overall number of users attacked with any malware, the situation is different. According to KSN statistics, one in five (20.05%) users in Brazil encountered financial malware in 2014. Turkey holds second place with 14.9% of users. Italy is in third place with 8.5% of users. Russia, which shows the highest number of attacks, is only in 8th place with 3.6% of users.

Country	% of users attacked by any type of malware in 2014	% of users attacked by any type of malware in 2013
Brazil	20.05%	10.4%
Turkey	14.9%	12.01%
Italy	8.5%	8.39%
United Kingdom	5.6%	5.6%
Germany	5.2%	5.5%
India	4.2%	6.7%
Vietnam	4.1%	7.4%
Russian Federation	3.6%	6.1%
France	2.1%	2.7%
United States	1.8%	3.1%

Table 2. Users attacked by financial malware as a share of the overall number of users attacked with any malware in 2013-2014

The number of attacks against users in the US declined significantly, as did the share of users attacked with financial malware. This was apparently caused by the behavior of the Zbot family. Attacks with this malware accounted for 75.54% of all malicious financial attacks registered in the country. The decrease of Zbot attacks led to an overall decrease in financial attacks in the US.

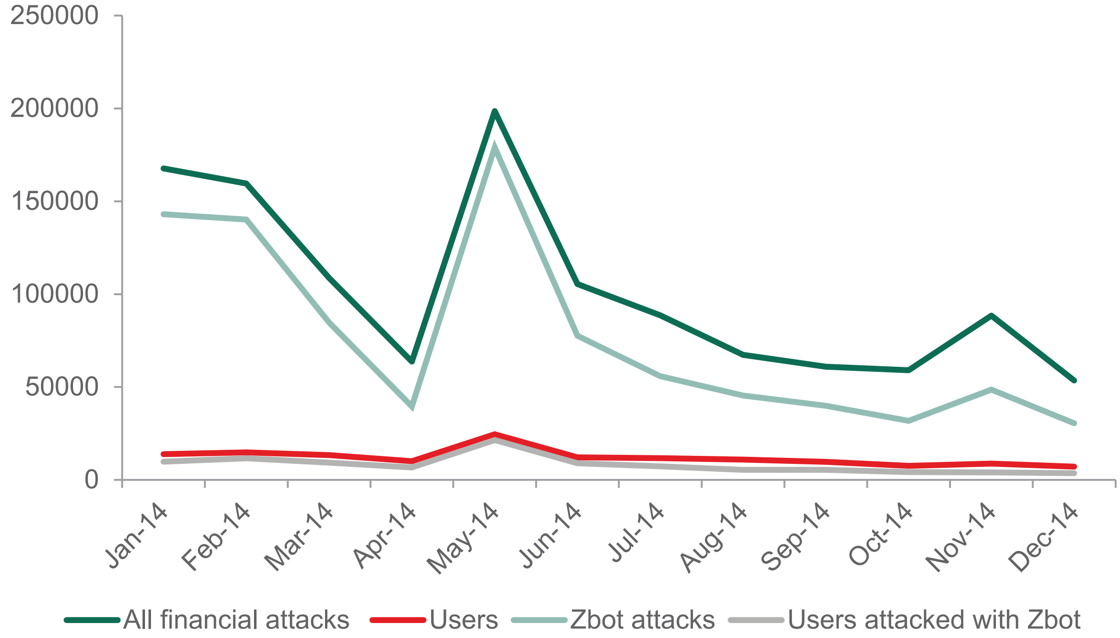

Fig. 22. Attacks with financial malware registered in the US during 2014

As the graph above shows, on the whole a financial attack in the US meant a Zbot attack. Other malicious financial programs showed extremely low levels of prevalence in the country.

It is important to point out that among the countries attacked most often with financial malware, the Zbot family is usually the leader. It holds first place in Russia (24.06% of attacks), Germany (43.35% of attacks), India (39.32% of attacks), the UK (59.75% of attacks), Italy (85.23%) and France (66.18%). However in several countries ZeuS is not on top of Mt Olympus. For instance, in Brazil.

From January to March 2014, the situation with financial malware in Brazil was relatively calm. But, starting in April, a significant leap in detections was registered.

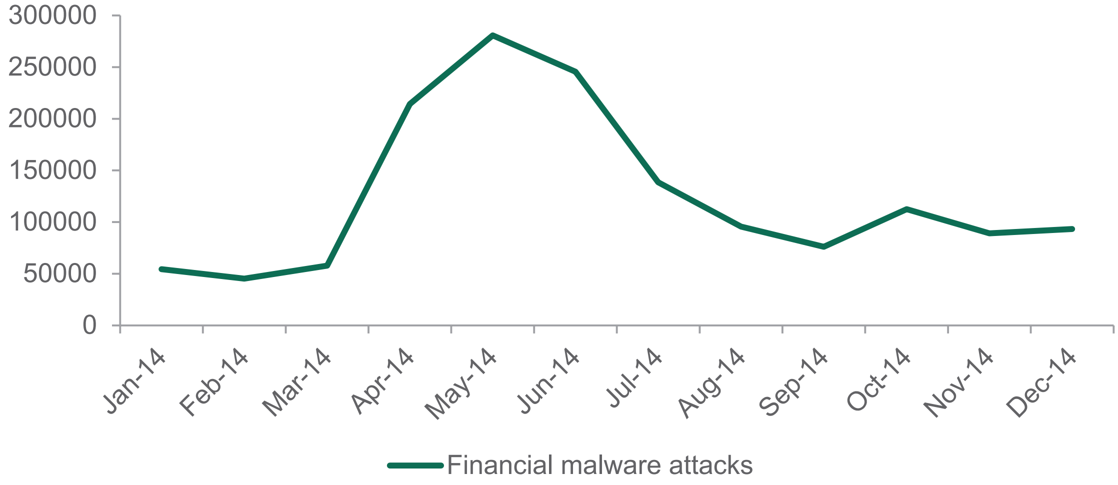

Fig. 23. Financial malware attacks registered in Brazil during 2014

A more detailed investigation of the situation showed that the increase was mostly down to the Trojan-Banker family.

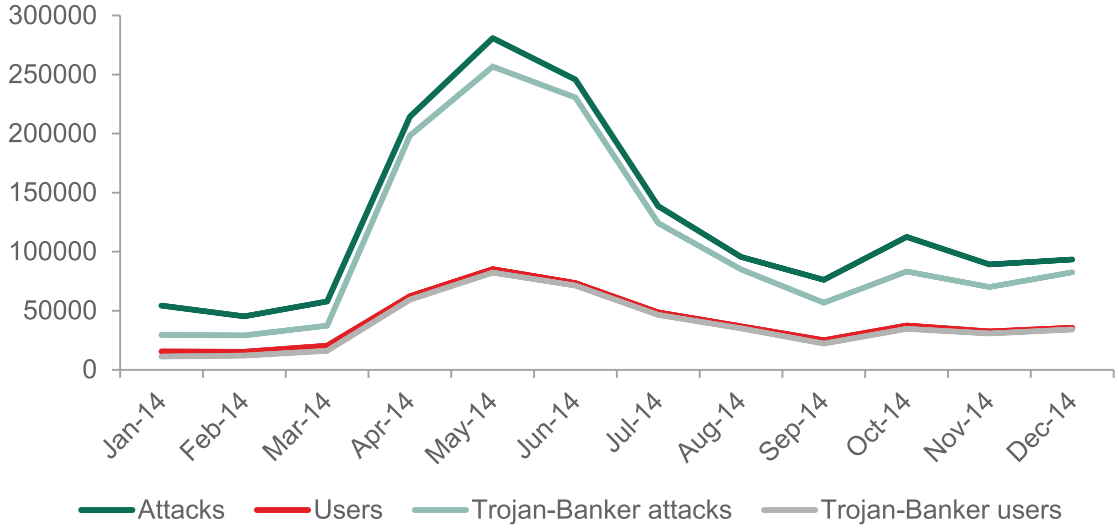

Fig. 24. Financial malware attacks in comparison with Trojan-Banker attacks in Brazil during 2014

Further analysis showed that the main reason behind the rise in the number of attacks was two malicious programs: ChePro and Lohmys.

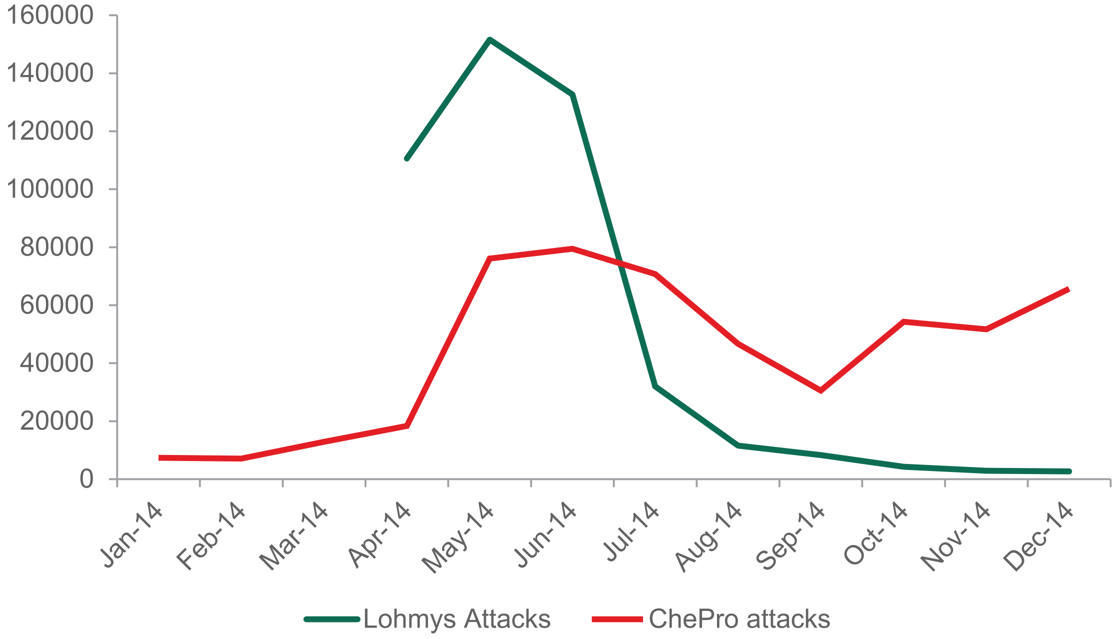

Fig. 25. Lomys and ChePro attacks registered in Brazil during 2014

Both families have the same functionality and are spread via spam messages with a theme related to online banking (for example, an invoice from an online banking service). The email includes a Word document with a picture attached: and clicking on the picture launches the malicious code execution. These two threats topped the list for the most prevalent financial malware in Brazil. And while the period of activity of Lohmys was relatively short: from April to June, ChePro Trojan continued to attack Brazilian users throughout the entire year.

ANDROID FINANCIAL THREATS

In 2014, Kaspersky Lab and Interpol released a joint study on Mobile cyberthreats which – among other things – covered financial malware targeting Android users. According to the study findings, there were 3,408,112 attacks against 1,023,202 users registered in the period from August 1st, 2013 to July 31st 2014. About 500,000 users had at least once encountered mobile malware designed to steal money. Interestingly enough, although 59.06% of all malicious attacks against Android users were generated by malware aimed at stealing users' money (Trojan-SMS and Trojan-Banker), Kaspersky Security Network actually detected a noticeable decrease in such attacks during the second half of the period, due to the rapid collapse of Trojan-SMS detections in spring 2014. One possible reason for the fall in the number of Trojan-SMS attacks was mobile-phone operators in Russia (the main source of Trojan-SMS threat) adopting an Advice of Charge (AoC) mechanism. This means that 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.

More than half a year has passed since the end of the period covered by the Kaspersky Lab and Interpol study, and this is how things have changed since then.

During 2014 Kaspersky Lab Android products blocked a total of 2,317,194 attacks against 775,887 users around the world. The lion's share of these attacks (2,217,979 attacks against 750,327 users) used Trojan-SMS malware and the rest (99,215 attacks against 59, 200 users) used Trojan-Banker malware.

Together, attacks with Trojan-SMS and Trojan-Banker malicious programs accounted for 48.15% of all attacks against Android users detected by Kaspersky Lab in 2014.

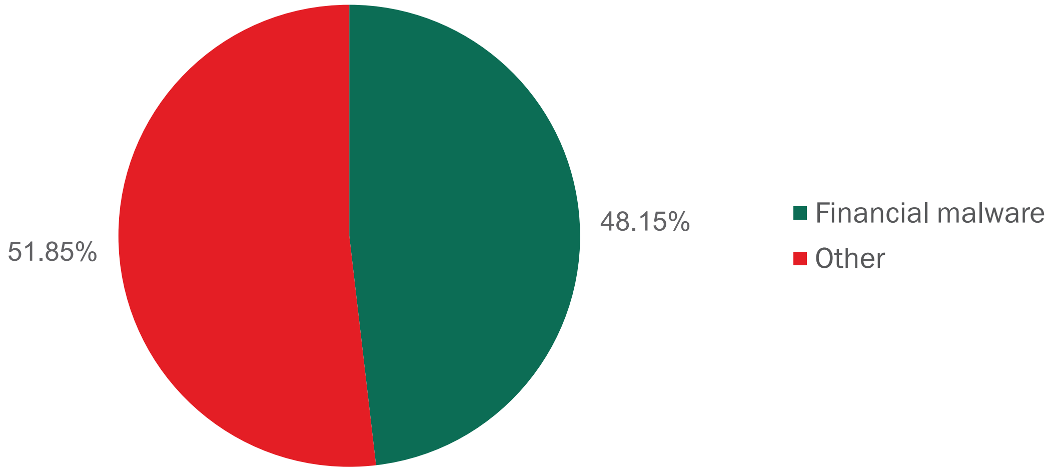

Fig. 26. Share of financial attacks against users of Android-based devices in 2014

Compared with 2013, the number of financial attacks against Android users grew 3.25 times (from 711,993 to 2,317,194 attacks) and the number of attacked users rose 3.64 times (from 212,890 to 775,887 users).[3]

[3] It should be emphasized that in 2014 the number of Kaspersky Lab's Android product users tripled in comparison with 2013.

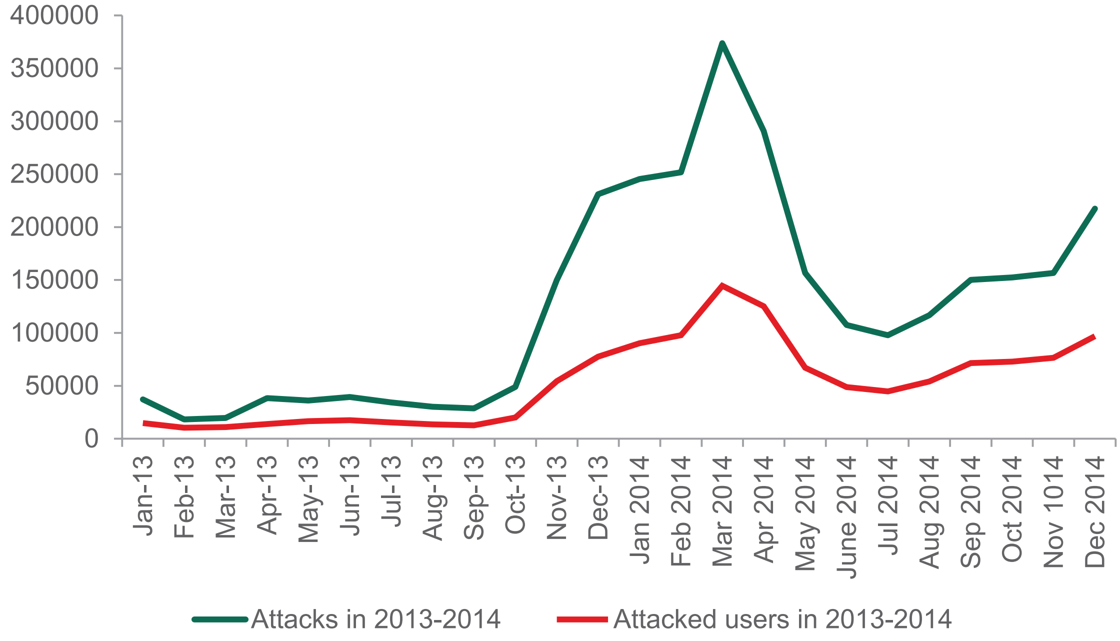

Fig. 27. Financial attacks against users of Android-based devices in 2013 and 2014

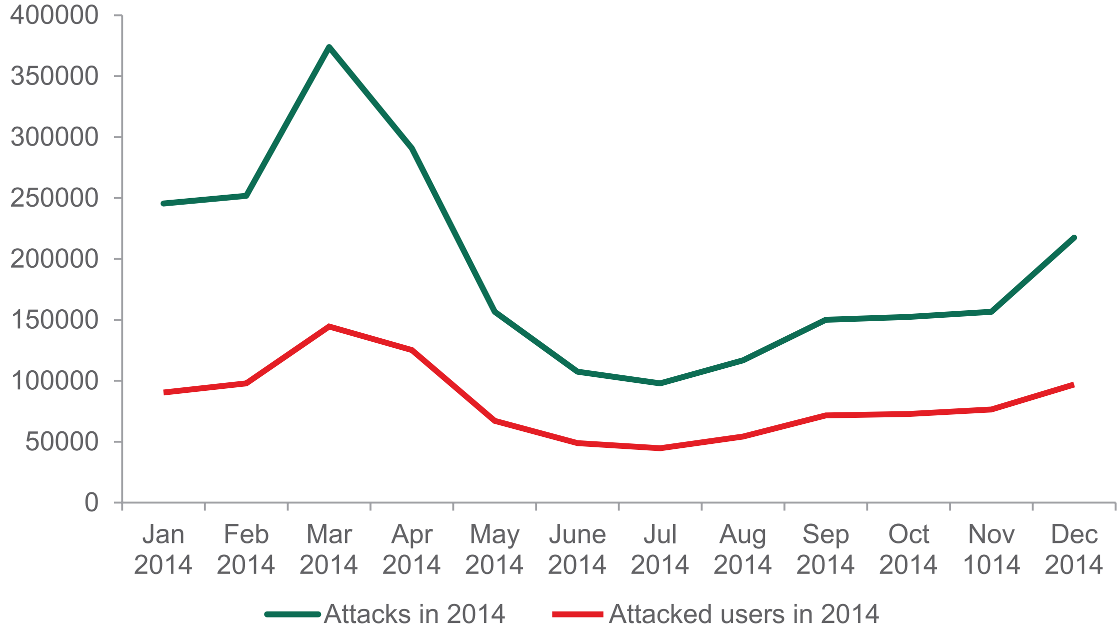

Fig. 28. Financial attacks against users of Android-based devices in 2014

The decrease in attacks that was noted in our previous report ended in July and was followed by a steady increase throughout the rest of the year. The growth speeded up in December, traditionally a "high" season for merchandise and for criminals targeting financial data. It's too early to determine if the December increase in the number of attacks and attacked users could be the sign of a Trojan-SMS resurrection, but according to Kaspersky Lab experts, it is technically possible. They have already seen examples of malware capable of infection and theft even with AoC implemented in the cellular network. For example, such functionality was discovered recently by Kaspersky Lab experts in Opfake.a and Fakeinst malware modifications. Both are very active Trojan-SMS representatives.

Although the Trojan-Banker contribution to the overall volume of financial attacks against Android users is relatively small, it continues to grow.

During the year Kaspersky Lab products detected 20 different malicious programs from Torjan-Banker. But there were only three star performers among them: Faketoken, Svpeng and Marcher. Svpeng and Marcher are capable of stealing credentials for online banking and credit card information by replacing the authentication fields of mobile banking apps and app stores apps on an infected device. And Faketoken is made for intercepting mTAN codes used in multifactor authentication systems, and forwarding it to criminals.

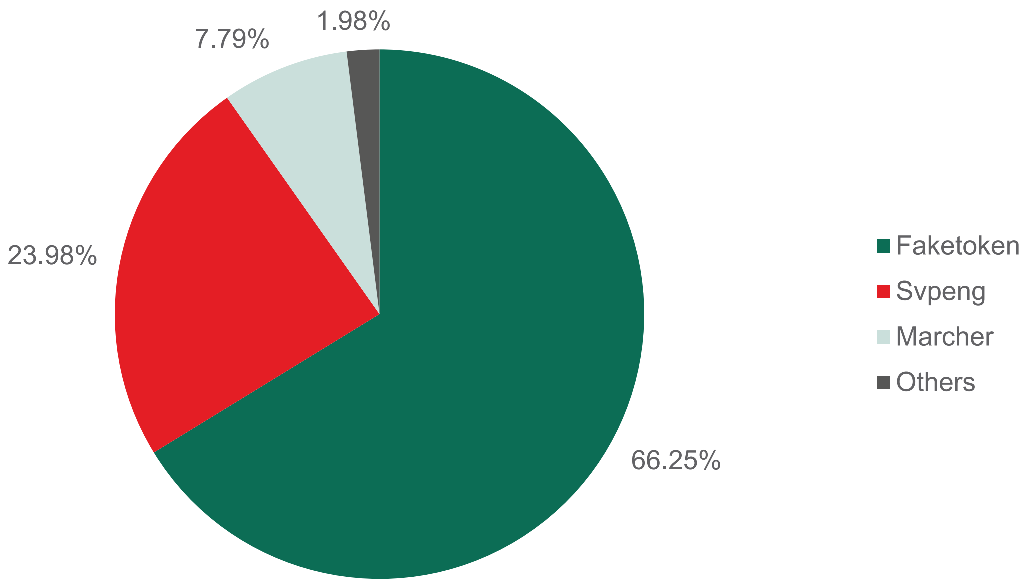

Fig. 29. Distribution of attacks with three main Android banking malware families

These three families accounted for 98.02% of all Trojan-Banker attacks. From April to October all three programs were relatively quiet in the wild, but with the beginning of the holiday season the criminals behind these malware became active and the number of attacks started to grow.

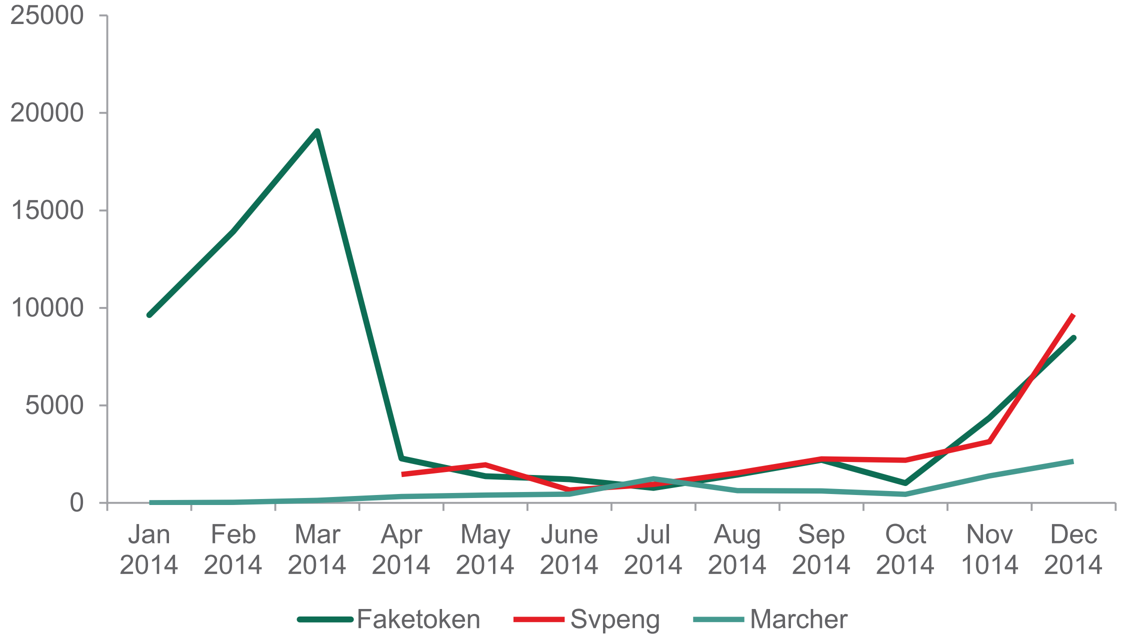

Fig. 30. Attacks with main Android banking malware families in 2014

The geography of financial attacks using financial malware comes as no surprise. Russia is the number one target with 63.87% of Trojan-SMS and Trojan-Banker attacks. It is followed by Kazakhstan (5.67%), Ukraine (2.95%), Germany (2.78%) and Malaysia (2.69%).

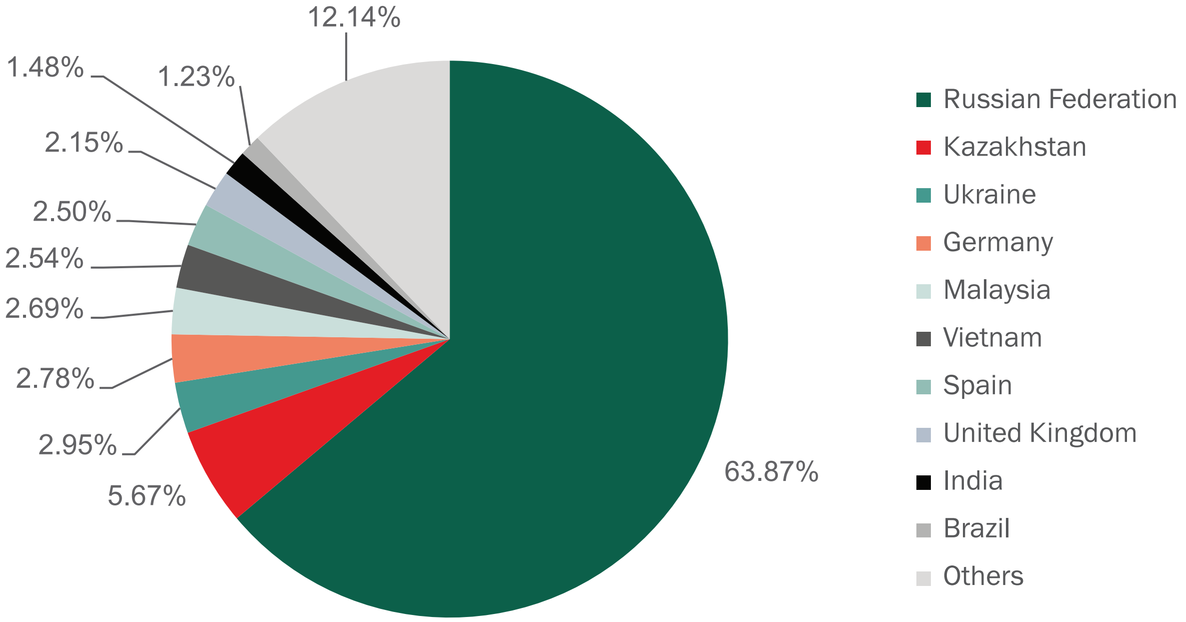

Fig. 31. Geographical distribution of attacks with financial malware targeting users of Android-based devices in 2014

When it comes to comparing the number of users attacked with financial malware with the number of users of Android-based devices attacked with any malware, the situation is slightly different. Russia and Kazakhstan swap places, followed by Spain, Ukraine and Malaysia with 63.3%, 60.5% and 58.4% of users respectively encountering financial threat.

Country	% of users attacked by any type of malware
Kazakhstan	71.7%
Russan Federation	71.1%
Spain	63.3%
Ukraine	60.5%
Malaysia	58.4%
United Kingdom	50.9%
Vietnam	46.3%
Germany	41.7%
Brazil	38,20%
India	9,40%

Table 3. Users of Android-based devices attacked by financial malware as a share of the overall number of users of Android-based devices attacked with any malware in 2014

Most of these countries are top targets for financial attacks because of the popularity of prepaid mobile contracts and premium SMS services – two factors that attract the attention of cybercriminals specializing in SMS-fraud schemes, because they make it easy to steal money direct from the user’s mobile account. That is why users from these countries should be especially cautious when it comes to the mobile applications they install on their devices.

▶ CONCLUSIONS AND RECOMMENDATIONS

The study shows that the risk of losing money online is still a very real one for millions of users worldwide: the share of malware attacks targeting online banking credentials rose significantly in 2014 along with the average intensity of attacks. It also shows that more and more users of Android-based devices are becoming a target of financial attacks, and reveals the direction in which criminals are heading in an attempt to get more illegal income. To help you protect yourself reliably against cyberthreats Kaspersky Lab experts make the following recommendations:

Home users

- Do not click on any links received from unknown people or suspicious links sent by your friends on social networking sites or via e-mail;
- Do not download, open or store unfamiliar files on your device;
- Do not use unreliable (public) Wi-Fi networks to make online payments;
- Always check the authenticity of any site before entering your data; at the very least, check the address of the site in the address bar to make sure it matches the official site of the organization;
- Only use sites which run with a secure connection (the address of the site should begin with HTTPS:// rather than HTTP://);
- While performing financial transactions online try to use multifactor authentication technology (one-time passwords, etc.) and, where possible, avoid services that do not use these technologies;
- Android-based mobile devices are an attractive target for cybercriminals, particularly in countries where prepaid mobile contracts and e-payments via premium SMS are widely used. To this effect, it is necessary to comply with at least a few basic safety rules for these devices: prevent the installation of applications from third-party stores and ensure you have the latest version of the operating system installed on your smartphone or tablet.
- Cryptocurrencies attract a lot of cybercriminal interest, so if you are a Bitcoin wallet holder, be sure to look after it: do not keep your Bitcoins in one wallet; if possible, store the wallet on an external media in an encrypted form. Do not use online services to store cryptocurrency.
- When working with a computer or a mobile device, use reliable security solutions that offer additional protection technology for online financial transactions in addition to traditional anti-malware, anti-phishing and other technologies.

Businesses

- To avoid the possible loss of financial data it is recommended that organizations not only use reliable security solutions on all workstations in the company, but also establish different policies for different categories of users and track user activity logs on their corporate devices;
- Use mobile device management systems to control which devices can be used in what way by which employees during financial transactions, and to protect them from possible cyberthreats;
- While performing financial transactions online try to use multifactor authentication technology (one-time passwords, etc.) and, where possible, avoid services that do not use these technologies;
- As the sophistication of financial cyberthreats and the methods used by online fraudsters increase all the time, do not forget to update all security solutions and anti-threat measures on a regular basis;
- Do not overlook the importance of teaching employees (especially those working with finances) the basics of cybersecurity;
- For financial services companies, it is recommended that a specialized anti-fraud solution is deployed both inside their infrastructure and on user devices including mobile ones – it helps to prevent possible financial attack rather than remediate it and, as result, prevents financial and reputational damage to the company itself.

▶ METHODOLOGY

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, information for a new threat is added to databases within minutes of a previously unknown threat being discovered. KSN's other function is to process de-personalized 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 (Windows and Mac OS X) and malware on Windows-based devices and mobile malware on Android-based devices. In addition it looked at statistics about the number of users attacked. The research also analyzed information about the geographic spread of the attacks.

The research covers the entire year of 2014; and the data was analyzed in comparison with the equivalent data collected in 2013. One of subjects of the research was 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 2014, Kaspersky Lab's experts separated threats associated with the generation and stealing of this currency into a separate category, and followed their evolution.

▶ NOTE ON RESPONSIBLE DISTRIBUTION OF INFORMATION

This document presents an analysis of the cyber-threat landscape as it relates to Windows and Android-based platforms. It is based on information about instances of Kaspersky Lab security products detecting applications and webpages 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 or webpage considered malicious or phishing one 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 as part of this study rely exclusively on data from Kaspersky Lab's customer community, which exceeds 80 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.

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

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

KASPERSKY lab