KASPERSKY lab

Financial Cyberthreats in 2016

February, 2017

Introduction and Key Findings

The financial cyberthreat landscape is constantly changing. In the last couple of years, financial cybercriminals have shifted their focus from attacks against the private users of online banking, e-shops and payment systems, to attacks on the infrastructure of large organizations: banks and payment processing systems, along with retailers, hotels and other businesses where POS terminals are widely used.

This increase in the number of attacks against large organizations could be explained by the fact that although the preparation and execution costs of such attacks are relatively high, the outcome may be a hundred times greater than the result of even the most successful malicious campaign against private users. This theory has been proved by the Carbanak financial cybercrime group and its "followers", including the so-called SWIFT hackers, who were responsible for the majority of big financial cybercrime incidents in 2016. Using non-trivial attack methods, and reducing to a minimum the use of unique malicious software in favor of open sourced tools, these groups have been able to steal millions of dollars and, unfortunately, they have not yet been caught.

However, even though professional criminals have shifted their crosshairs to the big fish, this doesn't mean that regular users and small and medium-sized businesses are no longer at risk of falling victim to financial cybercrime. On the contrary: after detecting a decrease in the number of attacked users in 2014 and 2015, the number of victims started to grow again in 2016. This report is dedicated to providing an overview of how the financial threat landscape has evolved during the last year. It covers the phishing threats that users of Windows-based and macOS-based computers encounter, and Windows-based and Android-based financial malware.

The key findings of the report are:

Phishing:

- In 2016 the share of financial phishing increased 13.14 percentage points to 47.48% of all phishing detections. This result is an all-time high according to Kaspersky Lab statistics for financial phishing caught on Windows-based machines.
- Every fourth attempt to load a phishing page blocked by Kaspersky Lab products is related to banking phishing.
- The share of phishing related to payment systems and e-shops accounted for 11.55% and 10.14% accordingly in 2016. This is slightly (single percentage points) more than in 2015.
- The share of financial phishing encountered by Mac users accounted for 31.38%.

Banking malware:

- In 2016 the number of users attacked with banking Trojans increased by 30.55% to reach 1,088,900.
- 17.17% of users attacked with banking malware were corporate users.
- Users in Russia, Germany, Japan, India, Vietnam and the US are the ones most often attacked by banking malware.
- Zbot is still the most widespread banking malware family (44.08% of attacked users) but in 2016 it was actively challenged by the Gozi family (17.22%).

Android banking malware:

- In 2016 the number of users that encountered Android malware increased 430% to reach 305,000 worldwide. This is mostly due to a single Trojan which has been exploiting a single security flaw in a popular mobile browser for months.
- Just three banking malware families accounted for attacks on the vast majority of users (81%).
- Russia, Australia and Ukraine are the countries with the highest percentage of users attacked by Android banking malware.

Financial Phishing

Financial phishing is one of the most widespread types of cybercriminal activity. Among all existing types of cybercrime, phishing is the most affordable in terms of the investment and level of technical expertise required. At the same time it is potentially profitable - in most cases, as a result of a successful phishing campaign, a criminal would receive enough payment card credentials to cash out immediately, or sell the details to other criminals for a good price. Perhaps this combination of technical simplicity and effectiveness makes this type of malicious activity attractive to amateur criminals, a pattern that we can clearly see in Kaspersky Lab's telemetry systems.

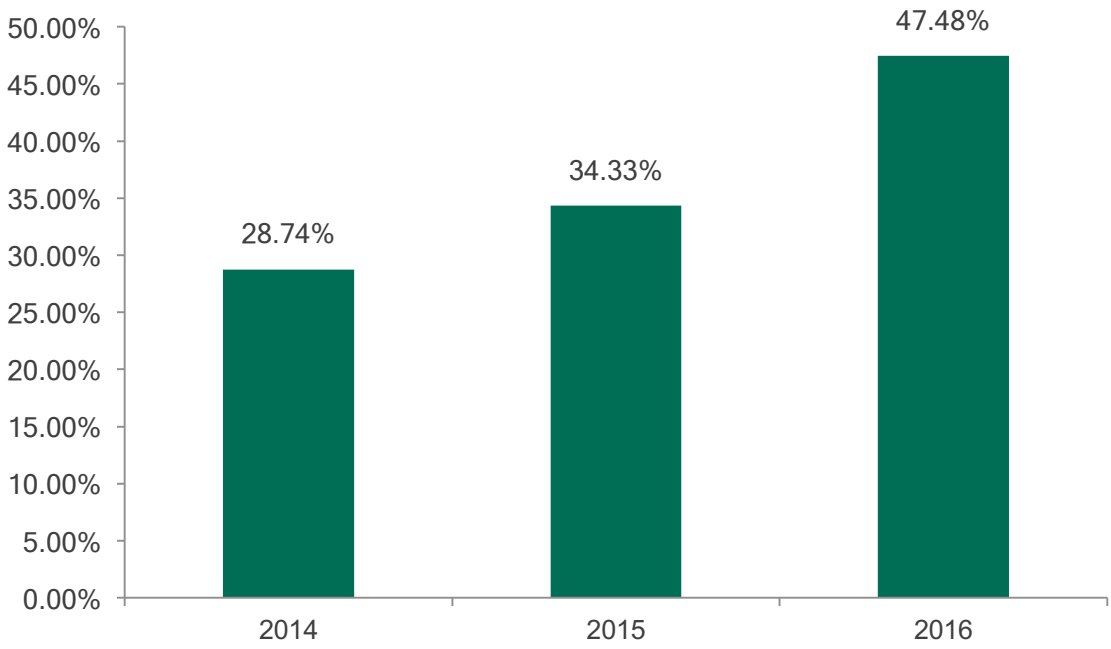


Fig. 1: The percentage of financial phishing detected by Kaspersky Lab in 2014-2016

In 2016 Kaspersky Lab's anti-phishing technologies detected 154,957,897 attempts to visit different kinds of phishing pages. Of those, 47.48% of heuristic detections were attempts to visit a financial phishing page. This is 13.14 percentage points more than the share of phishing detections registered in 2015 when 34.33% of them were related to financial fraud. At the moment this is the highest percentage of financial phishing ever registered by Kaspersky Lab.

Moreover, for the first time in 2016, the detection of phishing pages which mimicked legitimate banking services took first place in the overall chart, leaving the longtime leaders of this chart – global web portals and social networks - behind. In 2014 every fourth phishing page detected was a fake online banking page or other content related to banks. However in 2016, the result was 8.31 percentage points higher than in 2015.

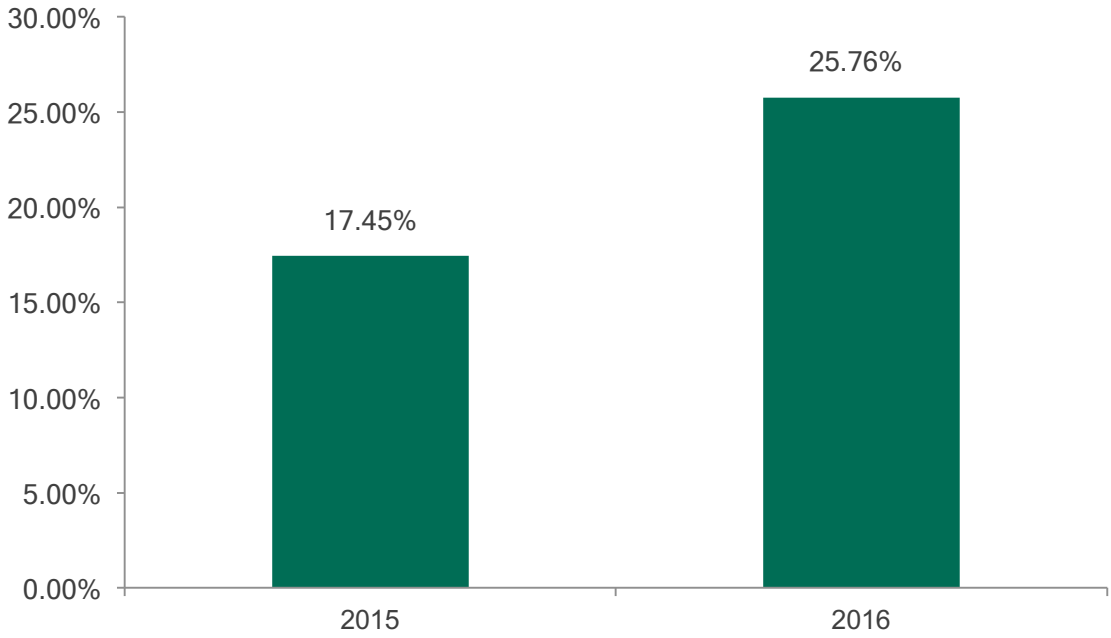


Fig. 2: The percentage of banking phishing detected by Kaspersky Lab in 2015-2016

At Kaspersky Lab we categorize several types of phishing pages as “financial”. Besides banks there is also the category of “Payment Systems”, which includes pages that are mimicking well-known payment brands such as PayPal, Visa, MasterCard, American Express and others. There is also the “E-shop” category which includes Internet shops and auctions like Amazon, Apple store, Steam, E-bay and others.

In 2016 both the “E-shop” and “Payment Systems” categories also showed visible growth. The share of phishing against payment systems increased by 3.75 p.p. and the attacks against e-shops increased 1.09 p.p. in comparison to results in 2015.

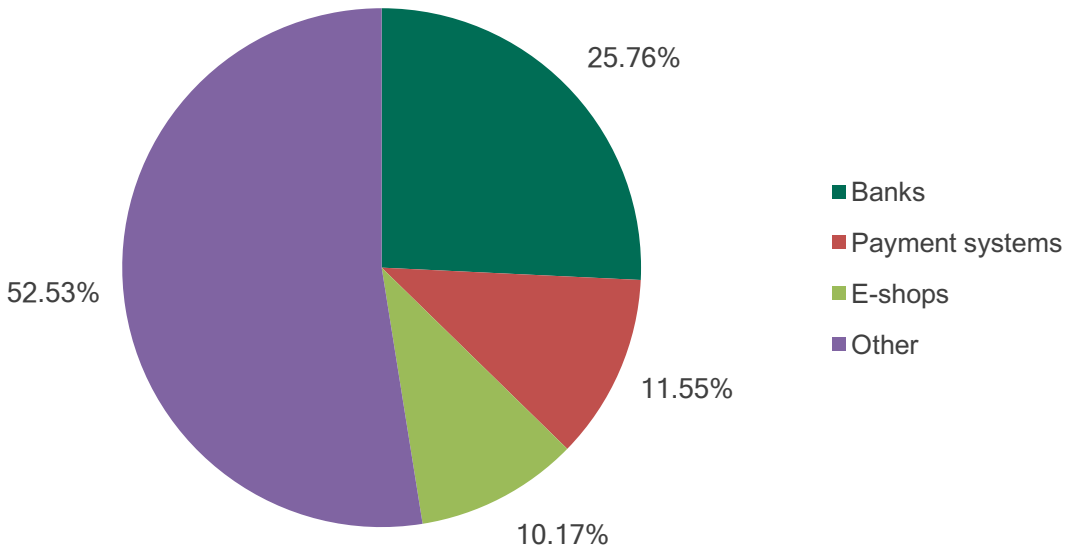


Fig. 4: The distribution of different types of financial phishing detected by Kaspersky Lab in 2016

The list of targets presents no surprises. Among the financial phishers' favorite targets are top transnational banks, popular payment systems and Internet shops and auctions from the US, China and Brazil. The list of those targets remains the same from year to year as the popularity of these brands remains a high and therefore lucrative target for cybercriminals.

Financial phishing on Mac

MacOS-based computers are generally considered to have a much safer platform than Windows. This is because the number of malware families existing for this operating system is lower than the amount of Windows malware. However, experts often forget that phishing threats don't care what OS the victim's device is running. Kaspersky Lab's statistics show that MacOS users often face phishing threats - if not with the same frequency as Windows users.

In 2016 31.38% of phishing attacks against Mac-users were aimed at stealing financial data. This is much less than in 2015, when 51.46% of financial attacks blocked by Kaspersky Lab were financially-themed. However, the 2015 situation was somewhat abnormal due to a huge amount of detections against a single international bank. The amount was so large that this bank moved to first place among the brands most often used in phishing scams encountered by Mac-users, leaving the usual "leaders" in the overall ratings (popular search engines and social networks) far behind.

In 2016 the wave of attacks against that bank decreased, bringing the overall share of financial phishing to a more realistic level. Still, 31.38% means that one in three phishing attacks blocked on Macs were trying to lure victims into sharing their financial information.

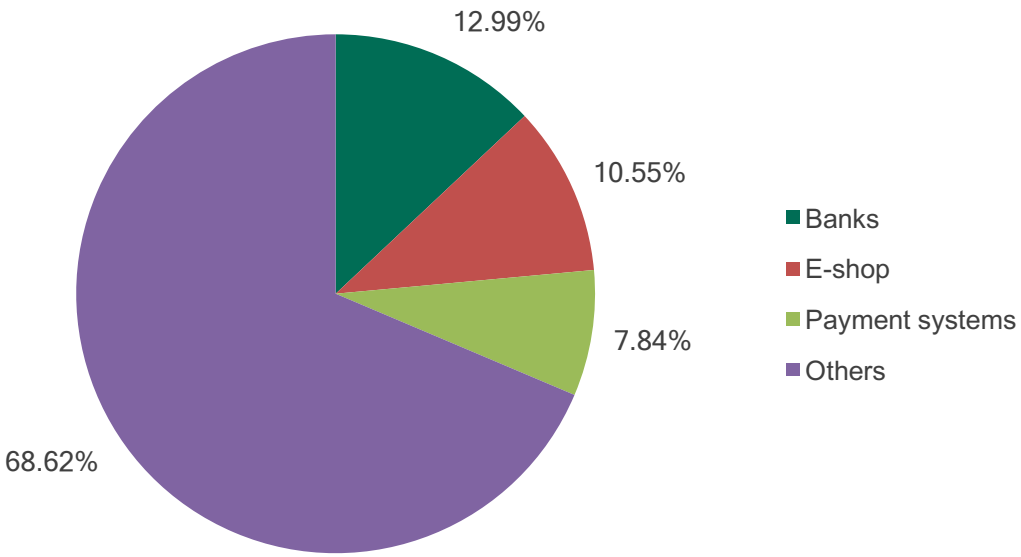


Fig. 5: the distribution of phishing attacks against Mac users in 2016

This bank, which was in the crosshairs of criminals in 2015, is still the primary target of banking phishing, but the number of attacks is much lower.

Mac vs Windows

We also detected one allegedly platform-related feature of the financial phishing landscape on Mac. Based on the phishing page detection statistics from Windows-based computers, the list of the most frequently used brands in the e-shop category is topped by Amazon – a longtime category “leader”. However, when it comes to Mac-phishing the leader is Apple. The latter is easy to explain: Apple’s ecosystem includes a number of recognizable and generally trusted web services, like iCloud, iTunes, AppStore and Apple Store. Criminals are aware of that trust and try to exploit it.

When it comes to the e-commerce and payment systems categories, the particular focus on Apple is not the only difference between the Mac and Windows financial phishing threat landscapes.

Mac	Windows
Apple	Amazon.com
Amazon.com	Apple
Global Sources	Steam
Alibaba Group	eBay
eBay	Taobao
Steam	Alibaba Group
Netsuite	Bell Canada
Bell Canada	NOVA PONTOCOM
Bharti Airtel Limited	Wal-Mart

Fig. 6: The most frequently used brands in "E-shop" financial phishing schemes

Mac	Windows
PayPal	PayPal
American Express	Visa Inc.
MasterCard	American Express
Visa Inc.	MasterCard
qiwi.ru	Western Union
Xoom	qiwi.ru
NACHA	Cielo S.A.
Skrill Ltd.	Skrill Ltd.
Western Union	eWallet

Fig. 7: The most frequently used brands in "Payment Systems" financial phishing schemes

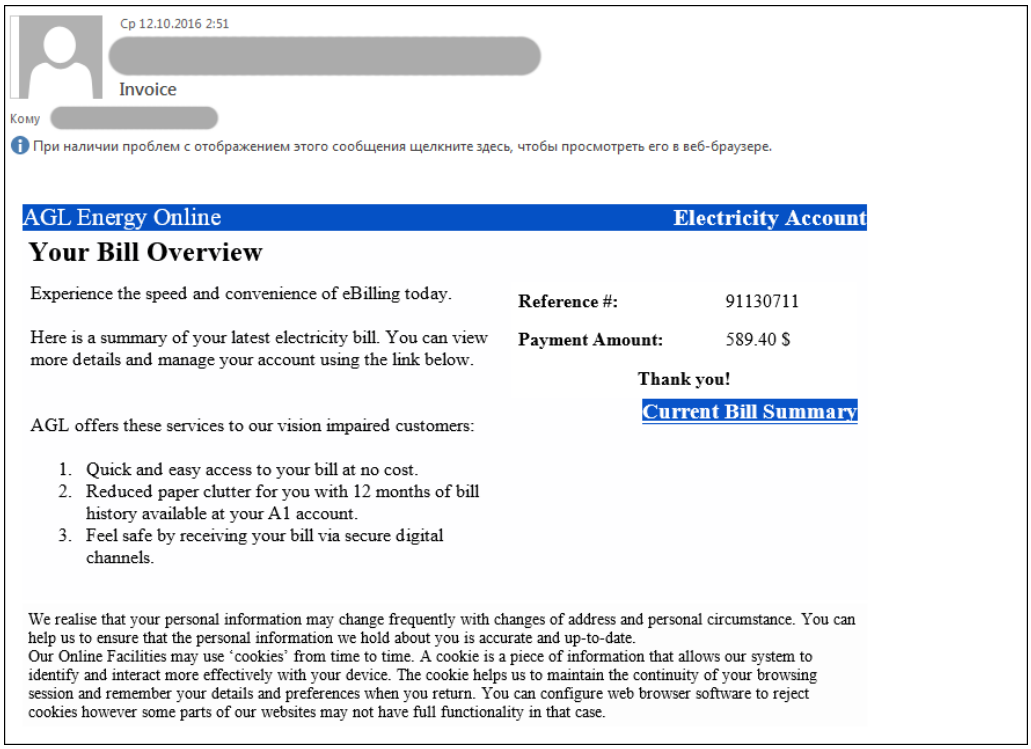
It is really hard to explain why the target profile on Macs is different to the one on Windows. It could be due to a difference in the consumer habits of Windows and Mac users, or it could be just the result of the distribution of Kaspersky Lab product users. However, the tables above can serve as an advice list for the users of the corresponding systems: they illustrate that criminals will use these well-known names in an attempt to illegally obtain user payment card, online banking and payment system credentials.

Phishing campaign themes

Besides a growing interest in phishing among amateur cybercriminals, the increase in financial phishing attacks may be explained by a rather “natural” reason: a rise in the use of online banking, e-shops and payment systems. With the audience for these services growing, it is also probable that the number of financial phishing detections will increase.

This is the conclusion drawn from the topics that criminals use in their scams. The list of topics is not limited to fairly old copies of online banking, payment systems or Internet shop web pages.

For example, in 2016 Kaspersky Lab analysts witnessed campaigns in which criminals disguised their phishing message as an e-mail from an electricity provider.


Ср 12.10.2016 2:51

Invoice

Кому

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

AGL Energy Online — Electricity Account

Your Bill Overview

Experience the speed and convenience of eBilling today.

Here is a summary of your latest electricity bill. You can view more details and manage your account using the link below.

Reference #: 91130711

Payment Amount: 589.40 $

Thank you!

Current Bill Summary

AGL offers these services to our vision impaired customers:

1. Quick and easy access to your bill at no cost.
2. Reduced paper clutter for you with 12 months of bill history available at your A1 account.
3. Feel safe by receiving your bill via secure digital channels.

We realise that your personal information may change frequently with changes of address and personal circumstance. You can help us to ensure that the personal information we hold about you is accurate and up-to-date.
Our Online Facilities may use ‘cookies’ from time to time. A cookie is a piece of information that allows our system to identify and interact more effectively with your device. The cookie helps us to maintain the continuity of your browsing session and remember your details and preferences when you return. You can configure web browser software to reject cookies however some parts of our websites may not have full functionality in that case.

Fig. 8: The phishing message sent in the name of an electricity company.

The message contained the link to an external page, where the electricity bill summary was allegedly displayed. Of course that wasn’t real, the website actually belonged to a criminal and was built to collect critical user information.

In another example criminals exploited the ability to transfer money from cards issued by one bank, to cards issued by another, with no or minimal fee. Such services are popular in Russia and some neighboring countries.

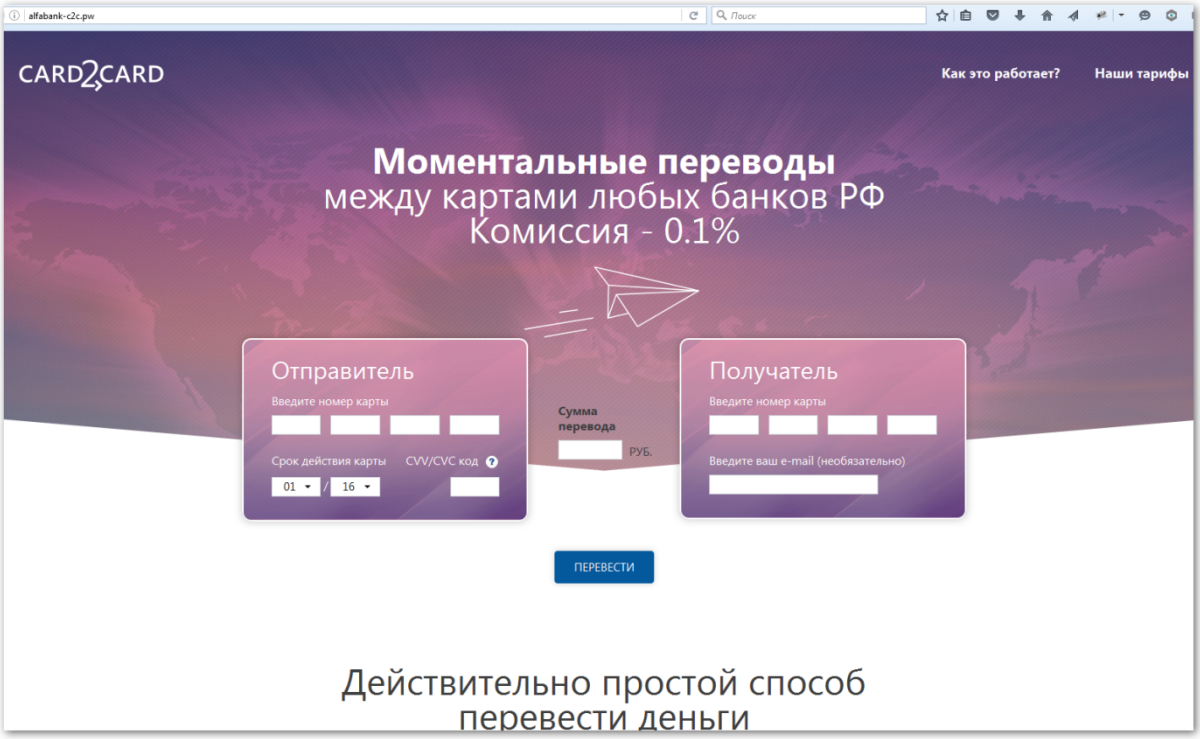


Fig. 9: A fake service offering quick card-to-card transfers with no additional fees

In this case fraudsters went to considerable efforts to build a website that looked very professional, and which bluntly asks visitors to insert all possible information about their plastic card from which money is supposed to be taken, as well as basic data about the card to which money should be transferred. Even though websites with such design parameters have been taken down multiple times in previous years, the criminals behind them have been persistent and have resurrected their websites on new domains over and over again. This, in itself, may be an indicator of the success that this scam has brought to its authors.

Local specifics are not only exploited by criminals in Russia. It is no secret that so-called boleto – special payment documents that are widely used in Brazil – have unfortunately been used by criminals as well as regular users. In this next example criminals created a fake Internet shop webpage offering TV sets for a significantly lower price than usual, but only if payment is made through boleto. If the victim clicks the link they are redirected to an identification page, where critical payment data is required.

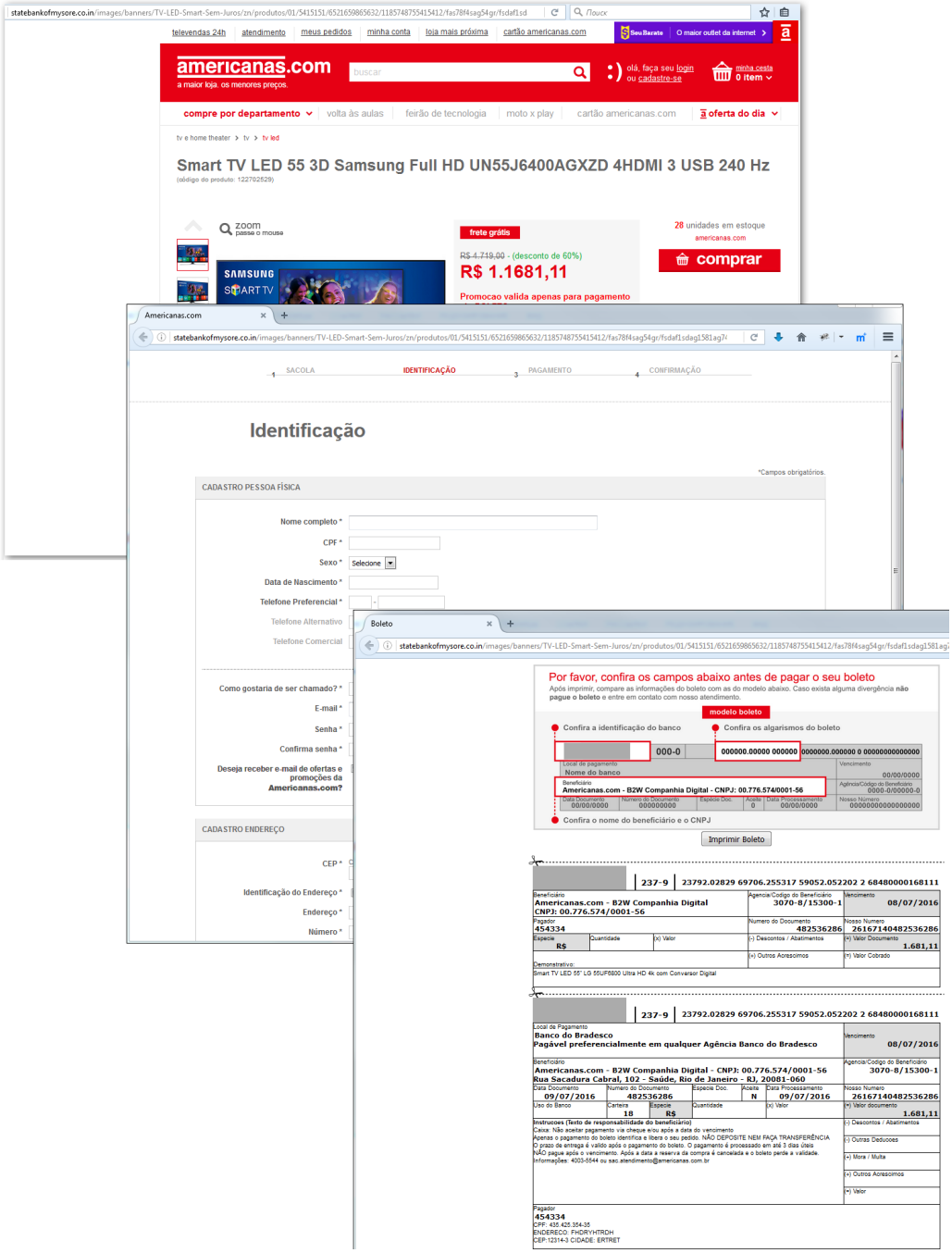


Fig. 10: The boleto-based phishing scheme

Once a victim has entered their data in boleto, they are required to go to an ATM or bank to pay in cash for their purchase. The credentials that the money should be transferred to, belong not to the real e-shop, but to an entity set up by the criminals. The victim thinks that they are paying an e-shop for a TV set, but in reality their money will go to criminals.

Another rather unique feature of this particular fraud scheme is that it was hosted on a legitimate domain owned by a bank. This fact makes the whole scheme more dangerous, because it looks very trusted from the victim's point of view.

Along with increasing the scale of attacks, cybercriminals are constantly improving the quality of the pages they lure users to visit and use.

Another unusual type of phishing is the example where the target of the fraudulent campaign wasn't the bank, the payment system or e-shop, but a well-known American organization which, among other things, provides car buying, insurance, financial and retirement planning services.

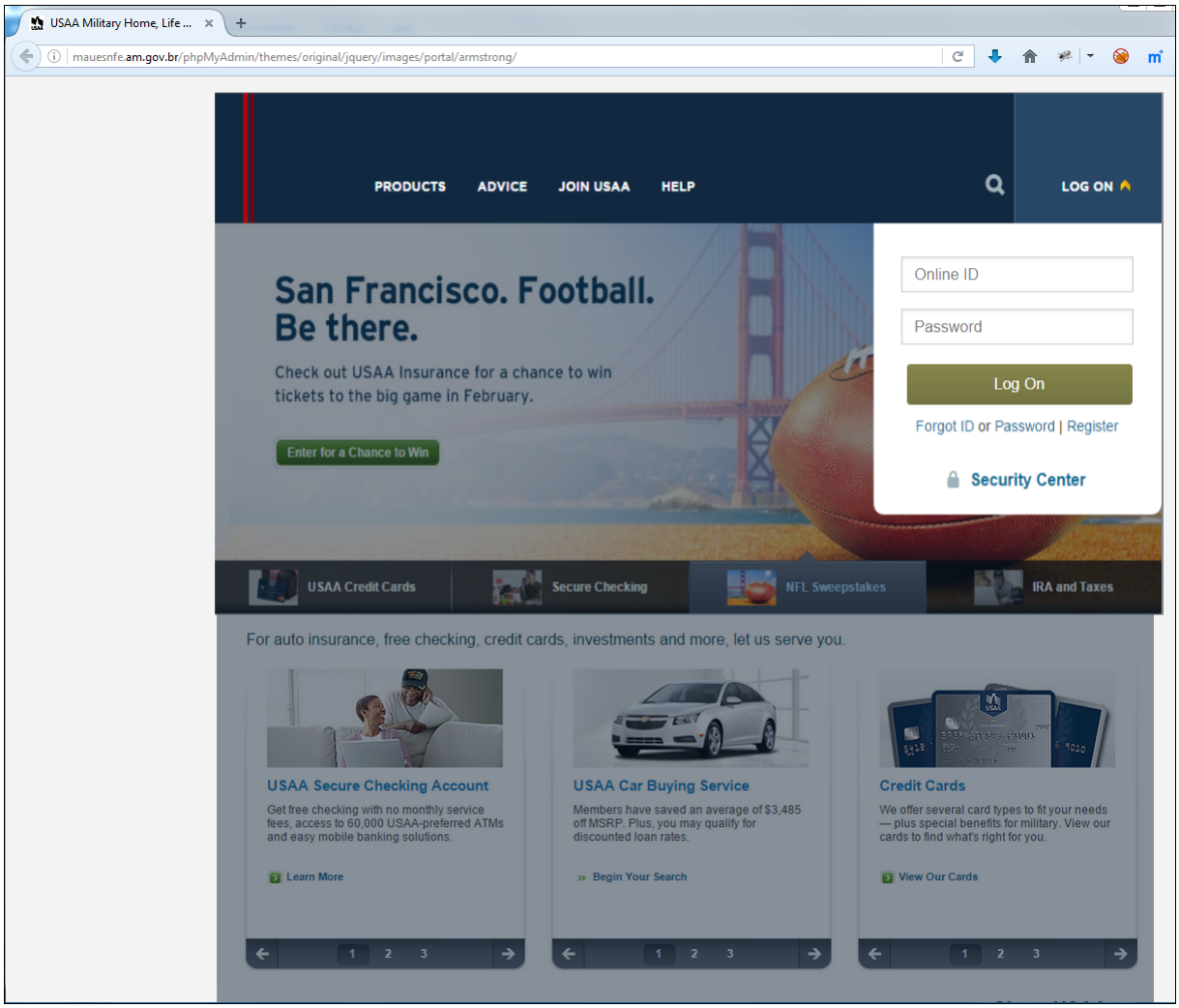


Fig. 11: An example of a phishing page mimicking the legitimate multiservice financial organizations' website

The combined nature of services provided by organizations like this one draws the attention of criminals, because successful access to the account of an active customer can potentially give them several types of financial data, related to the services described above.

Virtual goods are also becoming more and more valuable to cybercriminals. In many popular games, items for in-game purchase can cost thousands of dollars and this attracts criminals. Although phishing schemes hunting for credentials to accounts on gaming services are not new, and have been observed in the past, the quality of these fakes is improving.

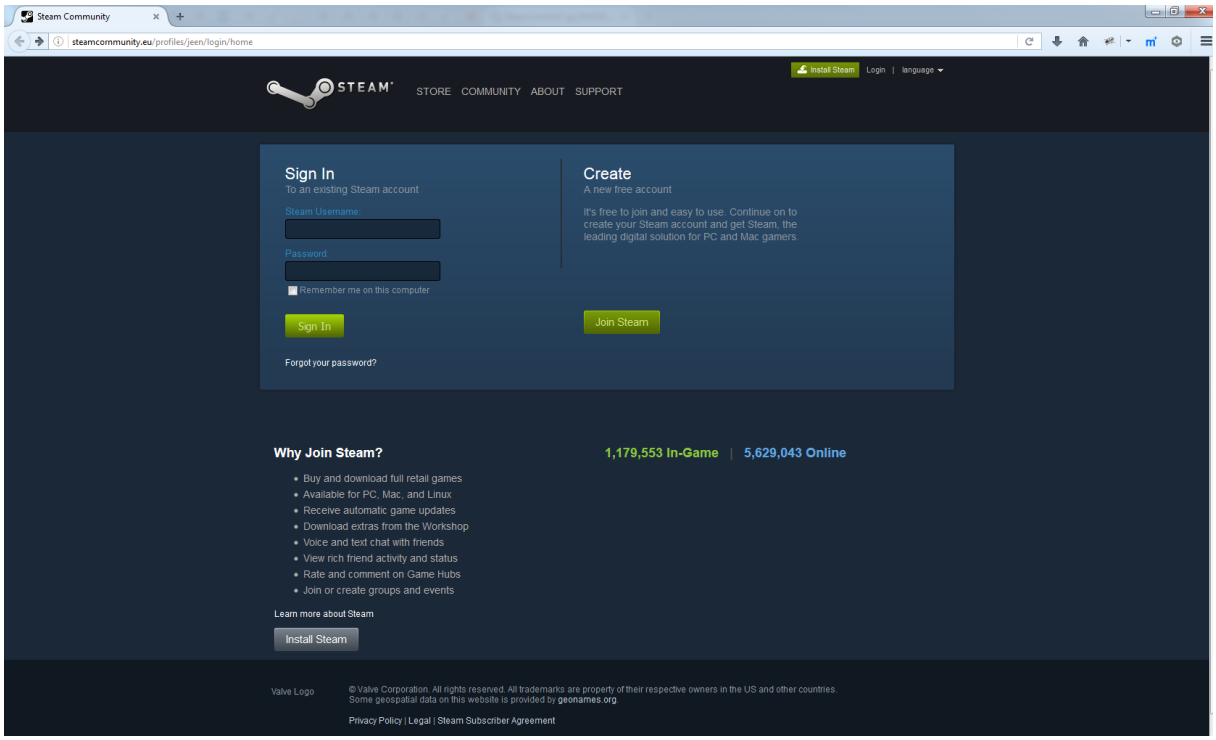


Fig. 12: A phishing copy of the popular Steam gaming service

As can be seen on the screenshot above, the phishing version of the Steam login page looks very much like the real one (below), with just a few differences.

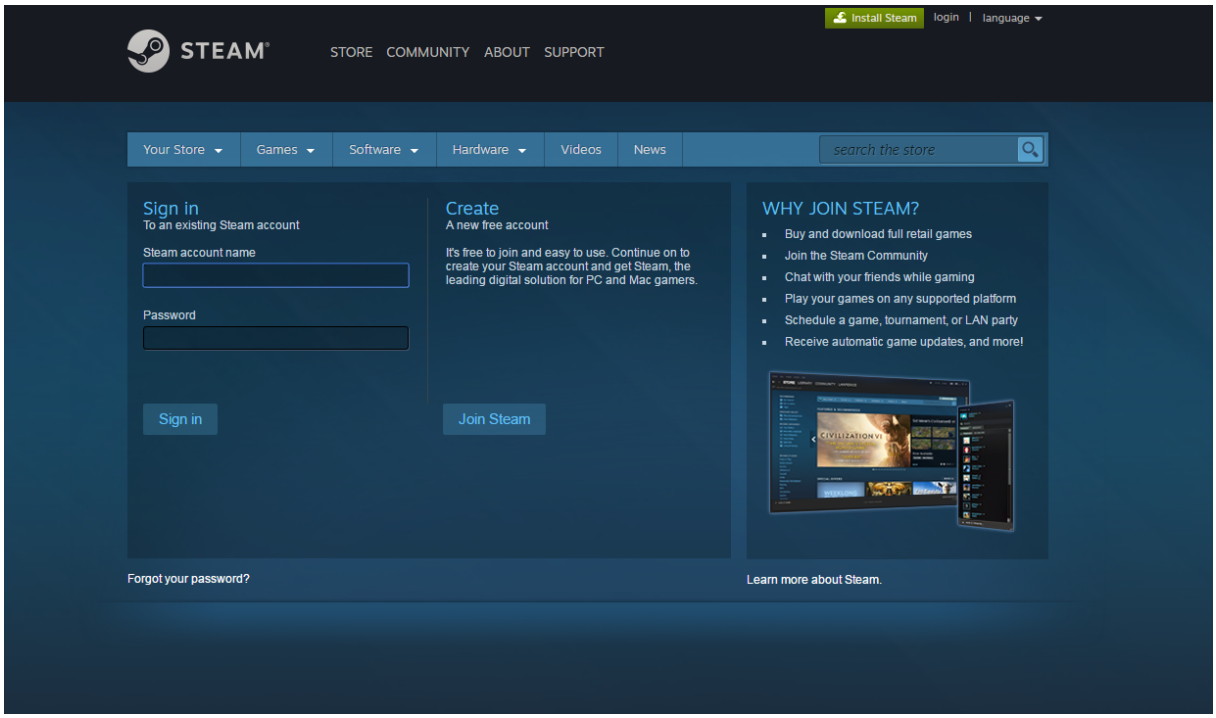


Fig. 13: The real login page of the popular Steam gaming service

Cybercriminals even bothered to create URLs which would contain the word ‘steam’ in order to make the fake even more like the original and deceive inexperienced gamers.

There have been some changes among the relatively standard phishing schemes in which known financial brands are exploited. For example Kaspersky Lab researchers have seen a lot of phisher attempts to exploit PayPal’s efforts to care about the security of its customers. For this, criminals have tried to fake messages from the company’s security team, expecting the victim to trust such message more than the “usual” phishing scheme that blatantly requests credentials. In these “security” messages fraudsters have been informing the victim that some suspicious activity has been detected in their account. They then urge them to click a link, which of course leads to a phishing page.

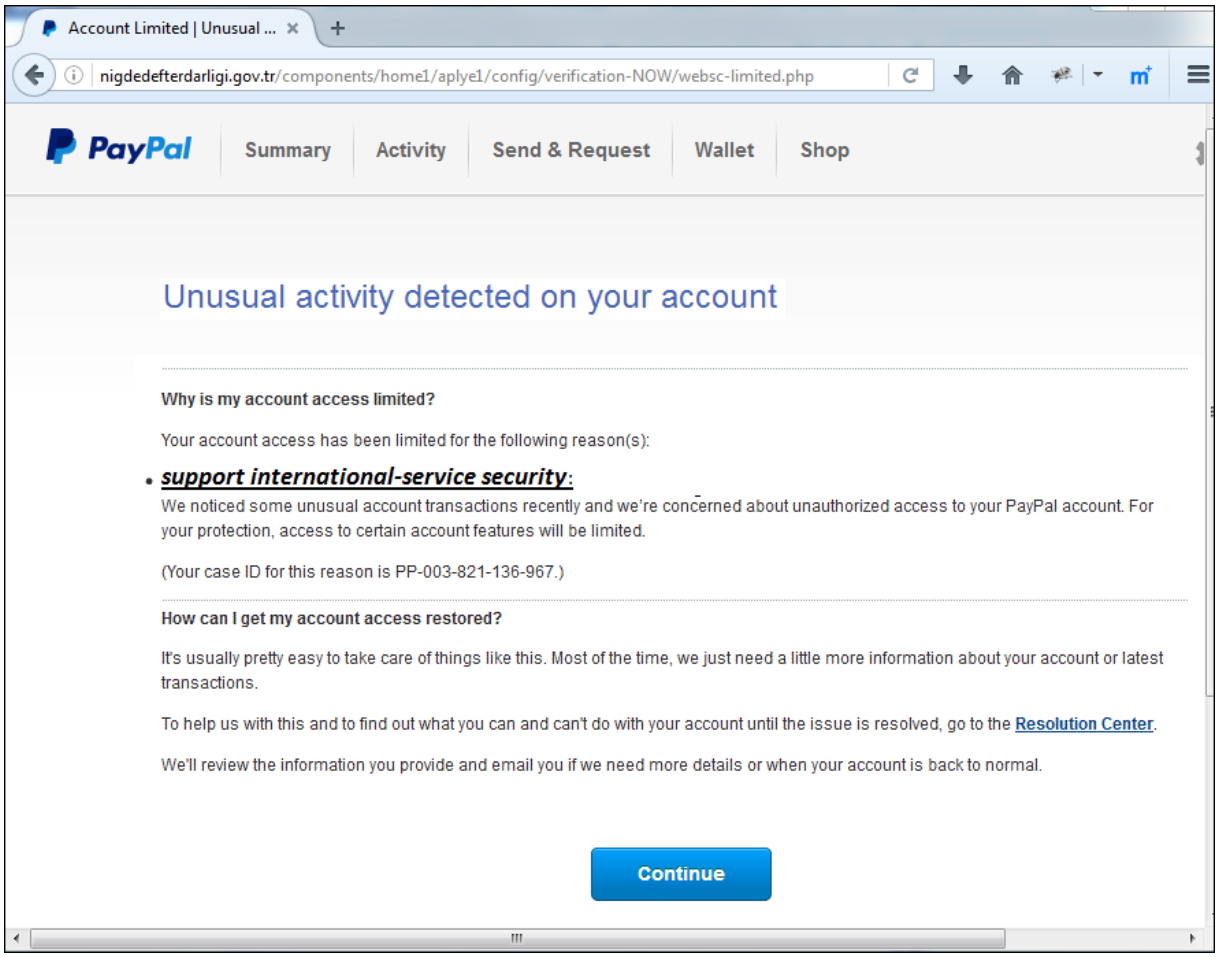


Fig. 14: An example of a phishing page mimicking a security warning from PayPal.

If the victim clicks the link, they are redirected to a “security page” where they are required to confirm their private data by entering it into the corresponding fields.

Kaspersky Lab researchers also found similar security-themed phishing scams utilizing some other famous brands. However, even though criminals put a lot of effort into making their scams as realistic as possible, it is still relatively easy to identify a fake. For example, on the screenshot above it is easy to see that the webpage with the message allegedly from PayPal is hosted on a domain that has nothing common with the real payment system. This is one clear indicator of a scam. Other markers are the email addresses used by phishing fraudsters.

Fig. 15: An example of a phishing mail disguised as a security notification from Qiwi.ru

The above is a screenshot of an email allegedly sent by the Qiwi.ru security team – a payment system popular in Russia and CIS countries. While the name of the sender seems to be legit, the actual email address has nothing to do with the original service.

Don’t show your credit card data to strangers

In general there is no surprise in the fact that financial fraudsters use phishing as a tool for illegal financial gain. It is not only financial hackers who do this. Even professional groups of hackers focusing on cyber-espionage rely heavily on spear-phishing as a method for the initial compromise of a targeted system. In fact, this is a must-have stage for almost any offensive cyber operation.

The reason is clear and simple for hackers – no matter what goal they pursue. Even if the attacked computer has all of its software updated, and is protected by a proven security solution, there is still a big chance that the user (the operator of the attacked device), due to lack of attention or experience, will believe the content of a phishing message. This is all an attacker needs.

The conclusion here is also simple: The first, and sometimes final, frontier between the user’s private financial data and the thief is the user himself. If someone in real life asked you to show him your credit card, social security card or passport, you would treat their request as suspicious unless you have proof that their intentions are legitimate. Should this situation be placed into the digital environment, the same rules should apply. In order to avoid financial or other losses on the web, users should be suspicious of any offers and requests that somehow involve their private data.

Banking malware

In our previous financial threat reports, including the annual Kaspersky Security Bulletin, we have focused on several types of malware which can be called financial. The core of the category is banking malware: a type of malicious program made specifically to find and steal credentials used to access online banking or payment system accounts and to intercept 2FA codes (one time passwords). The other participants in this category are: versions of generic keyloggers spotted in attacks against online banking and payment systems; so-called “Hosts” malware – a type of Trojan that changes the host settings of the attacked computer in order to silently redirect the victim from a real website to a fake one; and also some generic Trojans used for multiple purposes including stealing banking credentials.

Altogether these categories of malware can be defined as financial threats and the overall landscape of these threats has been covered in our annual Kaspersky Security Bulletin 2016, published in December. This paper will only focus on banking Trojans.

In 2014 we spotted a significant decrease in the number of users attacked with any kind of financial malware. In 2015 the decrease continued, but in 2016 the number of users attacked with malware targeting financial data started increasing again.

This change affected the number of users attacked with banking Trojans as well. In 2015 at least 834,099 users worldwide encountered an attack by a banking Trojan at least once. In 2016 there were 1,088,933 users worldwide, 30.55% more. This change means that although professional cybercriminal groups shifted a lot of their attention to targeted attacks against large companies, including banks and other financial organizations, smaller groups of criminals are continuing to target victims with the help of relatively widespread malware, which is available on the open web.

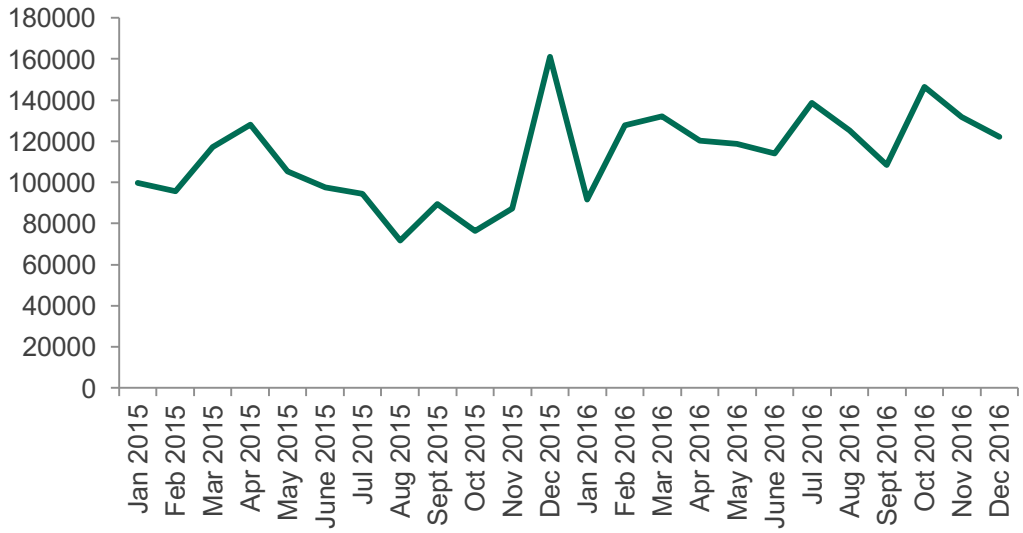


Fig. 16: The dynamic change in the number of users attacked with banking malware 2015-2016

The geography of attacked users

As it can be seen on the charts below, more than half of all users attacked with banking malware in 2015 and 2016 were located in only ten countries, and in 2016 the share of the top 10 increased by 5.6 percentage points.

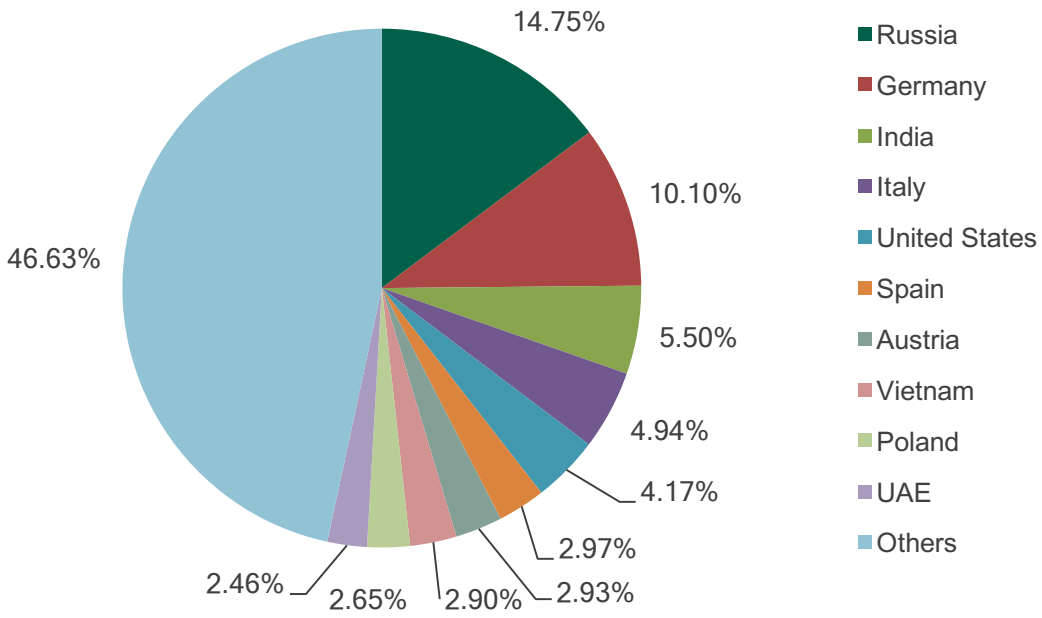


Fig. 17: The geographic distribution of users attacked with banking malware in 2015

The top 10 of the most often attacked countries has changed. In 2016, Spain, Austria, Poland, and UAE left the list, leaving room for Japan, Brazil and Turkey. The share of users from Russia and Germany increased 5.5 and 4.8 percentage points accordingly, while the percentage of users in the US, Italy and India dropped.

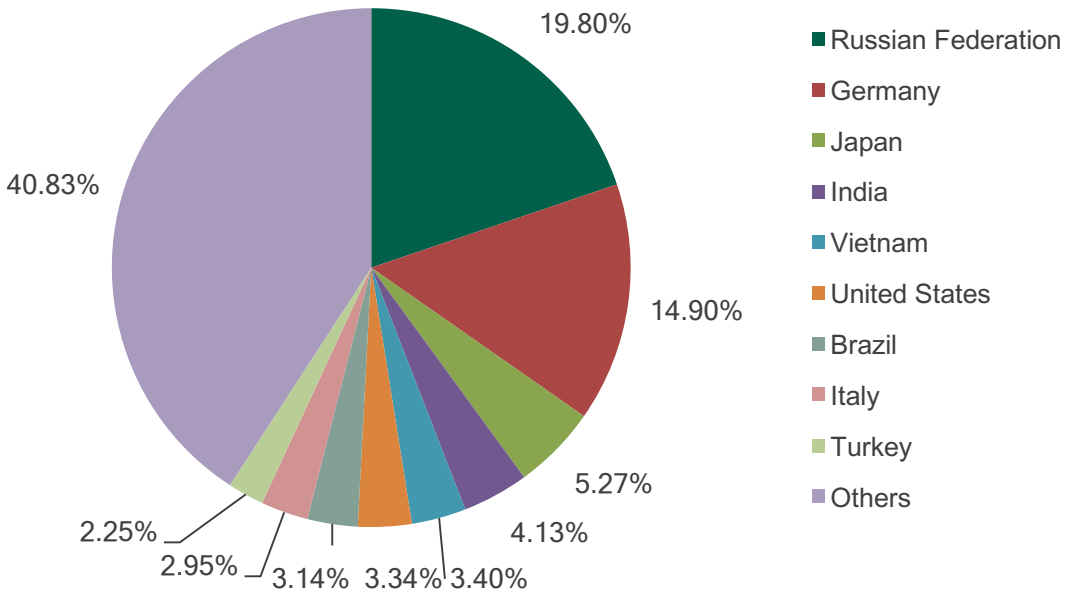


Fig. 18: the geographic distribution of users attacked with banking malware in 2016

The type of users attacked

Although most banking malware (excluding POS and ATM Trojans) is generally meant to target private users, based on our statistics this is not always the case.

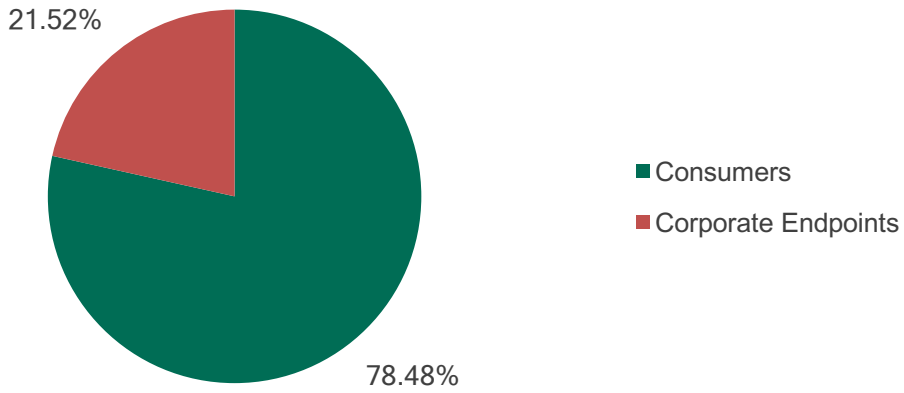


Fig. 19: The distribution of attacked users by type in 2015

In 2015 21.52% of users attacked with banking malware were corporate users. In 2016 the share of such users dropped to 17.17% but the actual number of targets increased 4.16% from 179,494 in 2015 to 186,965 in 2016.

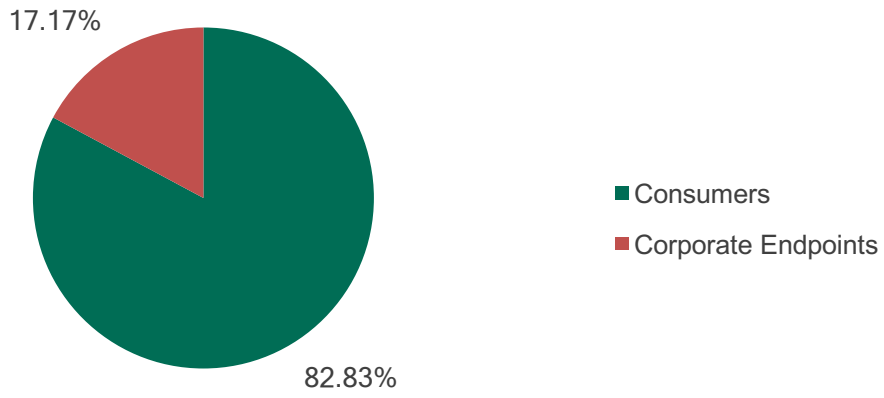


Fig. 20: The distribution of attacked users by type in 2016

It is hard to say so far if this trend towards decrease is here to stay, but there is ground for at least one solid conclusion: for two years in a row, almost every fifth user attacked with banking malware was a corporate user. It is hard to underestimate the danger of such attacks: in a successful attack against a private user, the criminal will get access to his or her private banking or payment system. If such an attack is successful against a corporate user, then it is not only the private account of the employee at risk, but also the financial assets of the company he or she is working for.

The main actors and developments

At Kaspersky Lab we track around 30 families of banking malware, but only a few of these form the current landscape of banking threats. Below is the list of the top seven most active banking malware families. In 2015 these were Zbot, Tinba, Caphaw, Neurevt, Shiotob, ZAccess and SpyEye.

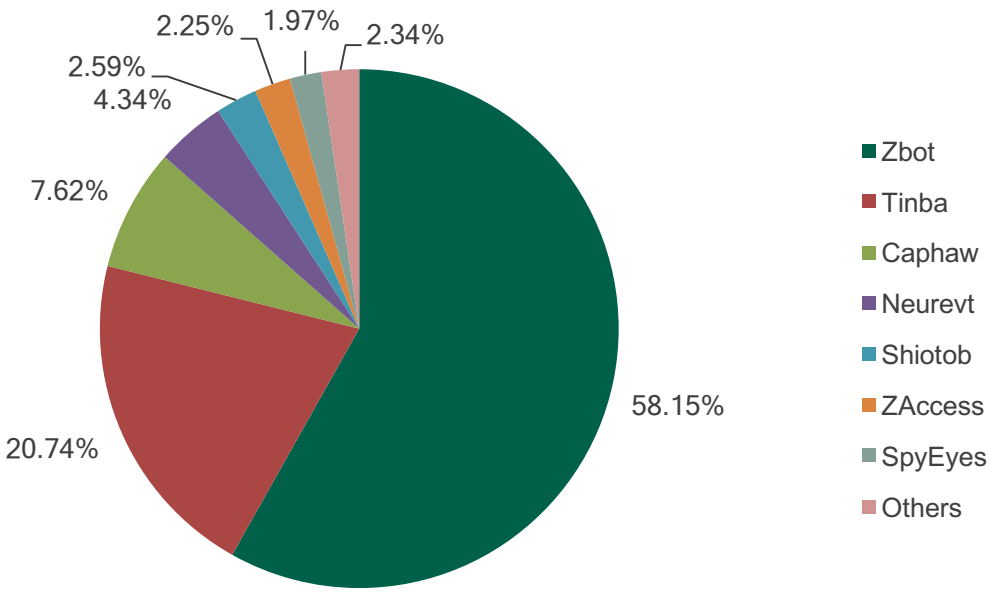


Fig. 21: the distribution of the most widespread banking malware families in 2015

In 2016 the situation became slightly different. While Zbot kept its leadership position, it was actively challenged by Gozi – a family of banking Trojans which was extremely active in 2016. At the same time, Tinba lost several positions, dropping from second place in 2015 to sixth in 2016.

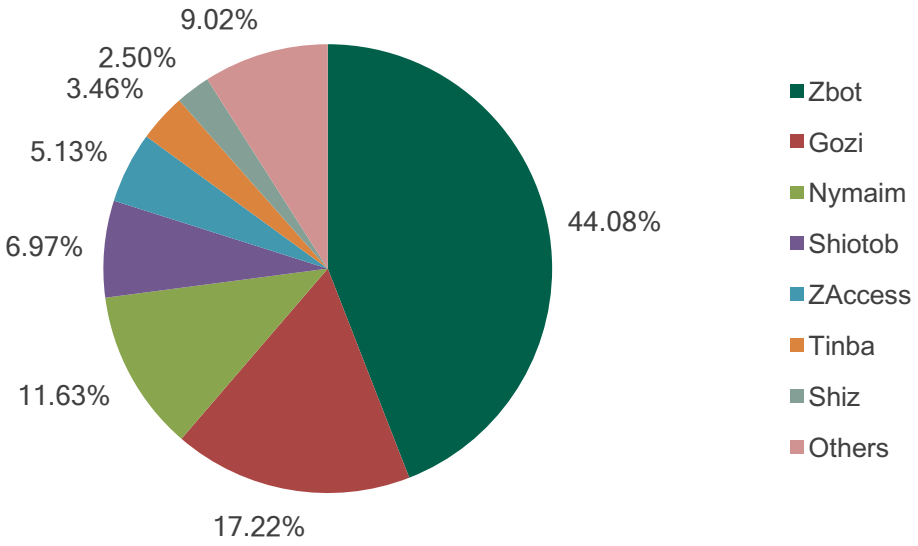


Fig. 22: The distribution of the most widespread banking malware families in 2016

The unquestionable leadership of Zbot is explained by the fact that its source code has been available on the open web for several years. There are also lots of additional modules developed specially for this malware family, offering criminals vast opportunities to create very different versions of the malware in terms of function and ability to attack particular organizations.

In general 2016 was rich with interesting events and the development of the banking malware underground. One of the key events was the arrest of the Lurk group, which was responsible for the theft of tens of millions of dollars. Along with the operations of the group, one of the most powerful exploit kits – Angler – was actively used by Lurk to spread banking malware and ransomware before being shut down. The disappearance of Lurk and the Angler exploit kit brought a lot of paranoia and concern to cybercriminal communities, with some actors temporarily stopping their operations. But these events didn't affect the research and development efforts of malware writers.

In 2016 researchers discovered the GozNym banking Trojan, which incorporates the code of the Gozi Trojan with that of the Nymaim downloader. The result is a powerful combined malware with extended functionality, but the most interesting thing here is that GozNym is not the first hybrid: in December 2014 Kaspersky Lab researchers found the Chtonic banking Trojan, which was a combination of the ZuesVM malware and Andromeda downloaders. Given that the GozNym concept repeats that of Chtonic, we can assume that this creation of hybrid, powerful, polyfunctional banking malware may become a trend.

2016 also saw some comebacks. For example, we found the new version of the Emotet banking Trojan. This one left our radars some time ago, and has now reemerged. So far we haven't seen the new version of Emotet actively spreading, but the very fact of its existence means that the authors behind this family apparently still have some development plans. The other interesting comeback is the Trickster Trojan. Just like Emotet, it is not widely spread so far, but judging by the code particularities, this Trojan may be the successor to the Dyre (aka Dyreza) banking Trojan, which completely stopped activity in October 2015.

All in all, we can say that the banking malware underground keeps producing new "products" and the malicious code of these products keeps being upgraded. Even though in recent years, lots of banks have started investing heavily in end user security for their online products, criminals still find ways to steal money with help of malware. We therefore recommend that users be cautious when conducting financial operations online from PCs. Don't underestimate the professionalism of modern cybercriminals by leaving your computer unprotected.

Android Banking Malware

Android banking malware has been around in the wild for several years already. But in several previous years the number of users attacked with banking Trojans was rather small. For instance, during our last review of the financial cyberthreat landscape, which covered activity in 2014, we registered attacks using financial malware against almost 800,000 users globally. But most of those users were attacked by SMS Trojans, and only around 60,000 users were attacked with banking Trojans. At that time, in 2014, using SMS Trojans in order to silently subscribe the victim to a premium SMS service was one of the most common types of mobile financial fraud and it was the main financial threat to Android users. However, after action was taken by the local telecommunications regulator in Russia, this type of illegal business didn't make sense anymore. Criminals started to look for something else instead.

During 2015 the number of users attacked by Android banking Trojans was even lower than in 2014 – 57,607 users in 12 months. But then something unusual happened.

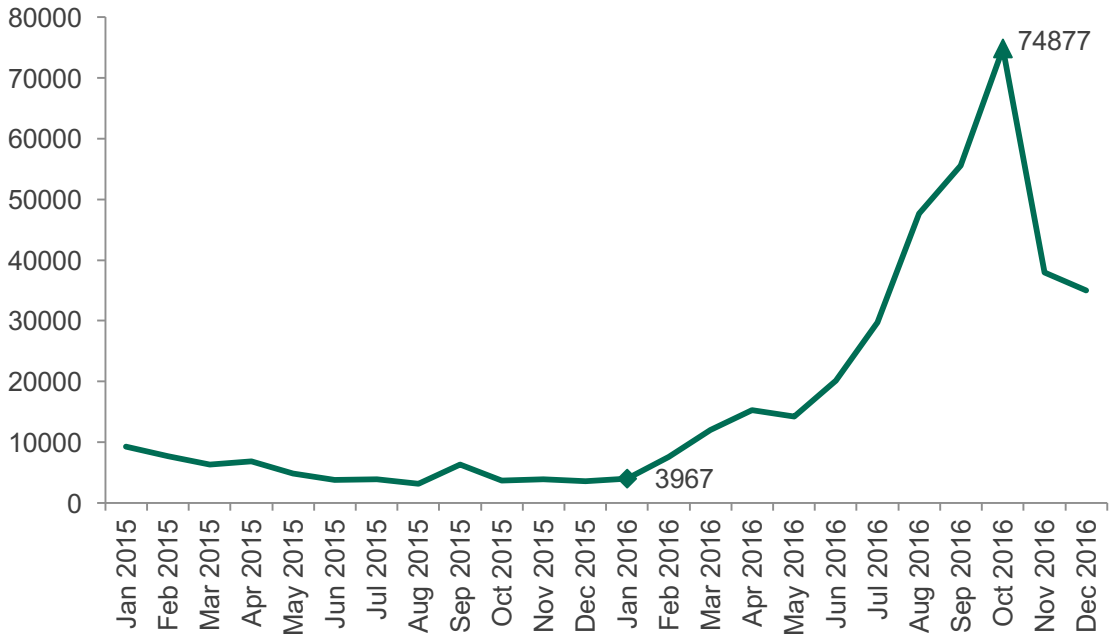


Fig.23: The change in the number of users attacked with Android banking malware 2015-2016

This is what happened: the number of attacked users started to grow rapidly from month to month, from just 3,967 users in January 2016 to almost 75,000 in October 2016.

In total, more than 305,000 users were attacked with financial malware in 2016, which is 5.3 times or 430% more than in 2015.

Of course Kaspersky Lab researchers started to investigate the reason behind this sudden increase as soon as the number of attacked users started growing. As a result we discovered that only two families of malware are responsible for this major shift. The first one – Asacub – was being distributed actively through SMS from the beginning of the year. The second was Svpeng, a well-known banking Trojan which we've described in our previous research many times. This Trojan has started distributing in a new way: through the Google AdSense advertising network.

The malware targeted mostly users from Russia and CIS, and only those who attended several popular news outlets. As our further investigation showed, the massive distribution of the Trojan became possible because of a security issue discovered by Kaspersky Lab researchers in a popular mobile browser, which allowed the malicious application to be automatically downloaded onto the attacked device. As soon as the browser's developer released a patch, and Google figured out how to identify and block the malicious ads, the number of attacked users started decreasing rapidly - as can be seen on the chart above.

The incident completely ruined our statistics. Judge for yourself: if the chart showing the most popular banking Trojans looked like this in 2015…

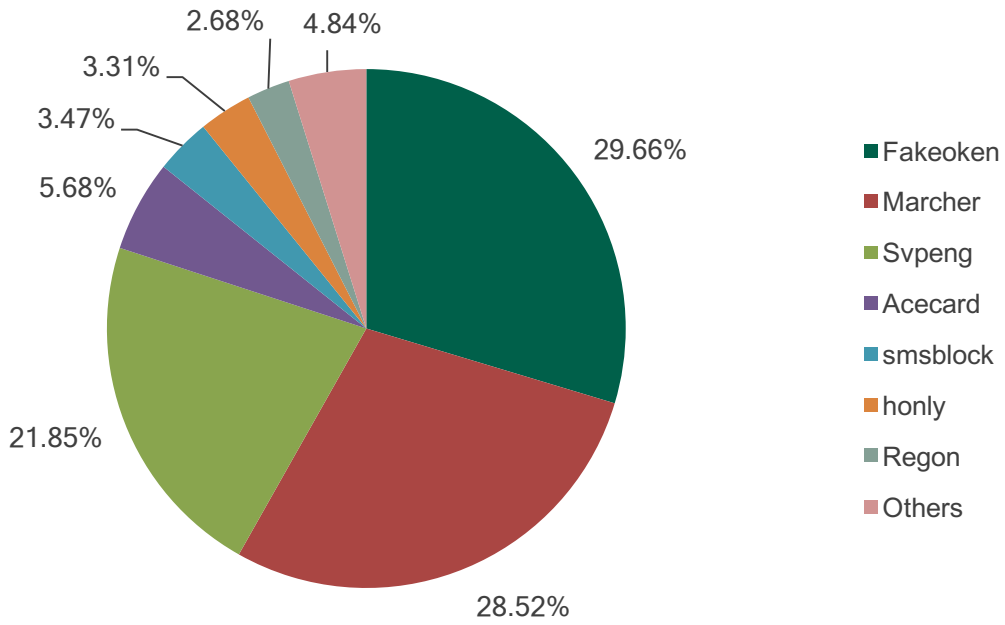


Fig. 24: The most widespread Android banking malware in 2015

Then in 2016, the chart turned out to be completely different.

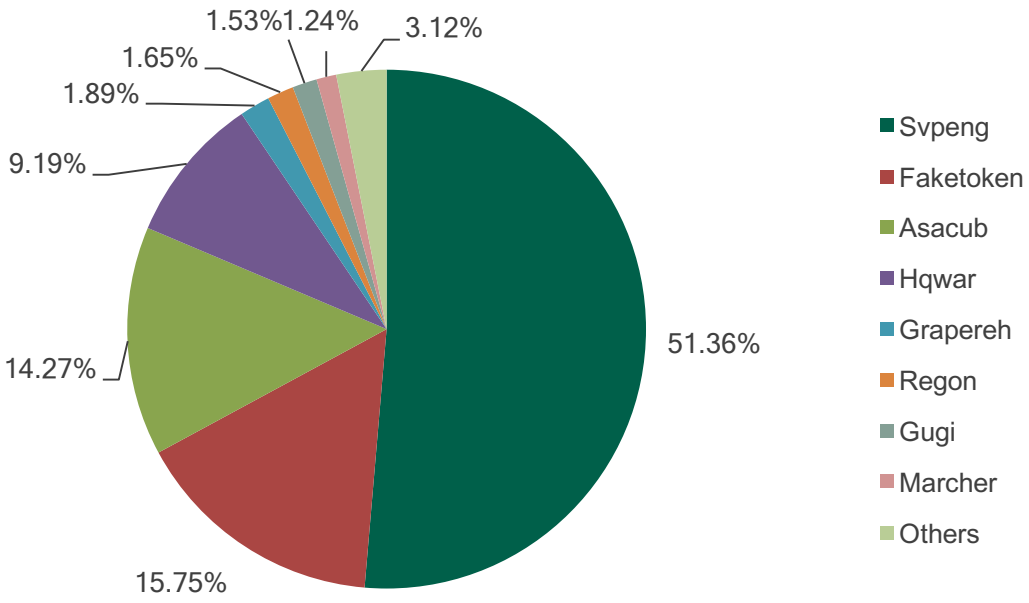


Fig. 25: The most widespread Android banking malware in 2016

More than half of the users that encountered an Android banking Trojan in 2016, were faced with Svpeng. It is important to note that this malware family wasn't the only one that improved its distribution method, hitting many more users than before as a result.

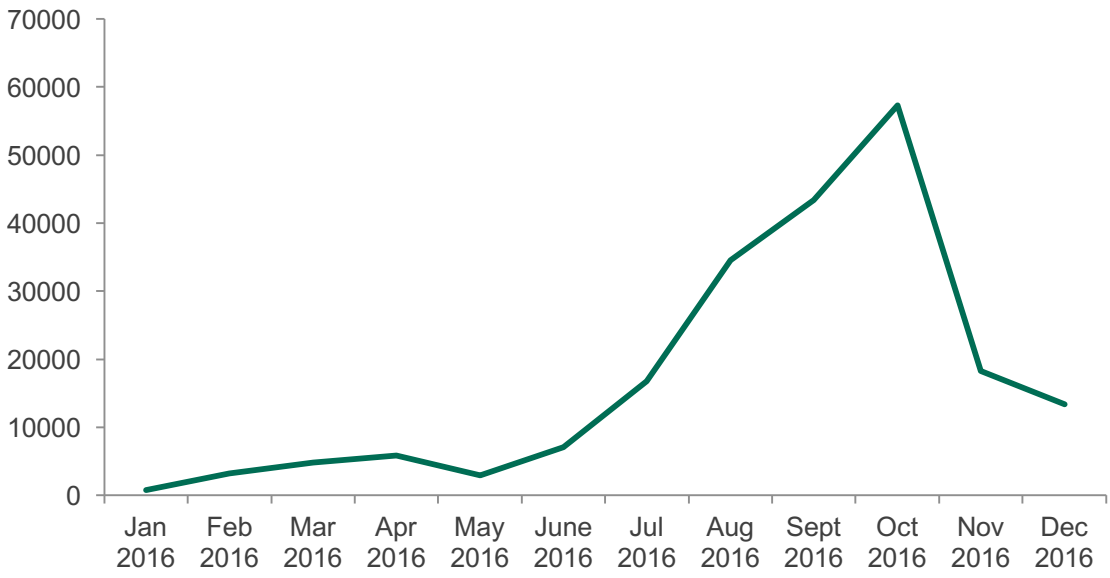


Fig.26: The change in the number of users attacked by the Svpeng Android banking Trojan

Criminals behind the Faketoken family (the leader in 2015) also did some promotional work – the result of which was an almost threefold (2.9 times) increase in the number of attacked users: from 18,700 in 2015 to 54,400 in 2016. We've seen Trojans from this family disguised as useful free applications and distributed actively through multiple malicious websites.

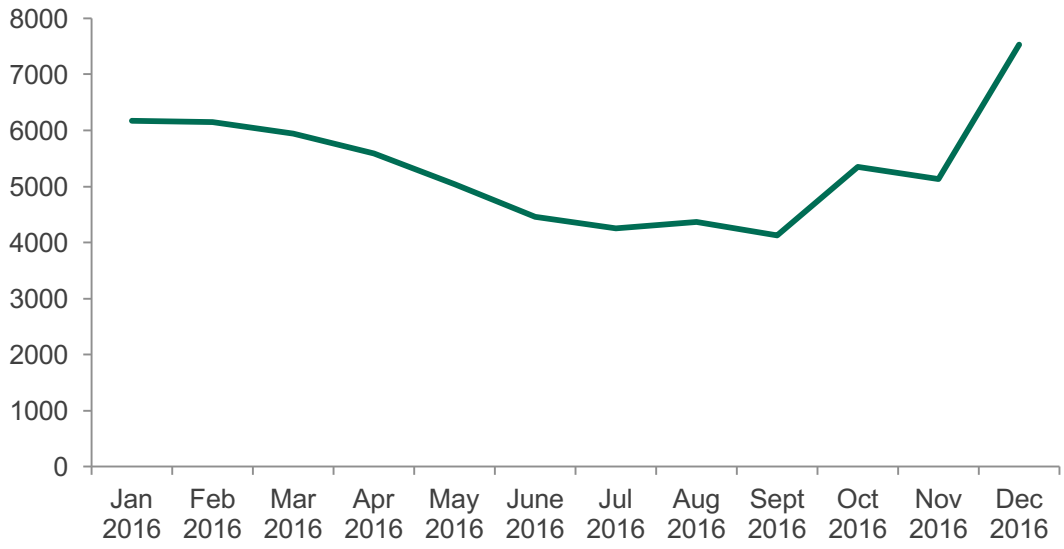


Fig.27: The change in the number of users attacked by Faketoken Android banking malware

Hackers behind Asacub, another member of the top Android banking Trojans in 2016, were seen using SMS-spam as their distribution method. Most of these campaigns were registered in the period from February to June and then from September to November, which is clearly visible on the corresponding chart below.

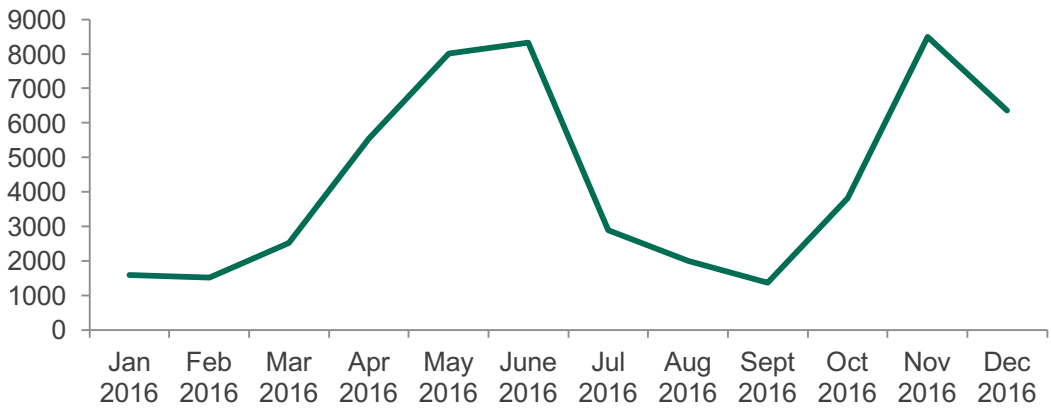


Fig. 28: The change in the number of users attacked with Asacub banking malware

Geography of attacked users

The geography of attacks also changed in 2016 compared to 2015.

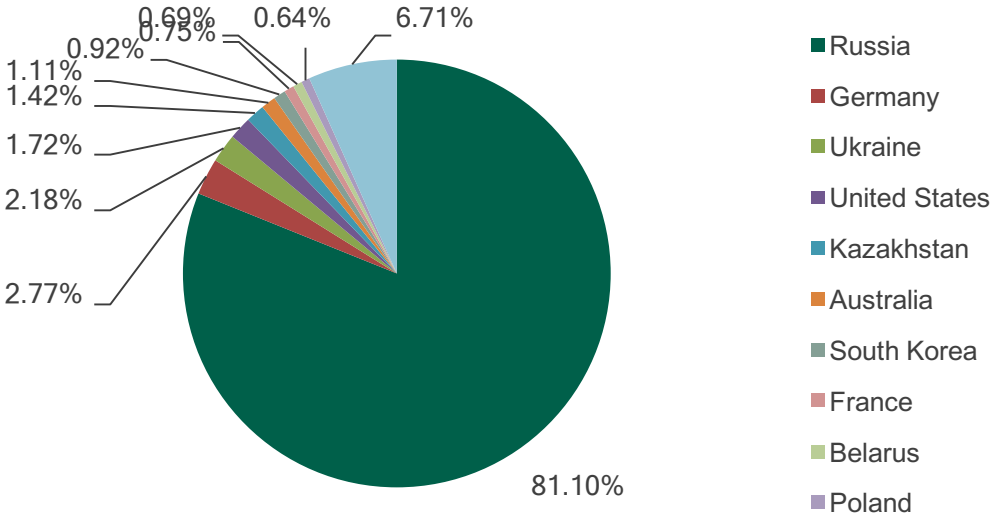


Fig. 29: The distribution of users attacked by Android banking Trojans in 2015

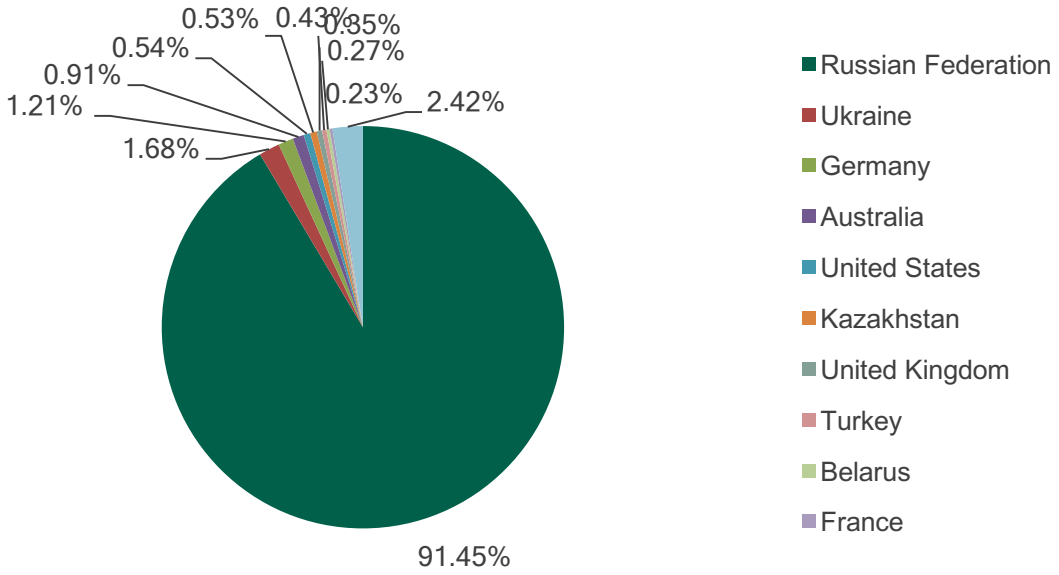


Fig. 30: The distribution of users attacked with Android Banking Trojans in 2016

As it can be seen on the charts above, Android banking malware is mostly a Russian problem. It should be said that these findings are affected by a largely generic distribution of

Kaspersky Lab product users, many of whom are located in Russia, as well as the Svpeng malware, which has exploited a vulnerability in a browser mostly used in Russia. With that in mind, the normalized picture of the geographical distribution of Android banking attacks (with Russian data excluded) looks like this.

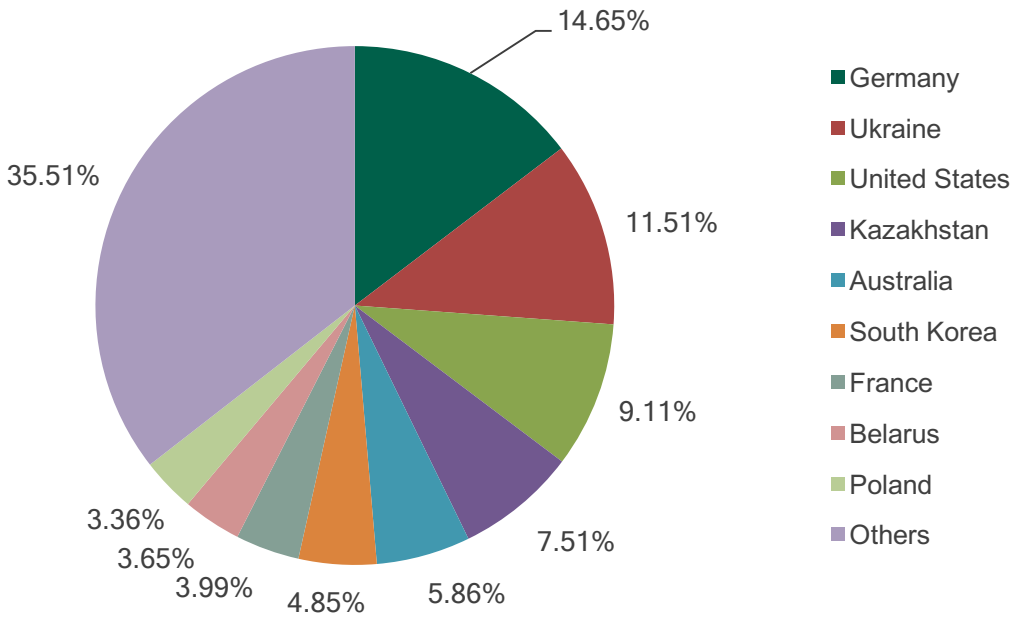


Fig. 31: The distribution of users attacked with Android banking malware in 2015 (a total of 10,887 users, Russia excluded)

And in 2016 it looked like this:

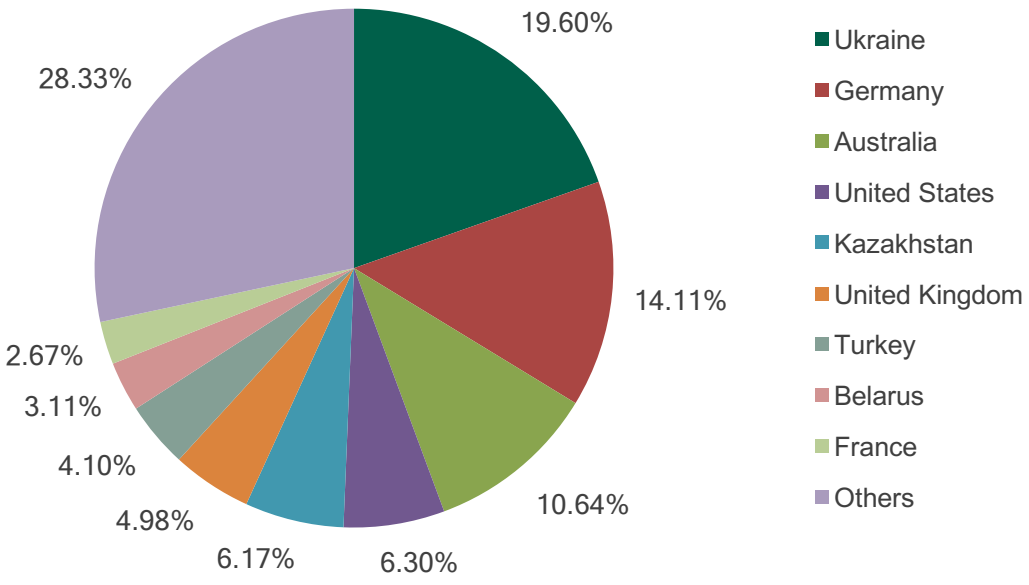


Fig. 32: The distribution of users attacked with Android banking malware in 2016 (a total of 26,110 users, Russia excluded)

Germany and Ukraine swapped positions in the ranking in 2016, compared to 2015. While the share of Ukrainian users attacked with Android banking malware almost doubled, the share of German users remained almost the same. In 2016 Australia also made it into the top three most often attacked countries (excluding Russia), and the US left the top three.

All in all we have to admit that - aside from in Russia - in every part of the world the Android banking malware problem is not the biggest one, if we look at the number of attacked users. In most countries, these rarely exceed a couple of thousand users. The only two exceptions here are Australia and Ukraine.

If we look at the same figures as a percentage of attacked users, the metrics show us what percentage of the total number of users in a particular country encountered banking malware. In 2016 1.57% of users of Kaspersky Lab products globally encountered a banking Trojan at least once. And when it comes to the countries with the highest percentage of such users, the picture looks like this.

Russia	4.01%
Australia	2.26%
Ukraine	1.05%
Uzbekistan	0.70%
Tajikistan	0.65%

South Korea	0.59%
Kazakhstan	0.57%
China	0.54%
Belarus	0.47%
Moldova	0.39%

Fig. 33: The top 10 countries with the highest percentage of users that encountered Android banking malware in 2016

As can be seen in the table above, even though the actual numbers of attacked users in Ukraine and Australia are incomparable with the one for Russia, the share of such users in the total volume is. This means that along with Russian users, Australian and Ukrainian owners of Android-based smartphones should be aware that the probability of them encountering banking malware is higher than in most other countries.

Major changes to the Android banking malware landscape

Of course statistics are not the main tool we use to observe changes and developments in the threat landscape. Our key method is the analysis of actual malware found in the wild. In total we discovered five new banking malware families in 2016, much less than in 2015, when we found discovered new families.

Newcomers

The most dangerous of these new families was Tordow.(Trojan-Banker.AndroidOS.Tordow.a). First of all, this malware is capable of rooting the attacked device. In general, after this procedure any malware can steal anything, but we identified Tordow as a banking Trojan because we've seen it hunting for banking credentials. Besides the ability to get root privileges, it has a modular structure – depending on the particular task, the list of functions that the Trojan is capable of may vary, and new functions are being downloaded from the command and control server.

Another dangerous newcomer for 2016 was Fareac. This is a fake app that offers to recharge users' mobile phones and add credits, but the app actually only clones credit cards from Brazilian users. It has been distributed through Google Play.

We also discovered three rather simple yet dangerous Trojans. Gatewis (Trojan-Banker.AndroidOS.Gatewis) can intercept SMS, show phishing pages, and make USSD requests, which are used to redirect phone calls, among other things. The Ledoden Trojan has more or less the same list of functions, but it can also automatically subscribe its victims' devices to wapclick premium subscriptions.

The third rather interesting malware family, discovered in 2016, is called Nomo. Its main feature is that it is written in .net programming language. Because of this, the final size of the malicious file is 10-20 times bigger than if it was written on Java (the more common language for Android malware writers). We spent some time thinking why criminals would use .net in the malware's development, and came to the conclusion that perhaps they believed this would help them to avoid detection better - the code is obfuscated and the help of an interpreter is required to make the malware work on Android.

Evolution of known families

Besides detecting new families in 2016 we've observed some developments in known families. We've already mentioned the progress made by Svpeng with the help of a vulnerability in a popular mobile browser. This wasn't the only change.

For example, the Faketoken Trojan has been updated with functions allowing it to serve as crypto ransomware, as well as modules allowing it to show fake login windows for more than 2000 banking applications.

The Marcher Trojan has adopted the web injections technique, allowing it to show fake data entry fields in the browser. This is a rather widespread technique when it comes to PC banking Trojans, but no other Android banking malware family has used it so far, at least according to our observations.

The Gugi banking Trojan adopted several techniques, allowing it to bypass some security measures introduced in the latest versions of Android OS. Based on what we're observing now, these techniques are more or less successful, because now we can see some other families adopting the set of specific functions that were first introduced in Gugi.

Watch out for your smartphone

It would be too presumptuous to say that every kind of epidemic related to banking Trojans is out there now. Things are more or less calm in the worldwide situation around this type of mobile malware. Nevertheless, we are observing several groups of criminals who keep updating their malware with new features, investing resources into new ways of distribution and into the development of detection avoidance techniques. This all means that they see sense in doing what they do – or in other words, they get financial gain out of their activities.

We therefore advise owners of Android-based devices, especially those with financial applications installed, to be extremely cautious when surfing the web and using applications. There are predators hunting for financial data on mobile phones and they're ready to be persistent in order to be successful.

Conclusion and advice

In recent years the financial industry – banks, payment systems and e-commerce companies – have been working hard to make financial transactions online more secure. Multifactor authentication has been widely adopted and the security of websites working with financial data has been much improved. Organizations have also done a lot to inform their customers about financial cyber risks and are now offering security products as part of their online banking services. But as our threat statistics show, there is still plenty of room for financial fraud operations involving phishing and specific banking malware in this sphere. In order to avoid the risk of losing money as a result of a cyberattack, Kaspersky Lab's experts advise the following:

For home users

- Never click on links sent to you by unknown people or open suspicious ones – even if sent to you by friends via social networking or e-mail. These malicious links are designed to download malware onto your device or lead you to phishing webpages aimed at harvesting user credentials.
- Be wary of unfamiliar files. Never open or store them on your device as they could be malicious.
- Although convenient, public Wi-Fi networks can be insecure and unreliable, making hotspots a prime target for hackers to steal user information. To keep your confidential details safe, never use hotspots to make online payments or share financial information. However, if you have no other option, use a VPN service which will encrypt all of the data you transfer (such as the Secure Connection feature in flagship Kaspersky Lab solutions).
- Websites can be a front for cybercriminals, with the sole purpose of harvesting your data. To avoid your confidential details falling into the wrong hands, if a site seems suspicious or is unfamiliar, do not enter your credit card details or make a purchase.
- To avoid falling into a trap, always check that the website is genuine, by double-checking the format of the URL or the spelling of the company name, before entering any of your credentials. Fake websites may look just like the real thing, but there will be anomalies to help you spot the difference.
- To give you more confidence when assessing the safety of a website, only use websites which begin with HTTPS:// and therefore run across an encrypted connection. HTTP:// sites do not offer the same security and could put your information at risk as a result.

- Never disclose your passwords or PIN-codes to anyone – not even your closest family and friends or your bank manager. Sharing these will only increase the level of risk and exposure to your personal accounts. This could lead to your financial information being accessed by cybercriminals, and your money stolen.
- To help prevent financial fraud, a dedicated security solution on your device, with built-in features, will create a secure environment for all of your financial transactions. Kaspersky Lab's Safe Money technology is designed to offer this level of protection to users and provide peace of mind.
- To keep your credentials safe, it is important to apply the same level of vigilance and security across all of your devices – whether desktop, laptop or mobile. Cybercriminal exploits know no boundaries, so your security needs to be just as widespread to minimize your information falling into the wrong hands.

For businesses

- Instruct your employees not to click on links or to open attachments received from untrusted sources.
- Pay specific attention to endpoints from which financial operations are being completed: update the software installed on these endpoints first, and keep their security solution up to date.
- Invest in regular cybersecurity training for employees who use online financial tools at your company. Help them learn how to distinguish phishing emails, and how to identify if an endpoint has been compromised.
- Use proven security solutions, equipped with behavioral based protection technologies, which make it possible to catch even unknown banking malware.