



# **FINANCIAL CYBERTHREATS IN 2017**

February, 2018

## Introduction and Key Findings

The world of financial cyberthreats has been evolving and changing for years. As one of the most profitable fields of cybercriminal activities, it attracts malicious individuals targeting users of online financial services and payment systems, as well as large banks and any industry where POS terminals are used. At the same time, criminals have recently started shifting their attention from users to the systems and services themselves.

In 2017, we saw a number of changes to the world of financial threats and new actors emerging. As we have previously [noted](#), fraud attacks in financial services have become increasingly account-centric. User data is a key enabler for large-scale fraud attacks, and frequent data breaches - among other successful attack types - have provided cybercriminals with valuable sources of personal information to use in account takeovers or false identity attacks. These account-centric attacks can result in many other losses, including those of further customer data and trust, so mitigation is as important as ever for both businesses and financial services customers.

Attacks on [ATMs continued to rise in 2017](#), attracting the [attention](#) of many cybercriminals, with attackers targeting bank infrastructure and payment systems using sophisticated fileless malware, as well as the more rudimentary methods of taping over CCTVs and drilling holes. In 2017, Kaspersky Lab researchers uncovered, among other things, attacks on ATM systems that involved new [malware](#), [remote](#) operations, and an ATM-targeting malware called '[Cutlet Maker](#)' that was being sold openly on the DarkNet market for a few thousand dollars, along with a step-by-step user guide. Kaspersky Lab has published a [report](#) outlining possible future ATM attack scenarios targeting ATM authentication systems.

It is also worth mentioning that major cyber incidents continue to take place. In September 2017, Kaspersky Lab researchers identified a new series of targeted attacks against at least 10 financial organizations in multiple regions, including Russia, Armenia, and Malaysia. The hits were performed by a new group called [Silence](#). While stealing funds from its victims, Silence implemented specific techniques similar to the infamous threat actor, [Carbanak](#).

Thus, Silence joins the ranks of the most devastating and complex cyber-robbery operations [like](#) Metel, GCMAN and Carbanak/Cobalt, which have succeeded in stealing millions of dollars from financial organizations. The interesting point to note with this actor is that the criminals exploit the infrastructure of already infected financial institutions for new attacks: sending emails from real employee addresses to a new victim, along with a request to open a bank account. Using this trick, criminals make sure the recipient doesn't suspect the infection vector.

Small and medium-sized businesses didn't escape financial threats either. Last year Kaspersky Lab's researchers discovered a new botnet that cashes-in on aggressive advertising, mostly in Germany and the US. Criminals infect their victims' computers with the [Magala Trojan Clicker](#), generating fake ad views, and making up to \$350 from each machine. Small enterprises lose out most because they end up doing business with unscrupulous advertisers, without even knowing it.

Moving down one more step – from SMEs to individual users – we can say that 2017 didn't give the latter much respite from financial threats. Kaspersky Lab researchers detected [NukeBot](#) – a new malware designed to steal the credentials of online banking customers. Earlier versions of the Trojan were known to the security industry as TinyNuke, but they lacked the features necessary to launch attacks. The latest versions however, are fully operable, and contain code to target the users of specific banks.

This report summarizes a [series](#) of Kaspersky Lab reports that between them provide an overview of how the financial threat landscape has evolved over the years. It covers the common phishing threats that users encounter, along with Windows-based and Android-based financial malware.

The key findings of the report are:

### **Phishing:**

- In 2017, the share of financial phishing increased from 47.5% to almost 54% of all phishing detections. This is an all-time high, according to Kaspersky Lab statistics for financial phishing.
- More than one in four attempts to load a phishing page blocked by Kaspersky Lab products is related to banking phishing.
- The share of phishing related to payment systems and online shops accounted for almost 16% and 11% respectively in 2017. This is slightly more (single percentage points) than in 2016.
- The share of financial phishing encountered by Mac users nearly doubled, accounting for almost 56%.

### **Banking malware:**

- In 2017, the number of users attacked with banking Trojans was 767,072, a decrease of 30% on 2016 (1,088,900).
- 19% of users attacked with banking malware were corporate users.
- Users in Germany, Russia, China, India, Vietnam, Brazil and the US were the most often attacked by banking malware.
- Zbot is still the most widespread banking malware family (almost 33% of attacked users), but is now being challenged by the Gozi family (27.8%).

### **Android banking malware:**

- In 2017, the number of users that encountered Android banking malware decreased by almost 15% to 259,828 worldwide.
- Just three banking malware families accounted for attacks on the vast majority of users (over 70%).
- Russia, Australia and Turkmenistan were the countries with the highest percentage of users attacked by Android banking malware.

## Financial Phishing

Financial phishing is one of the most common and widespread types of cybercriminal activity. It 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 will receive enough payment card credentials to cash out immediately, or to 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.

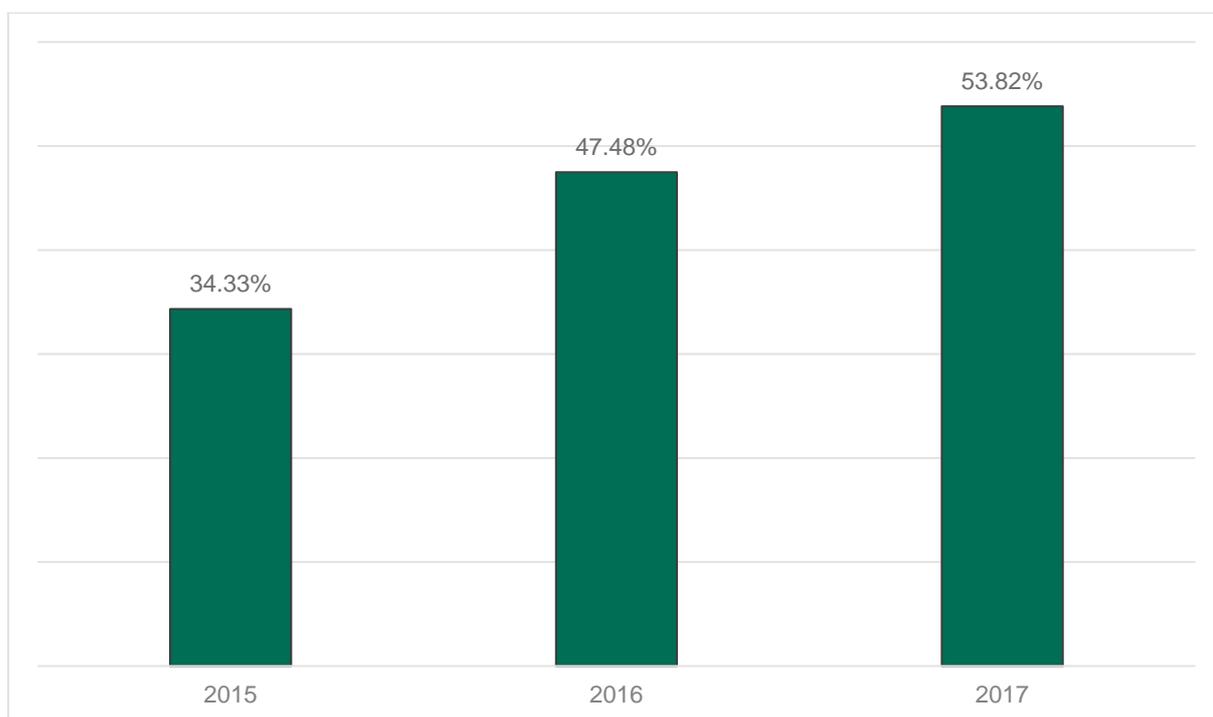


Fig. 1: The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky Lab in 2015-2017

In 2017, Kaspersky Lab's anti-phishing technologies [detected](#) 246,231,645 attempts to visit different kinds of phishing pages. Of those, 53.8% of heuristic detections were attempts to visit a financial phishing page – 6.3 percentage points more than the share of phishing detections registered in 2016 when it was 47.5%. At the moment, this is the highest percentage of financial phishing ever registered by Kaspersky Lab.

Moreover, in 2017, the detection of phishing pages which mimicked legitimate payment systems took second place in the overall chart, just behind banking services, leaving global web portals further behind.

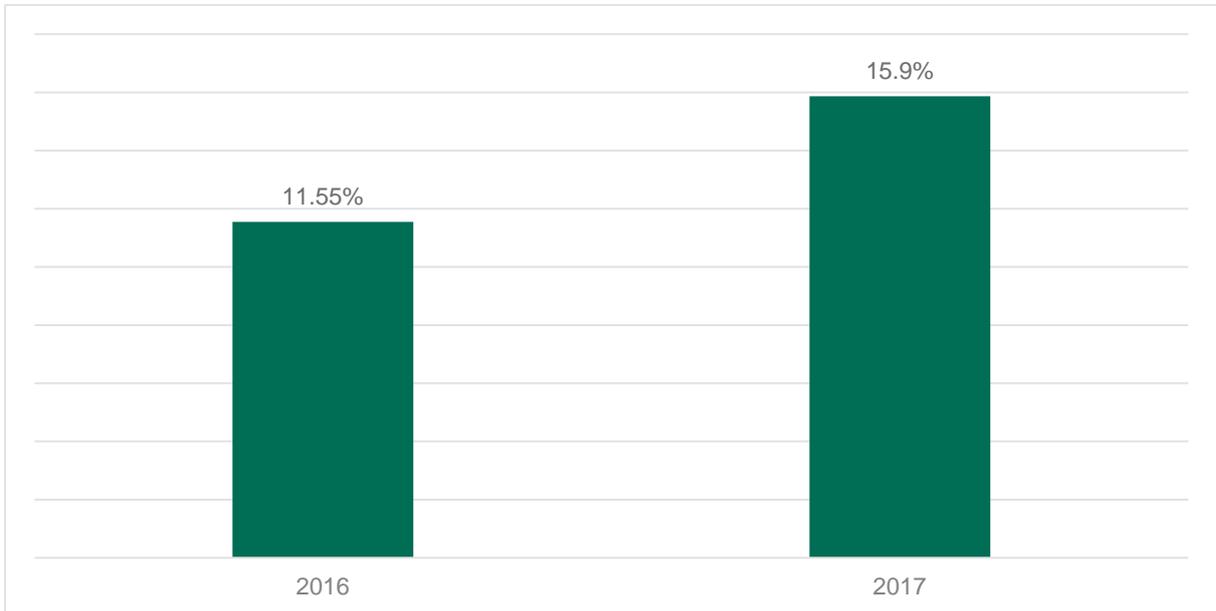


Fig. 2: The percentage of payment systems phishing (from overall phishing attacks) detected by Kaspersky Lab in 2016-2017

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 mimic well-known payment brands such as PayPal, Visa, MasterCard, American Express and others. There is also the 'online shop' category which includes internet shops and auction sites like Amazon, Apple store, Steam, E-bay and others.

In 2017 all of them experienced slight growth: the share of phishing attacks against banks, payment systems and online shops increased by 1.2, 4.3, and 0.8 percentage points respectively.

That said, 2017 became the first year when the top three categories of all phishing detections related to financial attacks:

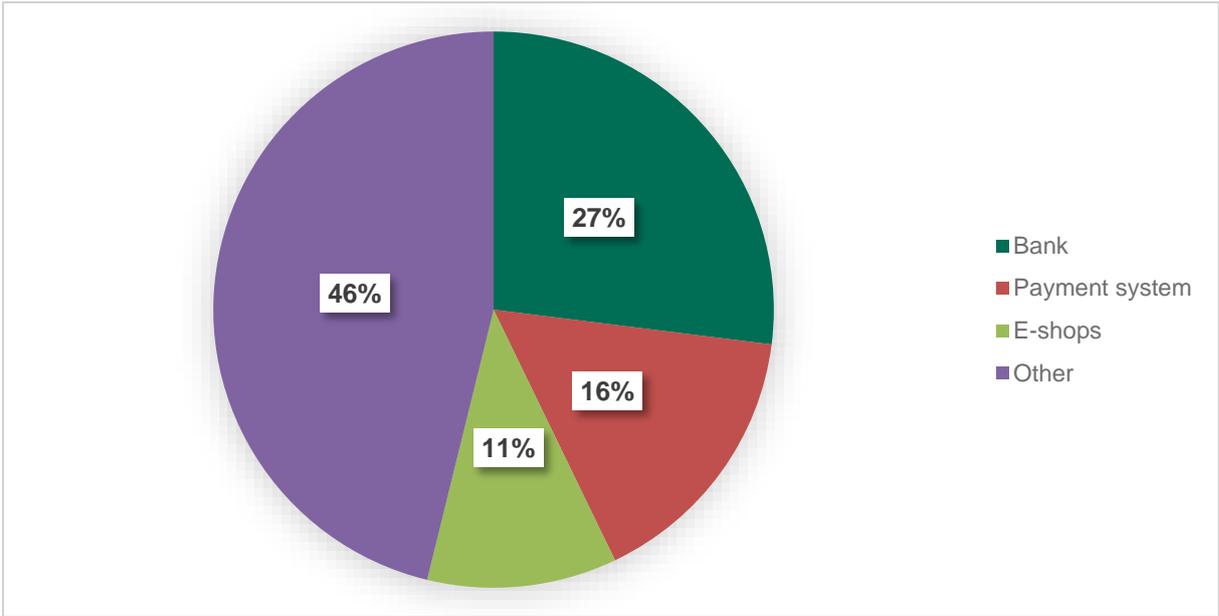


Fig. 3: The distribution of different types of financial phishing detected by Kaspersky Lab in 2017

That means that for the first time in our observations, payment systems and online shops hit the top three in all categories of phishing detections. The major reason behind this is quite simple – it is a result of the steady growth of these kinds of attacks on lucrative targets. Moreover – and also for the first time – the presented chart means that more than every second phishing attack in 2017 was related to the financial sector. This is largely due to the fact that while the online shop share grew slightly, the global internet portal category fell from second place in 2016 with 24.1%, to fourth place in 2017 with 10.9%. This looks like a global trend, as Yahoo left the top spot for good.

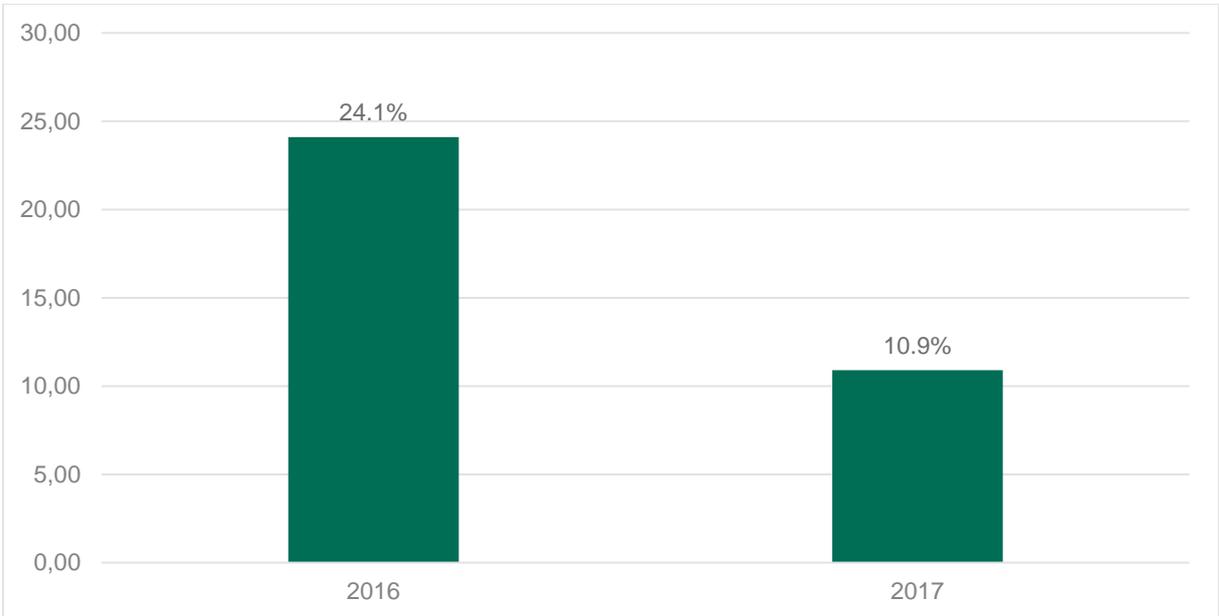


Fig. 4: The percentage of global internet portal phishing detected by Kaspersky Lab in 2016-2017

The list of targets has stayed more or less the same as in previous years. Among financial phishers' favorite targets are top transnational banks, popular payment systems

and internet shops and auction sites from the US and Asia. This is due to the popularity of these brands, which makes them attractive targets for cybercriminals.

## Financial phishing on Mac

MacOS is generally considered to be a much safer platform than Windows due to the lower number of malware families that exist for this operating system versus those for Windows. 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 other users. Moreover, 2017 also demonstrated that the figures almost doubled.

In 2016, 31.4% of phishing attacks against Mac-users were aimed at stealing financial data. This is almost half that seen in 2017, when 55.6% of financial attacks blocked by Kaspersky Lab were financially-themed. At the same time, the share of attacked unique users didn't show such significant growth.

That said, this near doubling of attacks can be explained by two factors:

- Strong growth in overall phishing detections – from over 150m detections in 2016, to over 246m in 2017. This is alarming and clearly indicates that phishing is on the rise.
- Criminals' tendency to repeatedly attack the same users. This is even more alarming as it increases the chances that victims will sooner or later lose vigilance and experience a hit.

Overall the split looks like this:

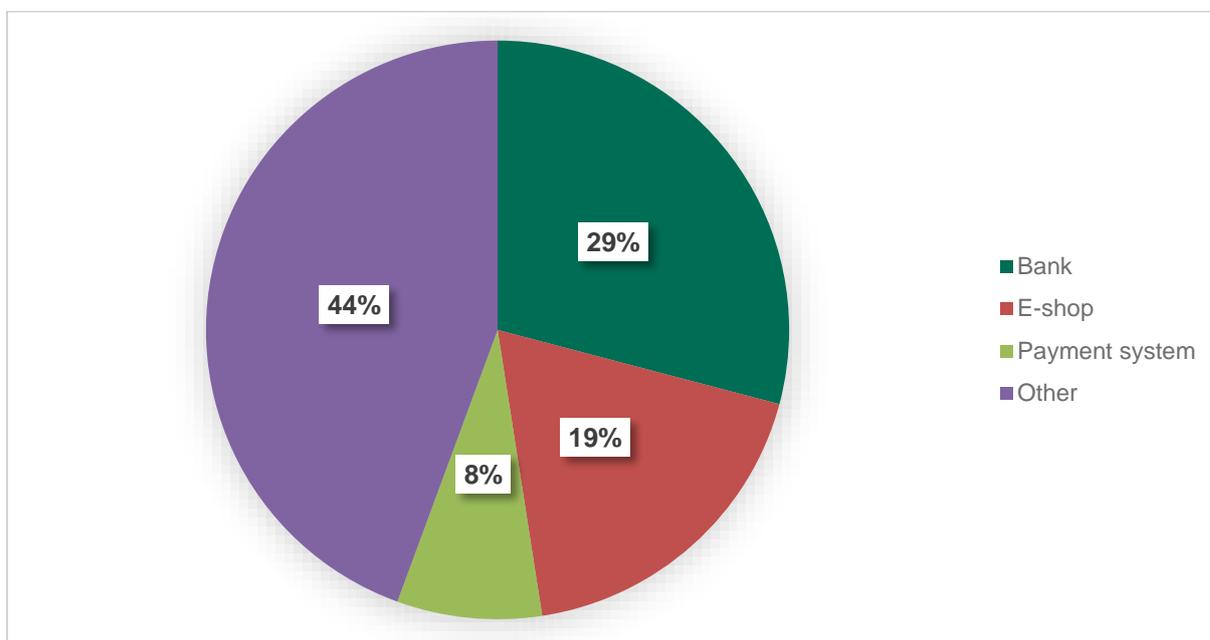


Fig. 5: The distribution of different types of financial phishing detected by Kaspersky Lab on Mac in 2017

Our data shows that the financial share of phishing attacks on Macs is also quite solid – as seen for other platforms. Let's have a closer look at both categories.

## Mac vs Windows

In last year's report, we detected one apparent platform-related feature of the financial phishing landscape for Mac. Based on the phishing page detection statistics from Windows-based computers, the list of the most frequently used brands in the online 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 the Apple Store. Criminals are aware of that trust and therefore try to exploit it.

Interestingly enough, this was not the case in 2017, as Apple became the leader in both categories - Mac and Windows detections.

Mac	Windows
Apple	Apple
Amazon.com: Online Shopping	Amazon.com: Online Shopping
eBay	MercadoLibre
Alibaba Group	Alibaba Group
Bell Canada	Steam
Steam	eBay
Wal-Mart Stores, Inc.	Focus Technology Co., Ltd
Netflix Inc	NOVA PONTOCOM COMERCIO ELETRONICO S.A
Apple	Wal-Mart Stores, Inc.

Fig. 6: The most frequently used brands in 'online shop' financial phishing schemes

When it comes to attacks on payment systems, the situation is as follows:

Mac	Windows
MasterCard International	Visa Inc.
PayPal	PayPal
American Express	American Express
Visa Inc.	MasterCard International
Xoom	qiwi.ru
Neteller	Western Union
alipay	Cielo S.A.
Skrill Ltd.	Skrill Ltd.
Western Union	alipay

Fig. 7: The most frequently used brands in 'payment systems' financial phishing schemes

In 2016, the leader was PayPal. It has now been replaced with Mastercard for Mac and Visa for Windows.

The tables above can serve as advisory lists 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 cards, online banking and payment system credentials.

## Phishing campaign themes

Today, cryptocurrency is no longer only for computer geeks and IT pros. It's starting to affect people's daily lives more than they realize. At the same time, it is fast becoming an attractive target for cybercriminals. Some cyber threats have been inherited from e-payments, such as changing the destination wallet address during transactions and stealing an electronic wallet, among other things. However, cryptocurrencies have opened new and unprecedented ways to monetize malicious activities.

In 2017, the main global threat to users was ransomware: in order to recover files and data encrypted by attackers, victims were required to pay a ransom in cryptocurrency. Further, in the first eight months of 2017, Kaspersky Lab products protected 1.65 million users from malicious cryptocurrency miners, and by the end of the year we saw this number exceed two million. In addition, in 2017 we observed the return of Bitcoin stealers after a few years in the shadows.

This also affected the topics that criminals use in their scams. The list of topics is no longer limited to fairly old copies of online banking, payment systems or internet shop web pages.

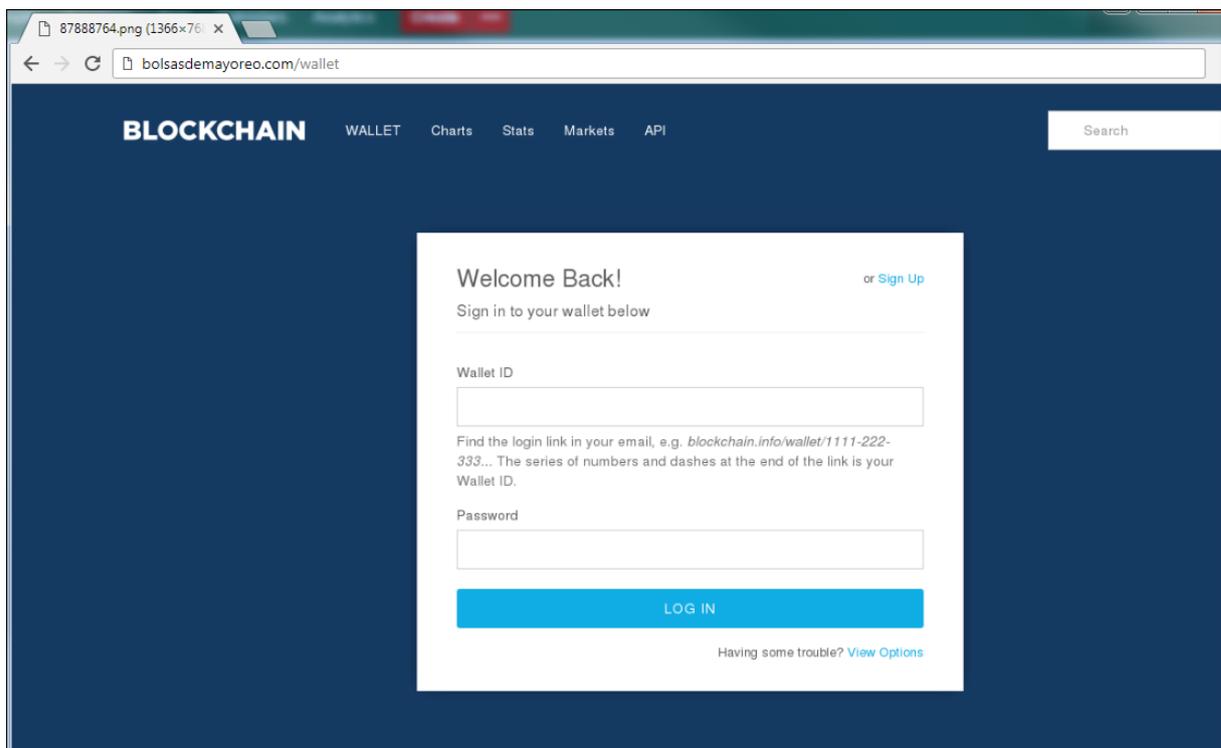


Fig. 8: A phishing message sent in under the guise of block chain wallet

One very interesting example emerged in the early part of 2017. The domain previously belonged to a real and legitimate major European bank.

```
Domain Name: [REDACTED].net
Registry Domain ID: 60268493_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.melbourneit.com
Registrar URL: http://www.melbourneit.com.au
Updated Date: 2013-01-04T03:05:00Z
Creation Date: 2001-02-12T14:13:57Z
Registrar Registration Expiration Date: 2014-02-13T01:13:57Z
Registrar: Melbourne IT Ltd
Registrar IANA ID: 13
Registrar Abuse Contact Email: abuse@melbourneit.com.au
Registrar Abuse Contact Phone: +61.386242300
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: [REDACTED]
Registrant Organization: [REDACTED]
Registrant Street: Kaiserplatz
Registrant City: Frankfurt a.M.
Registrant State/Province: Frankfurt a.M.
Registrant Postal Code: 60261
Registrant Country: DE
Registrant Phone: +49.6913645924
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: thomas.matzen@[REDACTED].com
Registry Admin ID:
Admin Name: Thomas Matzen
Admin Organization: Matzen
Admin Street: Mainzer Landstrasse 151
Admin City: Frankfurt am Main
Admin State/Province: Frankfurt am Main
Admin Postal Code: d - 60261
Admin Country: DE
Admin Phone: +49.6913624918
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: thomas.matzen@[REDACTED].com
Registry Tech ID:
Tech Name: Frank Plettenberg
Tech Organization: [REDACTED]
Tech Street: Mainzer Landstrasse 151
Tech City: Frankfurt am Main
Tech State/Province: Frankfurt am Main
Tech Postal Code: 60327
Tech Country: DE
Tech Phone: +49.6913645924
Tech Phone Ext:
Tech Fax: +49.6913650200
Tech Fax Ext:
Tech Email: frank.plettenberg@[REDACTED].com
Name Server: NS2.[REDACTED].com
Name Server: NS4.[REDACTED].com
Name Server: NS5.[REDACTED].com
Name Server: NS3.[REDACTED].com
```

Fig. 8: The bank's domain

In 2014, it stopped and the domain was acquired by fraudulent users who then uploaded phishing content to it. The phishing content was not only aimed at financial organizations, but also at the very same bank that previously owned the domain.

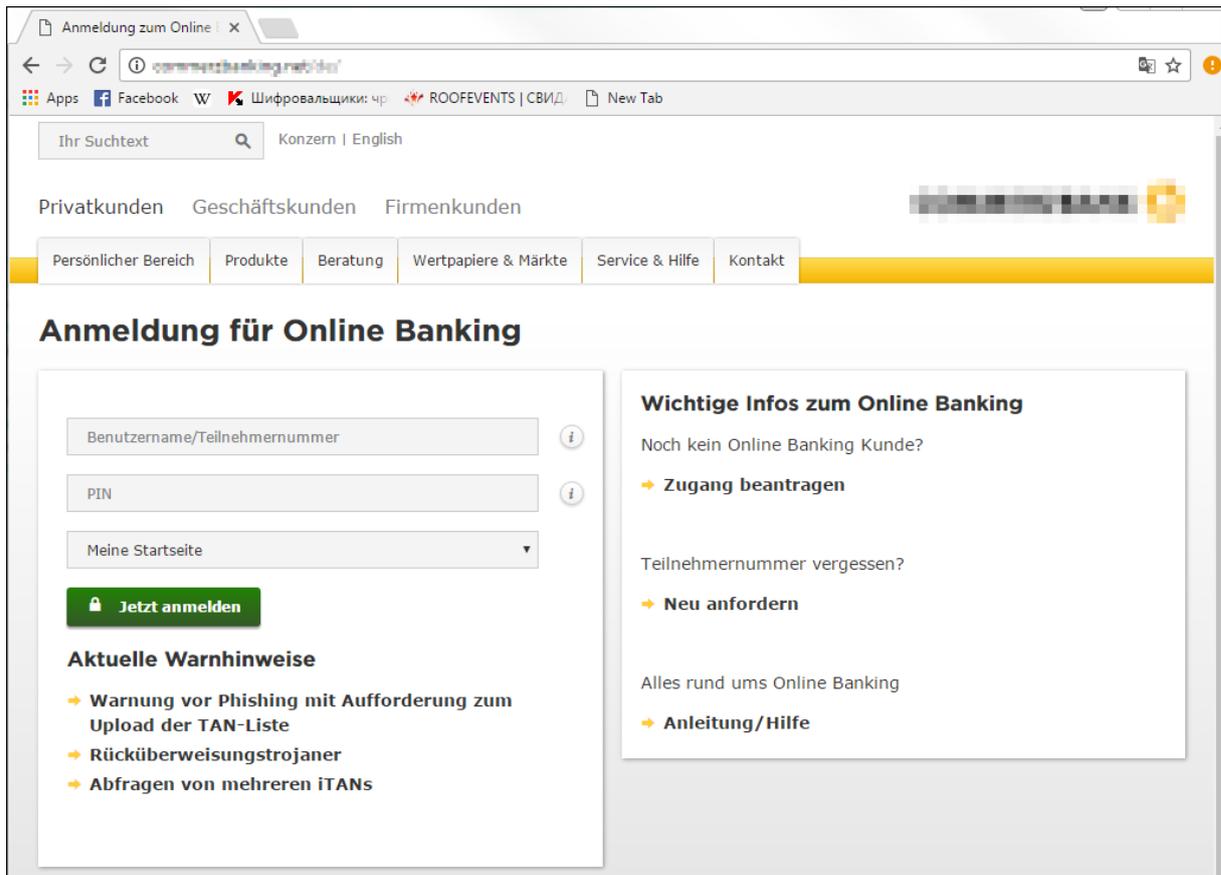


Fig. 9: The phishing page

This is a good example of how a domain with a good reputation allows criminals to reduce the risk of being caught or their attacks being blocked, and to increase victims' trust.

Another interesting case was the use of PayPal phishing pages placed on servers belonging to the state.

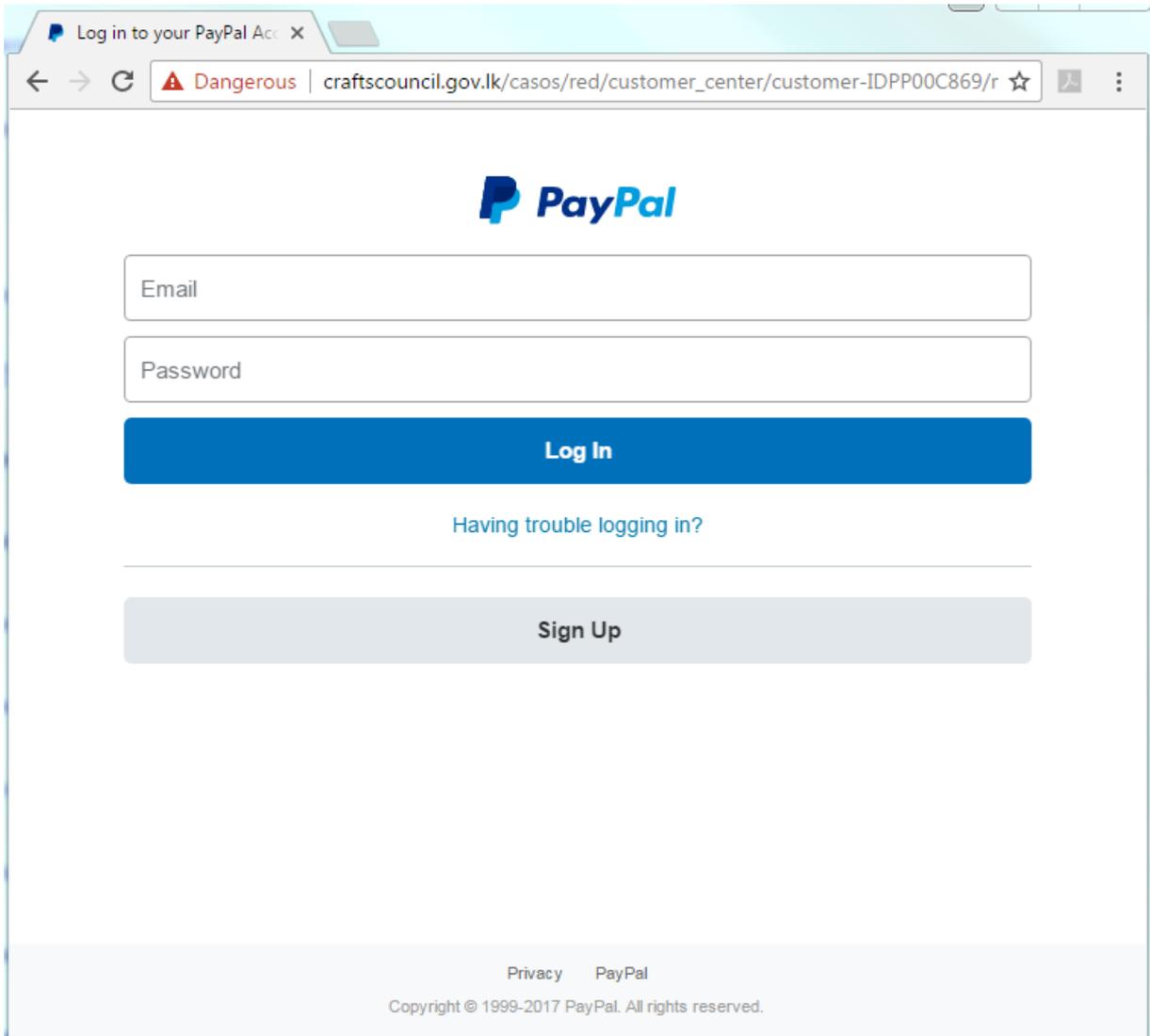


Fig. 10: A phishing message sent in the name of a government body.

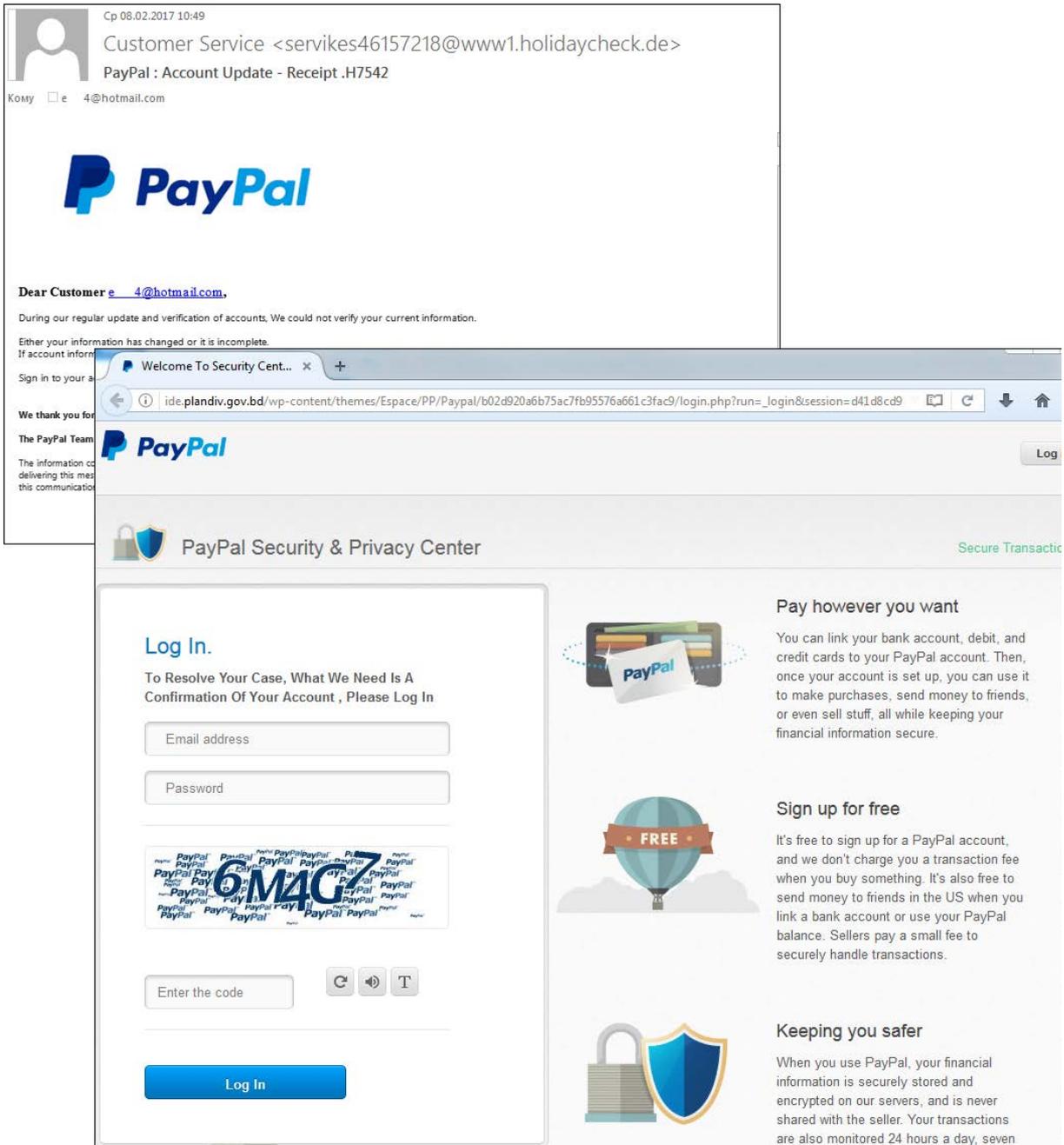


Fig. 11: A phishing messages sent in the name of a government body.

This is yet another reminder that we can be hit not only from the commercial side, sometimes state resources are also vulnerable to criminals. The message contained a link to an external page, where an information update was required. Of course, that wasn't real, it was all set up by criminals to collect critical user information.

Typically, financial and payment systems are the most common phishing themes. A good example is Visa phishing on the Salesforce server domain. A trusted service and https connection reduce vigilance and increase cybercriminals' chances of success.

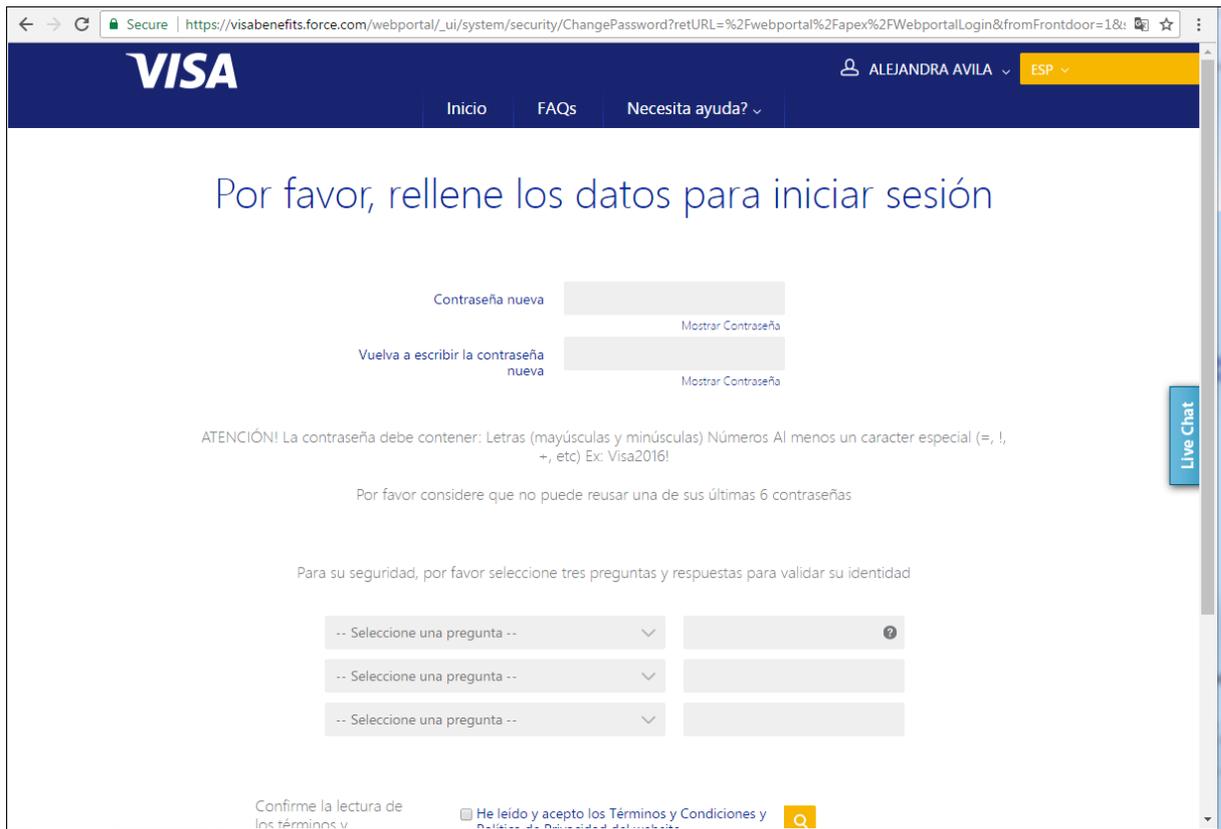


Fig. 12: A Visa-based phishing scheme

Apart from well-known commercial brands and state resources, another way to increase the chance of being perceived as a trusted source is to use the guise of security solutions. In 2017, we found an interesting example of a PayPal phishing attack with the use of a major cyber security vendor. Also, one of the most common tricks is intimidation, using the threat of blocking or breaking in to an account ("your account has been suspended").

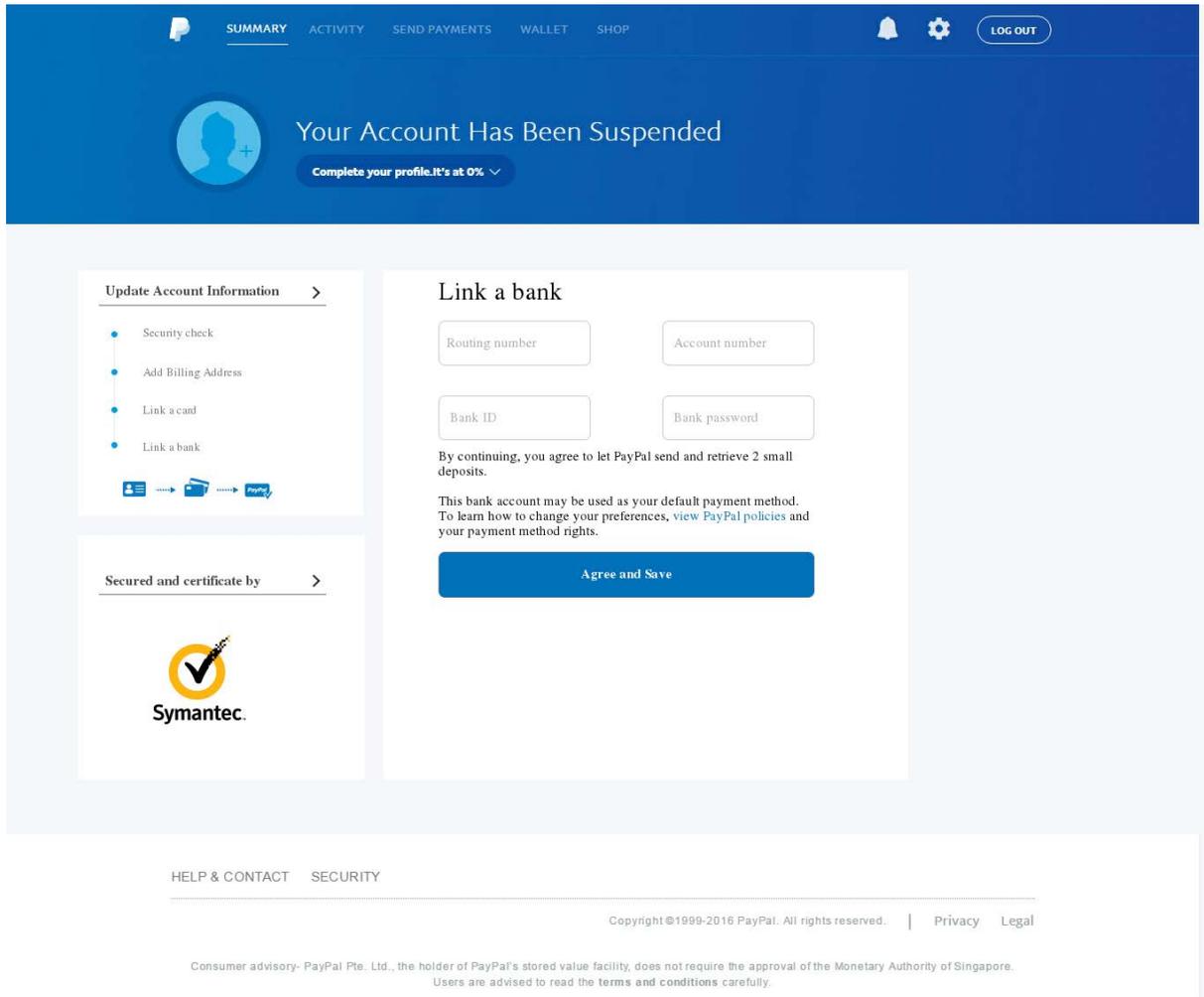


Fig. 13: A security solution-based phishing scheme

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.

## Don't show your credit card data to strangers

Phishing has for years been considered a tool that can be monetized. And not only by fraudsters – even APT actors involved in 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 conclusion here is simple: always stay vigilant. Always check the legitimacy of the website while paying online. This is indicated by the https connection, and the domain belonging to the same organization that you're going to pay. The legitimacy of emails is another fact you should examine, especially if they urge you to do something – like change your password.

If you can't be sure of the above - don't click the link.

And don't forget to use a proven security solution with behavior-based anti-phishing technologies. This will make it possible to identify even the most recent phishing scams that haven't yet been added to anti-phishing databases.

# Banking malware

When talking about financial malware, we at Kaspersky Lab historically mean several types of malicious software. First of all, there is banking malware, designed to steal the credentials used to access online banking or payment system accounts and to intercept one-time passwords. In addition, there have also been versions of generic keyloggers spotted in attacks against online banking and payment systems, 'Host' Trojans that change 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.

This paper will only focus on banking Trojans.

In recent years we have seen steady growth in the number of users attacked with any kind of financial malware – after falls in 2014 and 2015. In 2017, the decrease returned with the number of attacked users falling to 767,072 from 1,088,933 users worldwide in 2016 – almost a 30% decline. This is due to the fact that many leading malware families are becoming quite outdated, meaning criminals tend to use them less often. This is the case with Zeus, SpyEye, Neurevt, and Shitob. Another reason is that malicious users are turning their eyes to cryptocurrency theft or mining as a more profitable activity. This could be also a sign that criminals are becoming more experienced and are focusing a lot of their attention on targeted attacks against large companies.

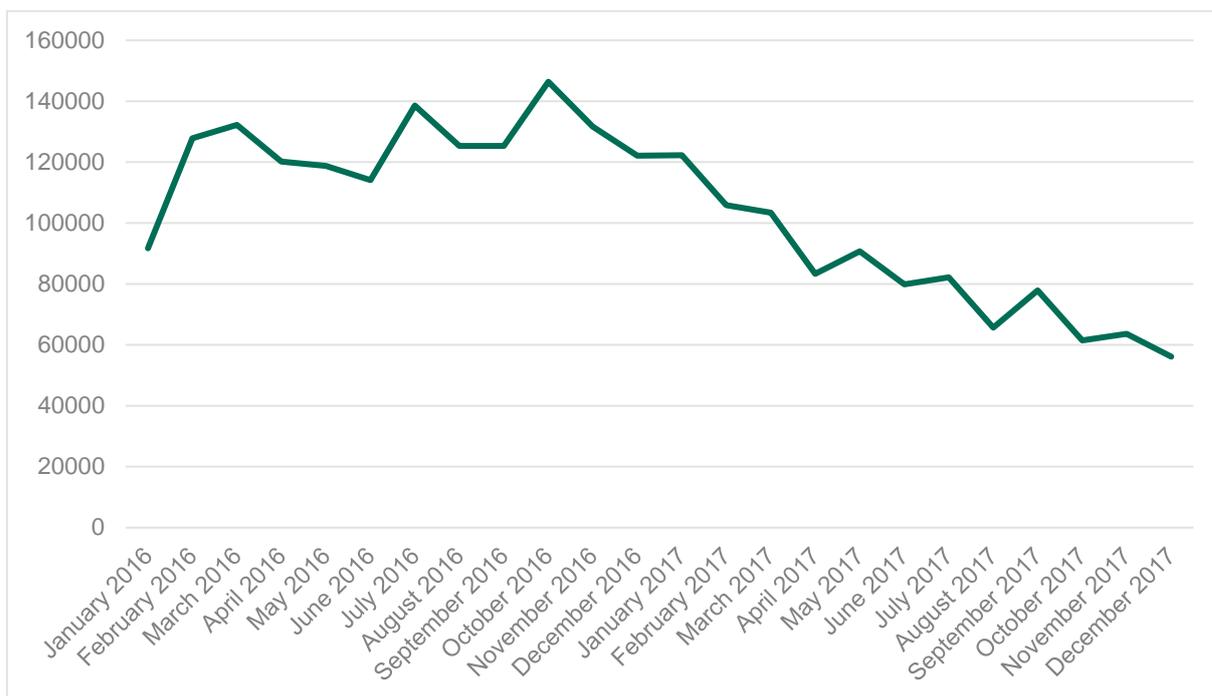


Fig. 14: The dynamic change in the number of users attacked with banking malware 2016-2017

## The geography of attacked users

As shown on the charts below, more than half of all users attacked with banking malware in 2016 and 2017 were located in only ten countries.

In 2016, the ultimate leader was Russia – just as in 2015. Last year it was followed by Germany and Japan.

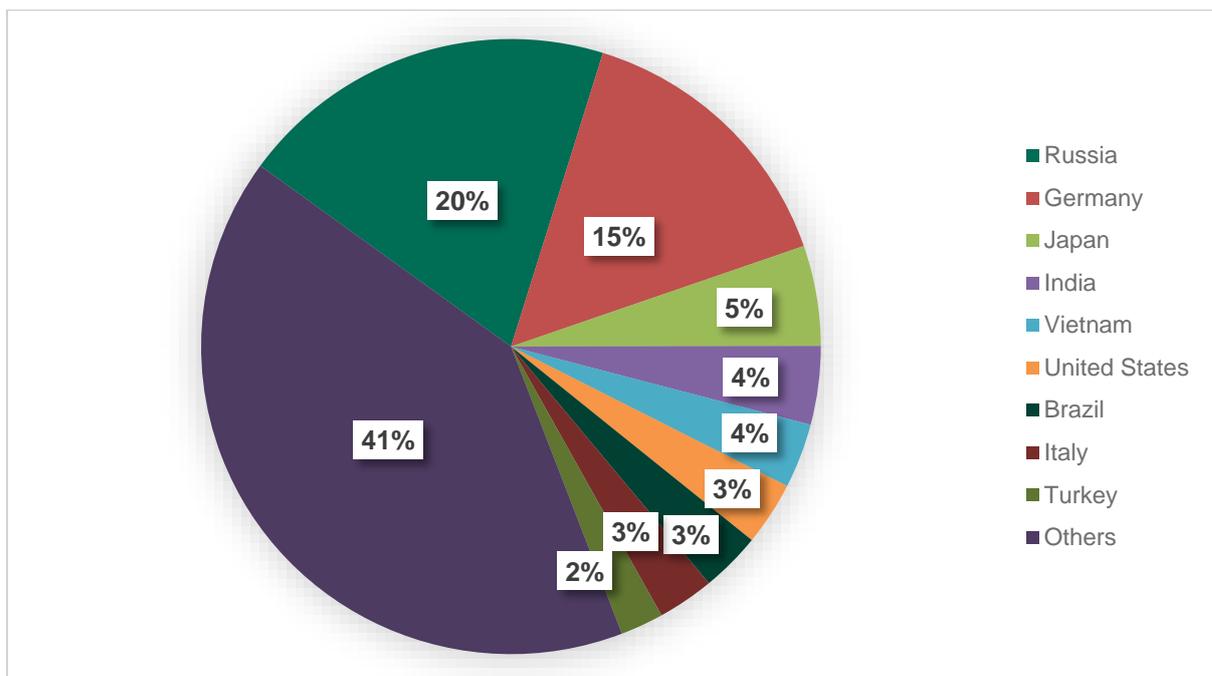


Fig. 15: The geographic distribution of users attacked with banking malware in 2016

In 2017, Russia was replaced by Germany, moving down to second position, followed by China. This shift was caused by two-factor authentication providing an extra layer of security being widely embraced in Russia's financial and payment services. This pushed criminals into looking for lucrative targets somewhere outside the region.

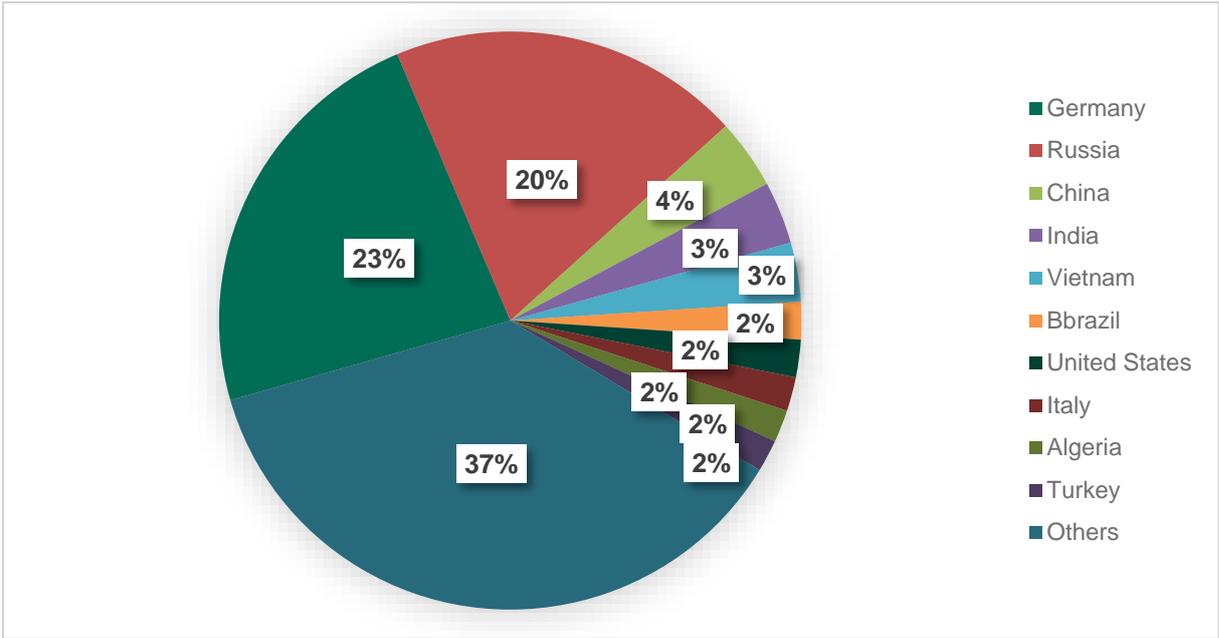


Fig. 16: the geographic distribution of users attacked with banking malware in 2017

## The type of users attacked

When speaking about banking malware, one could assume that it is always in reference to attacks on individual consumers. However, the statistics refute this.

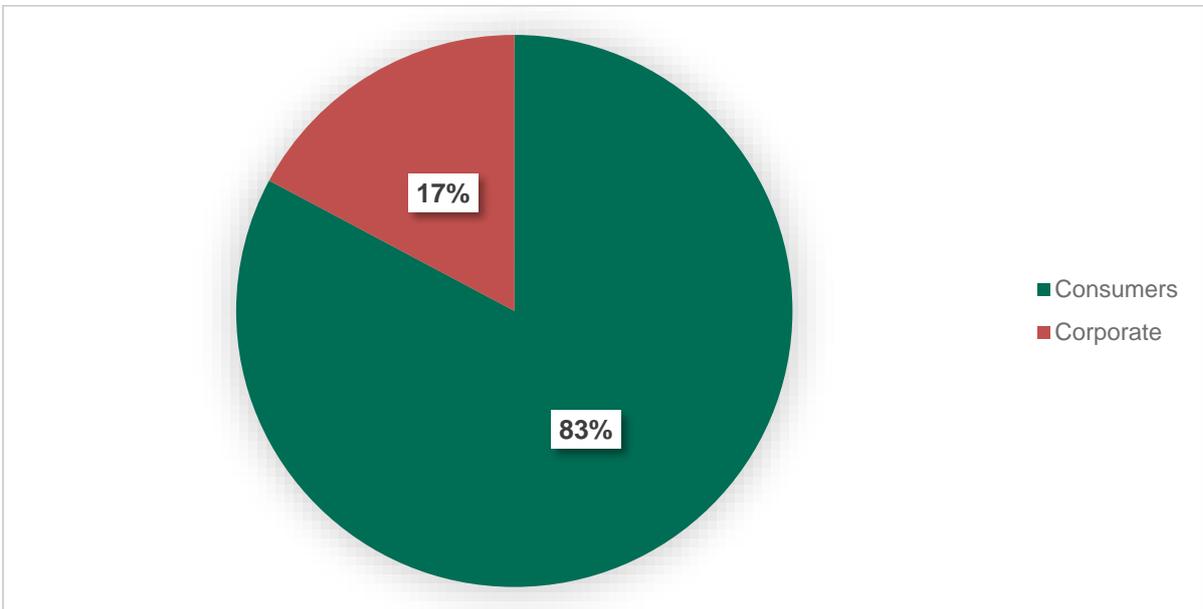


Fig. 17: The distribution of attacked users by type in 2016

As we can see, in 2016 the share of corporate users was 17.2%. But 2017 has shown a slight growth of this sector, confirming our hypothesis that criminals are shifting to targeted attacks on business – despite the overall fall of banking malware detection, the corporate users’ share is still showing a steady rise.

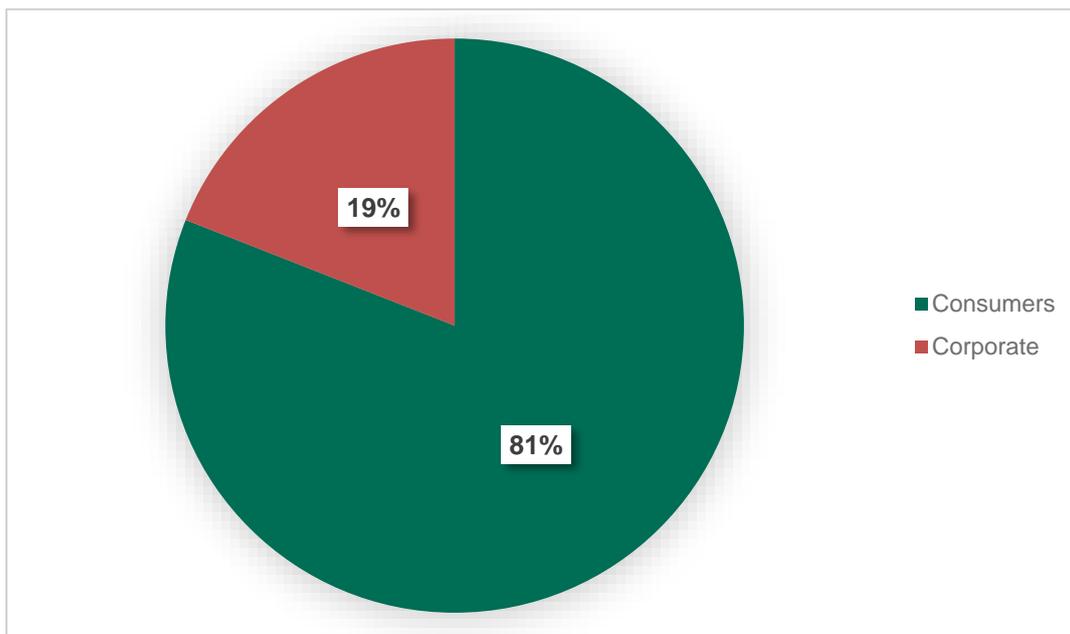


Fig. 18: The distribution of attacked users by type in 2017

This is alarming, as we see that for the last three years in a row, almost every 5<sup>th</sup> banking malware attack was focused on the corporate sector. And the share is growing. The reason behind this is clear – while attacks on consumers will only give a criminal access to banking or payment system accounts, successful hits on employees will also compromise a company's financial resources.

## The main actors and developments

At Kaspersky Lab we currently track over 70 families of banking malware. But when it comes to major players, the picture is different. Below you can see a list of the top seven most active banking malware families. In 2016, these were Zbot, Gozi, Nymaim, Shiotob, ZAccess, Tinba, and Shiz.

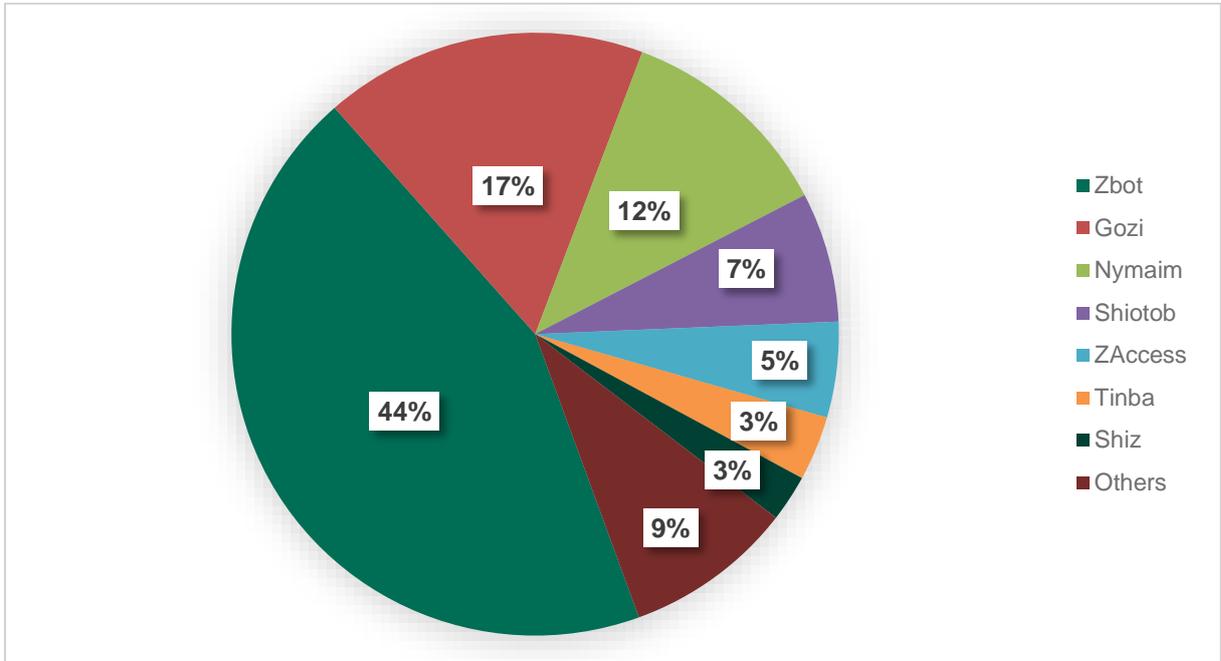


Fig. 19: The distribution of the most widespread banking malware families in 2016

In 2017, the situation changed slightly. While Zbot kept its leadership position, it was actively challenged by Gozi.

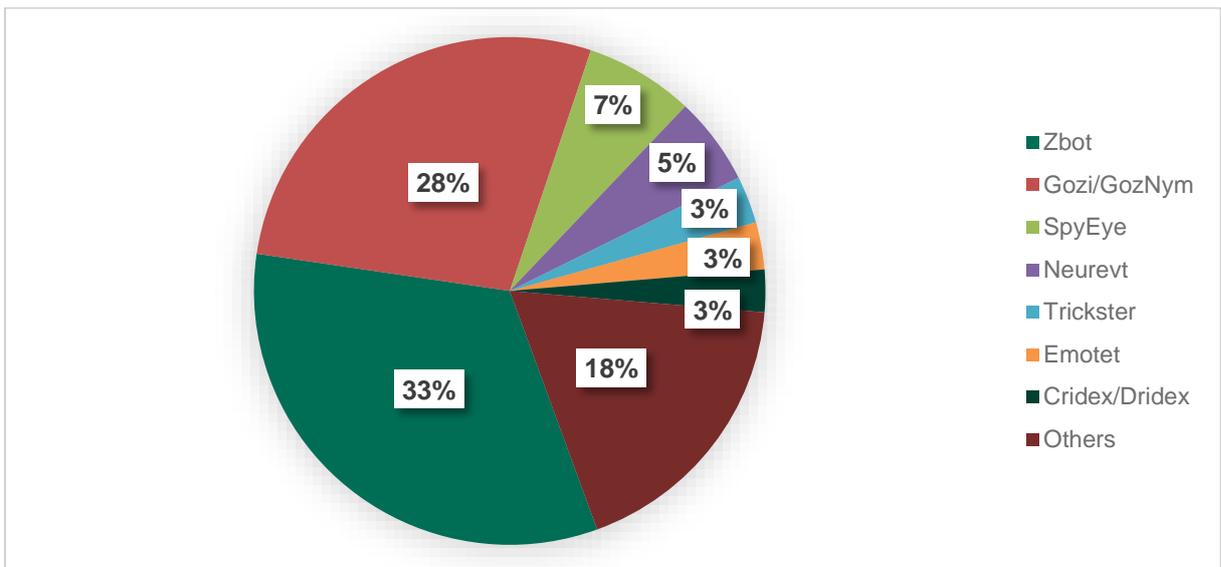


Fig. 20: The distribution of the most widespread banking malware families in 2017

As we can see in the statistics for 2017, Zbot's leadership was questioned due to the growing challenge of Gozi, which increased its share by more than 10 percentage points, while Zbot decreased its own from over 44% to 32.9%.

Even more interesting is the share of the 'others' category, which more than doubled, indicating that the financial threat landscape is becoming more and more diverse. That said, while the proportion of leaders is reducing, smaller players are becoming more active.

This is not good in terms of cyber security as it is much easier to track several big players than a centurion of attackers that are small and flexible in their tactics. Zbot, being on the last leg of its leadership, is apparently running out of its most beneficial resource – a source code that has been available on the open web for several years. At first this had attracted more and more criminals, but as the time has passed, security vendors have adapted their solution to this code, resulting in its decreasing efficiency.

Interestingly, if we take a look not at the users attacked, but at the unique attacks performed by the malware, the situation is different. These attacks include malware activities such as web injects, traffic redirection, URL spoofing, and form grabbing.

First of all, these almost doubled between 2016 and 2017:

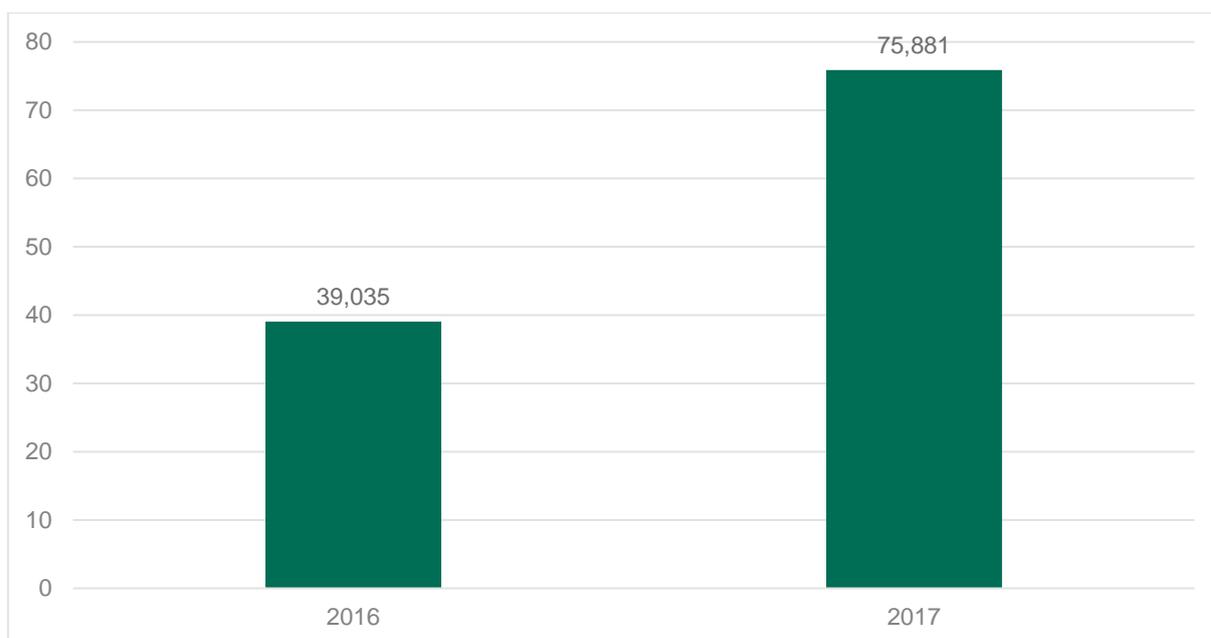


Fig. 21: The number of unique attacks by banking malware in 2016 and 2017

At the same time, the list of top players in the field is also different. As we can see below, the highest number of unique attacks was also performed by several players but with Citadel as the absolute leader.

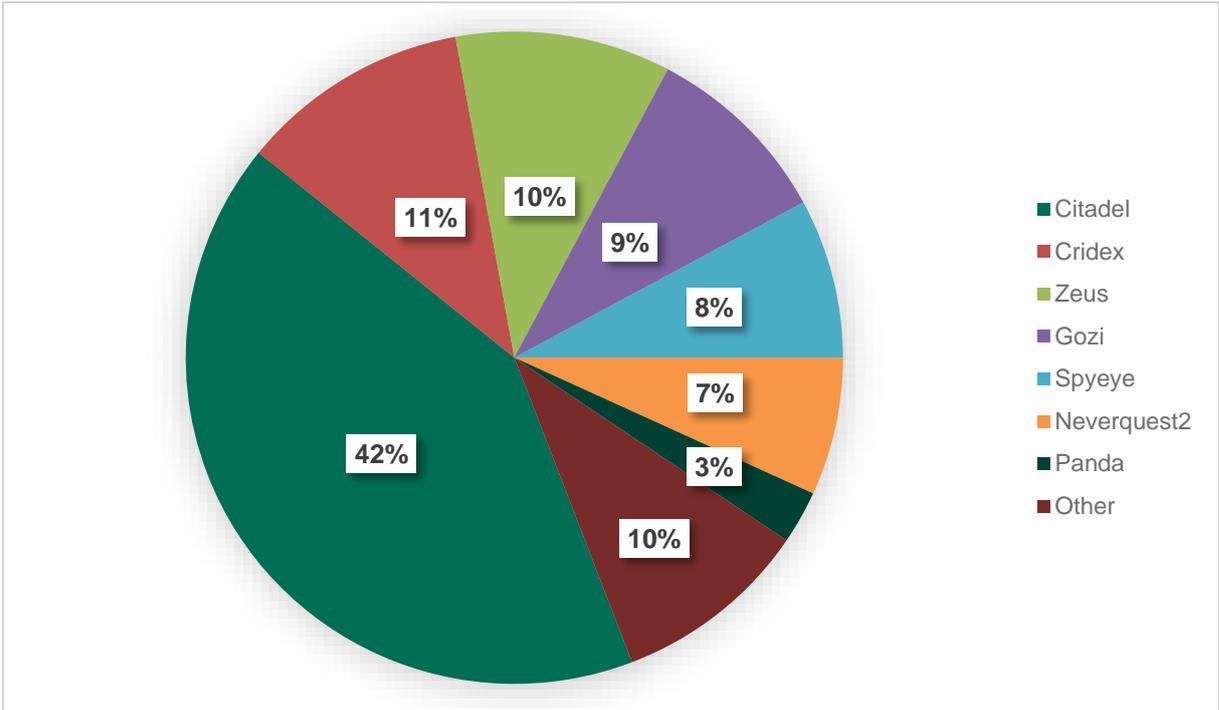


Fig. 22: Share of unique attacks by banking malware in 2016

And in 2017 it looked like this:

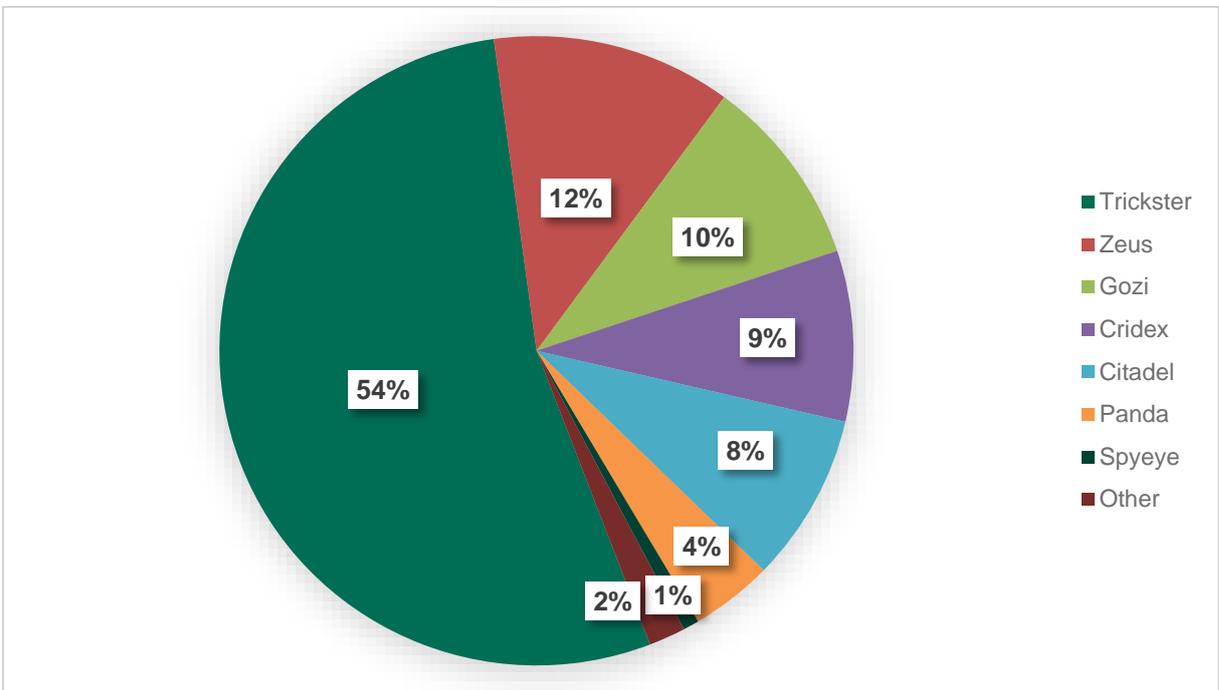


Fig. 23: Share of unique attacks by banking malware in 2017

In just one year the situation changed, with Trickster topping the list while Citadel fell to fifth place.

Both the difference in the number of attacks and in the share, could be explained by the explosive growth of the Trickster family. This family conducts traffic redirection to its server from over thousands of banking domains. The criminals behind it update configuration files several times per week, which has almost doubled the overall number of attacks.

Trickster itself is a [successor](#) to Dyre (aka Dyreza), which was highly [active](#) in 2014-2015. Its activity fell to nothing in November 2015, but then Trickster emerged at the end of 2016, changing the game in 2017 – yet another reminder that everything new is actually just the well-forgotten old.

With both top lists available, we can say that Gozi is an unchallenged leader in terms of its attack effectiveness – it is number two in terms of attacked users in both 2016 and 2017, while it enters the top three or top four in terms of the number of unique attacks.

In general, 2017 was rich with interesting new findings related to banking malware. It even [shed](#) some light on the Lazarus Group activities, and their connection to the much talked about February 2016 incident, when the attackers attempted to steal up to \$851M USD from Bangladesh Central Bank.

It was not obvious whether Lazarus was the one responsible for the fraudulent SWIFT transactions, or if Lazarus had in fact developed its own malware to attack the bank systems. Lazarus was previously known to conduct cyberespionage and cybersabotage activities, such as the attacks on Sony Pictures Entertainment (when volumes of internal data was leaked and many of the company's system hard drives were wiped). Their interest in financial gain is relatively new, considering the age of the group, and it seems that they have a different set of people working on the problems of invisible money theft or the generation of illegal profit.

We believe that Lazarus Group is very large and works mainly on infiltration and espionage operations, while a substantially smaller unit within the group, which we have dubbed Bluenoroff, is responsible for financial profit. Bluenoroff has targeted financial institutions, casinos, companies developing financial trade software and those in the cryptocurrency business, among others. One of the most notable Bluenoroff campaigns was its attacks on financial institutions in Poland.

Last year also revealed an alarming trend. Supply chain attacks appear to be the new 'watering holes' when it comes to targeting business victims. This was an emerging threat in 2017, seen in ExPetr and [ShadowPad](#), and it looks set to [increase](#) further in 2018. These attacks can be extremely difficult to identify or mitigate. For instance, in the case of Shadowpad, the attackers succeeded in Trojanizing a number of packages from Netsarang that were widely used around the world, in banks, large enterprises, and other industry verticals. The difference between the clean and Trojanized packages can be dauntingly difficult to notice – in many cases it's the command and control (C&C) traffic that gives them away.

For CCleaner, it was estimated that over two million computers received the infected update, making it one of the biggest attacks of 2017. Analysis of the malicious CCleaner code allowed us to correlate it with a couple of other backdoors that are known to have been used by APT groups in the past from the 'Axiom umbrella', such as APT17 (also known as Aurora). This proves the now extended lengths to which APT groups are willing to go, in order to accomplish their objectives.

Our assessment is that, at the moment, the amount of supply chain attacks is probably much higher than we realize, but some have yet to be noticed or exposed. During 2018, we expect to see more supply chain attacks, both from the point of discovery, as well as actual attacks. Trojanizing specialized software used in specific regions and verticals will become a move akin to waterholing strategically chosen sites, in order to reach specific swaths of victims. This will prove irresistible to certain types of attackers.

Given all the above, we can say that the banking malware underground keeps producing new ways and tactics to steal our money, or data which they can sell afterwards. This means that despite banks' heavy investment in cyber security, 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 is a well-known threat that has been in the wild for years. As we demonstrated last year, 2016 saw an explosive growth in Android banking malware, peaking from just 3,967 users in January 2016, to almost 75,000 users 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. But then the game changer came.

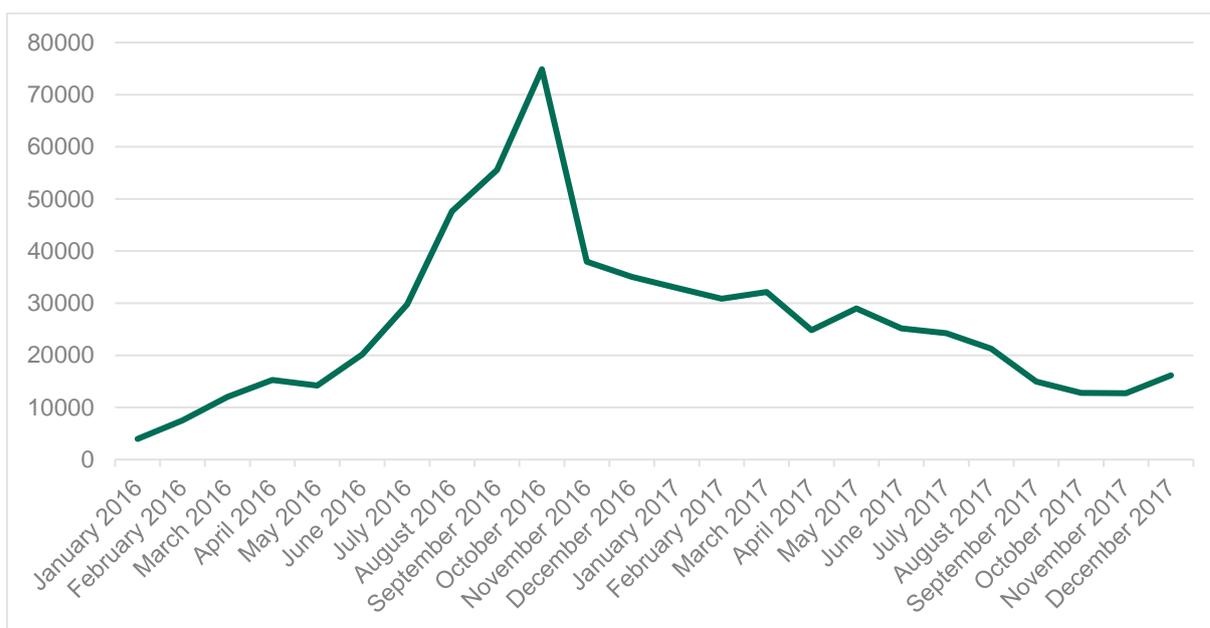


Fig.24: The change in the number of users attacked with Android banking malware 2016-2017

This is what happened: the number of attacked users started to fall rapidly from month to month, with the overall figure at the level of 259,828 – an almost 15% decrease y-o-y. At the same time, the share of users facing mobile financial malware also fell – from 1.57% in 2016 to 1.01% in 2017.

Kaspersky Lab experts took a closer look at the reasons why. The fall was due to different methods of distribution. In 2016 the leader was Svpeng, a well-known banking Trojan which we've described in our research many times. In the year before, it had started distributing in a new way: through the Google AdSense advertising network. While targeting mostly users from Russia and CIS, it reached a massive distribution because of security issues in a popular mobile browser, which allowed the malicious application to be automatically downloaded onto the attacked device. The Svpeng peak was in August-October, hitting the same users several times.

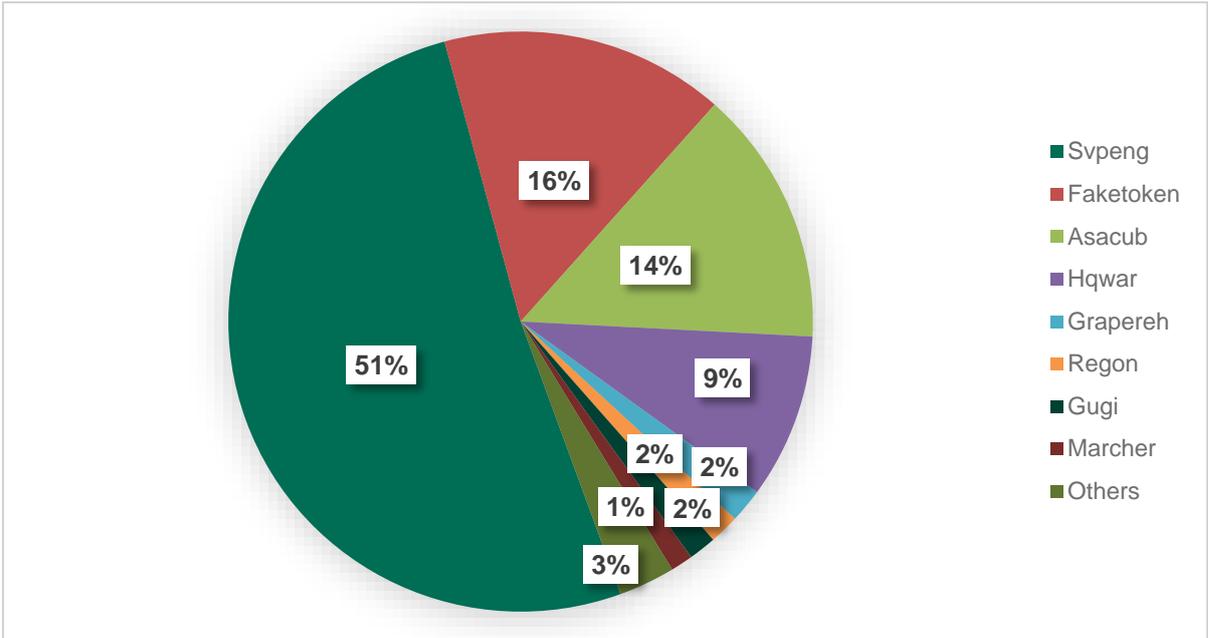


Fig. 25: The most widespread Android banking malware in 2016

Then in 2017, the chart turned out to be completely different - the distribution of the major families was calmer and smoother. Without Svpeng's super growth in June-October 2016, the statistic looked more or less balanced.

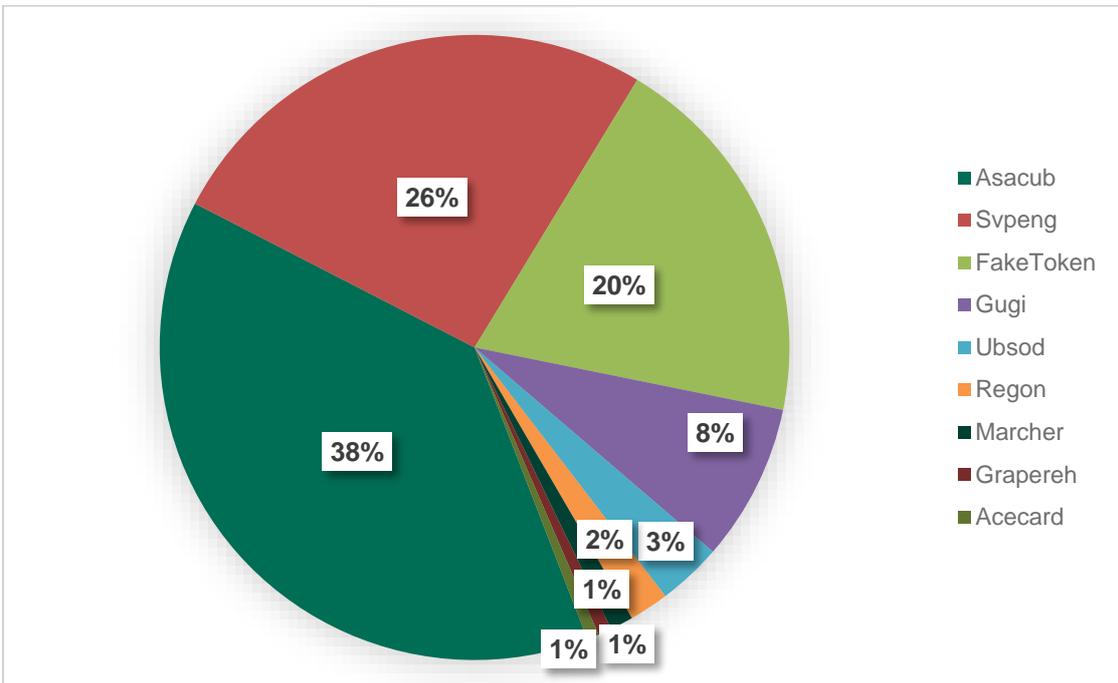


Fig. 26: The most widespread Android banking malware in 2017

If we take the overall number of detections, the absolute leader in 2017 was Hqwar. However, these detections relate to the Trojan-Dropper.AndroidOS.Hqwar obfuscator, used by a number of families from bankers to ransomware. If we exclude it, we get the picture above.

Svpeng fell from the throne, leaving first place to Asacub – with every third attack related to this. Asacub is spread via SMS and its distribution is highly uneven:

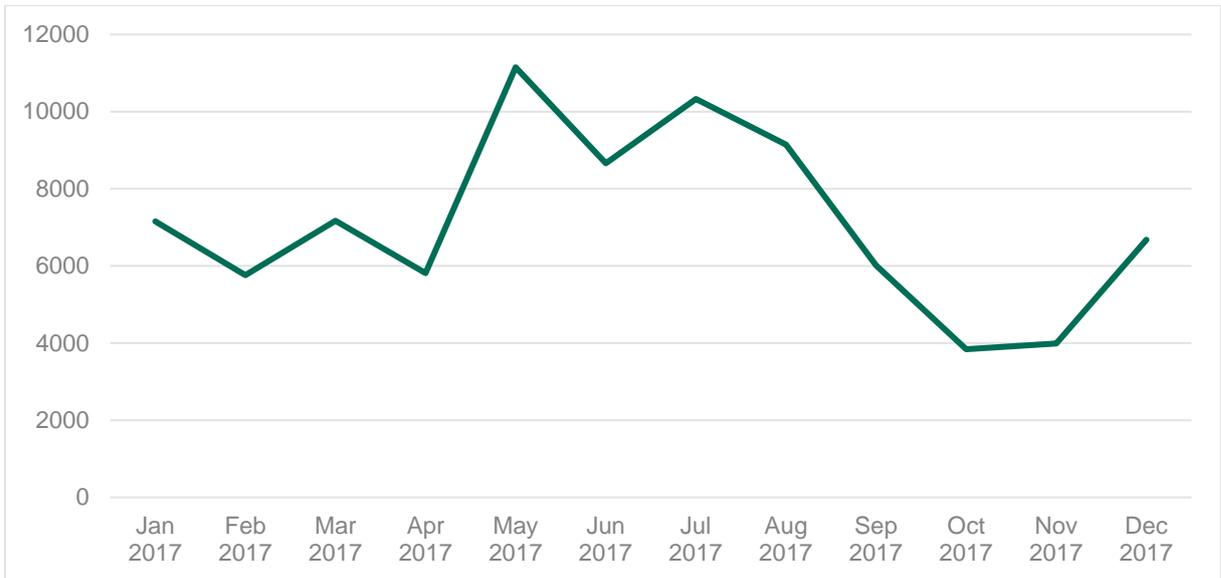


Fig.27: The change in the number of users attacked by the Asacub Android banking Trojan

At the same time, Svpeng evened out its activities, gradually lowering its hits from over 11,000 in January, to less than 3,000 in December.



Fig.28: The change in the number of users attacked by the Svpeng Android banking malware

The third major player in the field, Faketoken, demonstrated more or less the same picture.



Fig. 29: The change in the number of users attacked with Faketoken banking malware

## Geography of attacked users

In 2016 the geographical distribution was the following:

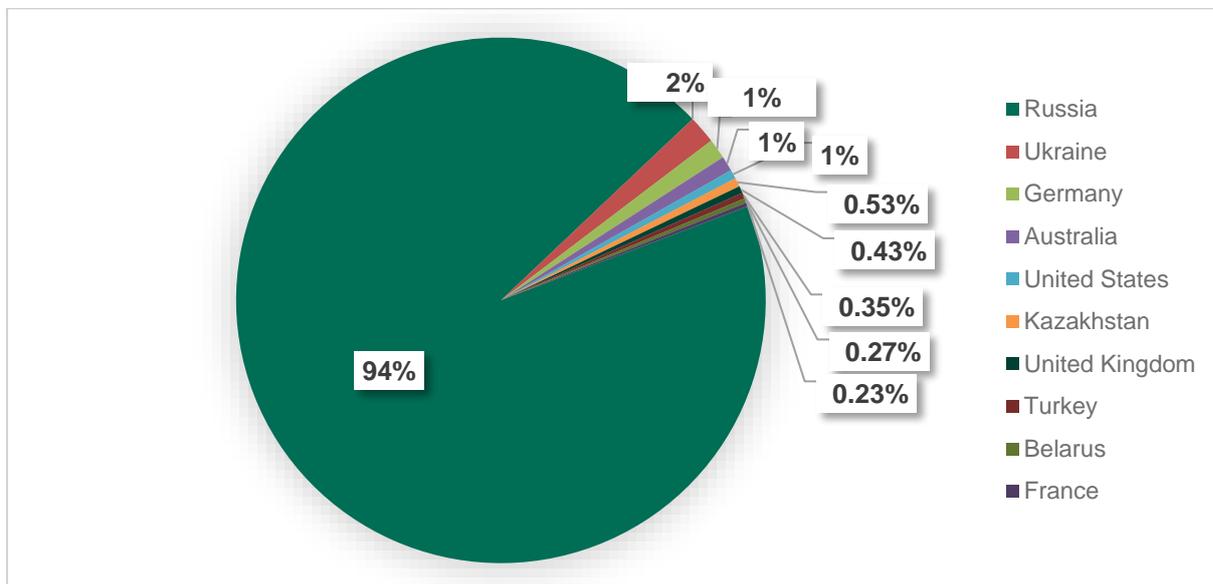


Fig. 30: The distribution of users attacked with Android Banking Trojans in 2016

A year later, the landscape had changed:

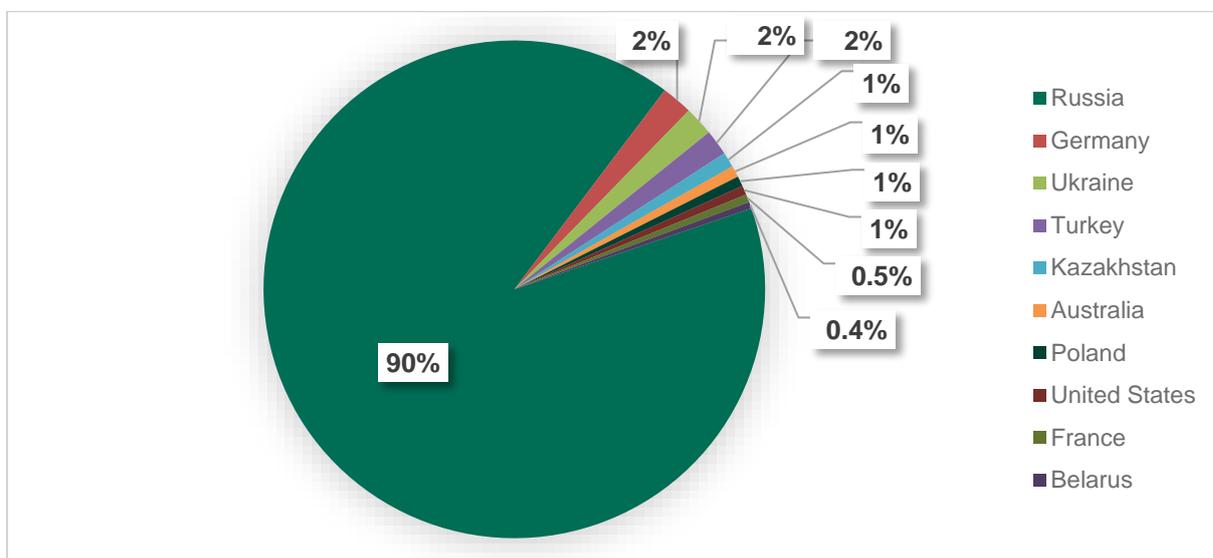


Fig. 31: The distribution of users attacked with Android Banking Trojans in 2017

While the top three included the same countries, the UK left the chart, and Turkey made it to 4<sup>th</sup> place – mainly due to Asacub activation in the region.

As can be seen on the charts above, Android banking malware is a mostly Russian problem. It should be said that these findings are affected by the fact that among the major countries, Russia presents the biggest interest for banking Trojans. This is mainly due to prevalence of SMS banking in the region, which allows attackers to steal money

with a simple text message in the case of successful infection. Previously, the same was true for SMS Trojans, but after regulative measures, criminals have found a new way to capitalize on victims in Russia.

However, if we exclude Russia we will see a more realistic picture. In 2016 it looked like this:

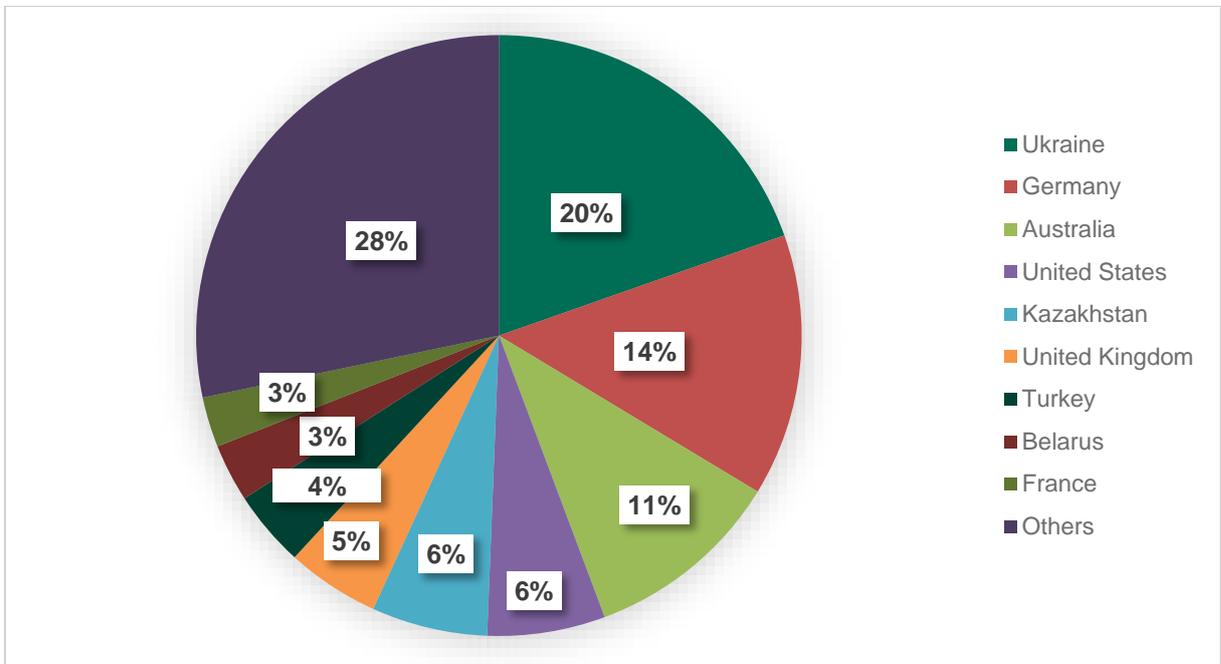


Fig. 32: The distribution of users attacked with Android banking malware in 2016 (a total of 26,110 users, Russia excluded)

And in 2017 it looked like this:

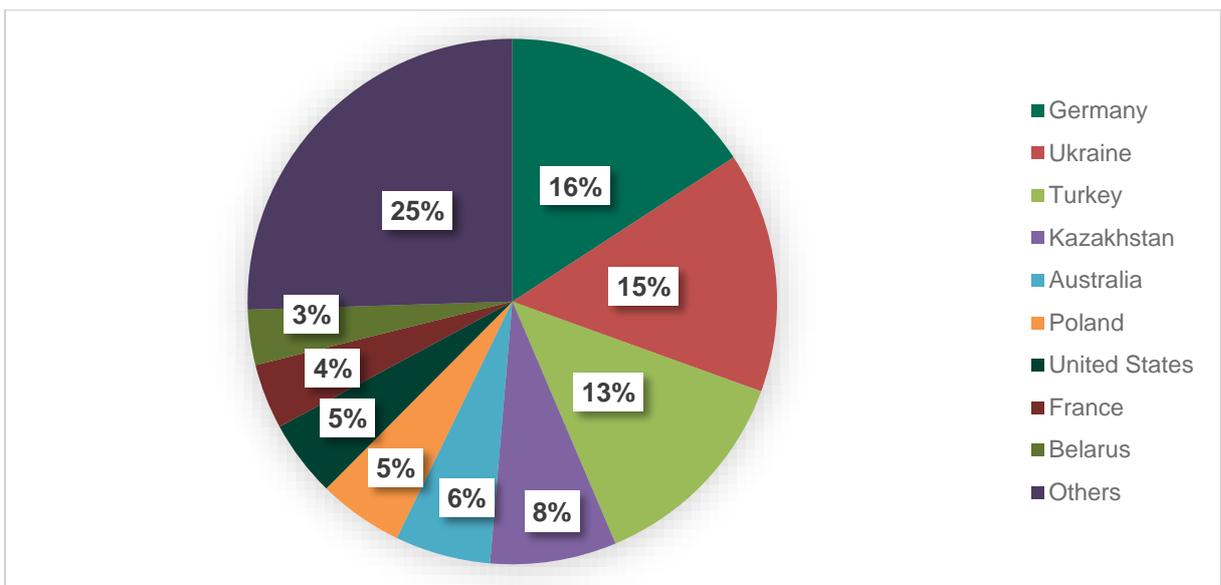


Fig. 33: The distribution of users attacked with Android banking malware in 2017 (a total of 32,058 users, Russia excluded)

Germany and Ukraine once again swapped positions in the ranking in 2017, compared

to 2016 and 2015. While the share of German users attacked with Android banking malware grew, the share of Ukrainian users fell. In 2017, Australia also left the top three most often attacked countries (excluding Russia), while Turkey joined the top three.

When it comes to major countries hit by the threat, the situation remains the same – while Russia tops the list, mobile banking malware is not the biggest threat for the other countries. However, in 2016 it rarely exceeded a couple of thousand users per nation. Interestingly enough, in 2017 a lot of the top 10 countries experienced an influx of attacks – for instance Turkey saw four-fold growth and France experienced a doubling growth. At this time, Russia felt some relief, reducing its number of hits by almost 20%. This could be a sign of new trend of mobile malware spreading more steadily across the regions.

When looking 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 2017, 1.01% of global Kaspersky Lab product users 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	2.44%	Kazakhstan	0.59%
Australia	1.14%	Tajikistan	0.56%
Turkmenistan	1.01%	Moldova	0.52%
Turkey	0.95%	Ukraine	0.51%
Uzbekistan	0.68%	Latvia	0.40%

*Fig. 34: The top 10 countries with the highest percentage of users that encountered Android banking malware in 2017*

As can be seen in the table above, while overall numbers across the regions are incomparable, the shares are. Obviously, Australian and Turkish owners of Android-based smartphones should also be cautious.

## 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. But statistics allow us to monitor the trends of malware increases and decreases, its geographical spread, and the activities of major actors. However, the examination of the latter also allows us to provide analysis of actual malware found in the wild.

An interesting newcomer for 2017 was [Ubsod](#) (Trojan-Clicker.AndroidOS.Ubsod), part of the clicker family. This is a powerful Trojan with lots of capabilities. It can download and install apps, overlay other apps with its windows (mostly to steal credentials or credit card details), show ads, send SMS messages, steal incoming messages and even execute commands in the device shell. Further, it has features that steal money by abusing WAP-billing services.

Besides this, malware families that already existing have also evolved. For example, we've already [discussed](#) that in 2017 there was a new modification of the well-known mobile banking malware family Svpeng – Trojan-Banker.AndroidOS.Svpeng.ae. The Svpeng malware family is known for being innovative. Starting from 2013, it was among the first to begin attacking SMS banking, to use phishing pages to overlay other apps to steal credentials, and to block devices and demand money. In 2016, cybercriminals were actively distributing Svpeng through AdSense, using a vulnerability in the Chrome browser. This makes Svpeng one of the most dangerous mobile malware families, and it is why we monitor the functionality of new versions.

In its new modification, cybercriminals have added a new functionality: it now also works as a keylogger, stealing entered text through the use of accessibility services. These capabilities, from the point of view of financial threats, are extremely dangerous, as they are hidden, work on modern devices, and there is no need to use exploits to increase privileges.

Accessibility services generally provide user interface (UI) enhancements for users with disabilities or those temporarily unable to interact fully with a device, perhaps because they are driving. Abusing this system feature allows the Trojan not only to steal entered text from other apps installed on the device, but also to grant itself more permissions and rights, and to counteract attempts to uninstall the Trojan. Attack data suggests this Trojan is not yet widely deployed. In the space of a week, we observed only a small number of users attacked, but these targets spanned 23 countries. Most attacked users were in Russia (29%), Germany (27%), Turkey (15%), Poland (6%) and France (3%).

This points to the fact that in 2017, cybercriminals further expanded the field of attack vectors on bank accounts, attacking versatile applications which users have attached their bank cards to.

Actors behind the Faketoken Trojan produced a [new](#) Trojan sample, Faketoken.q, which contained a number of curious features. The authors of Faketoken.q kept the overlay features and simplified them considerably. So, the Trojan is capable of overlaying several banking and miscellaneous applications, such as Android Pay, Google Play Store, and apps for paying traffic tickets and booking flights, hotel rooms, and taxis.

## P.S. Financial fraud on underground markets

Apart from general statistics, it is worth bearing in mind that there are communities where financial malware source codes are for sale, and new ideas emerge on enhancing outdated malicious software. Nowadays, each community can find almost everything for their dark business, from hacking tutorials and schemes for earning money, to various ransomware and malware for getting important information. The priority, however, is users and their data, which are turned into goods, ready for purchasing. We are constantly investigating underground markets to gain a better understanding of their structure, the nature of selling goods, and the intentions of the people who are constantly committing cybercrimes.

In this section, we highlight the problem and the scale of possible threats.

The world of hacking tools can be best described as a huge highly structured international marketplace, with a large amount of different shops, sellers and amateur vendors from all over the world. They offer a wide range of goods for all tastes - for those trying to make the most profit, as well as those potential buyers who are seeking premium items at the cheapest prices. Prices fluctuate according to demand (prices rise when demand is high and fall when it is low). And the dark markets' stores are expanding [?] and growing in complexity year on year. Their geography is spreading out, their vendors are becoming more powerful, highly organized and sophisticated, and their goods becoming more reliable and long lasting.

In percentage terms, the map of the dark market stores can be best presented in the form of a pie chart, representing the share of each country in the market world.

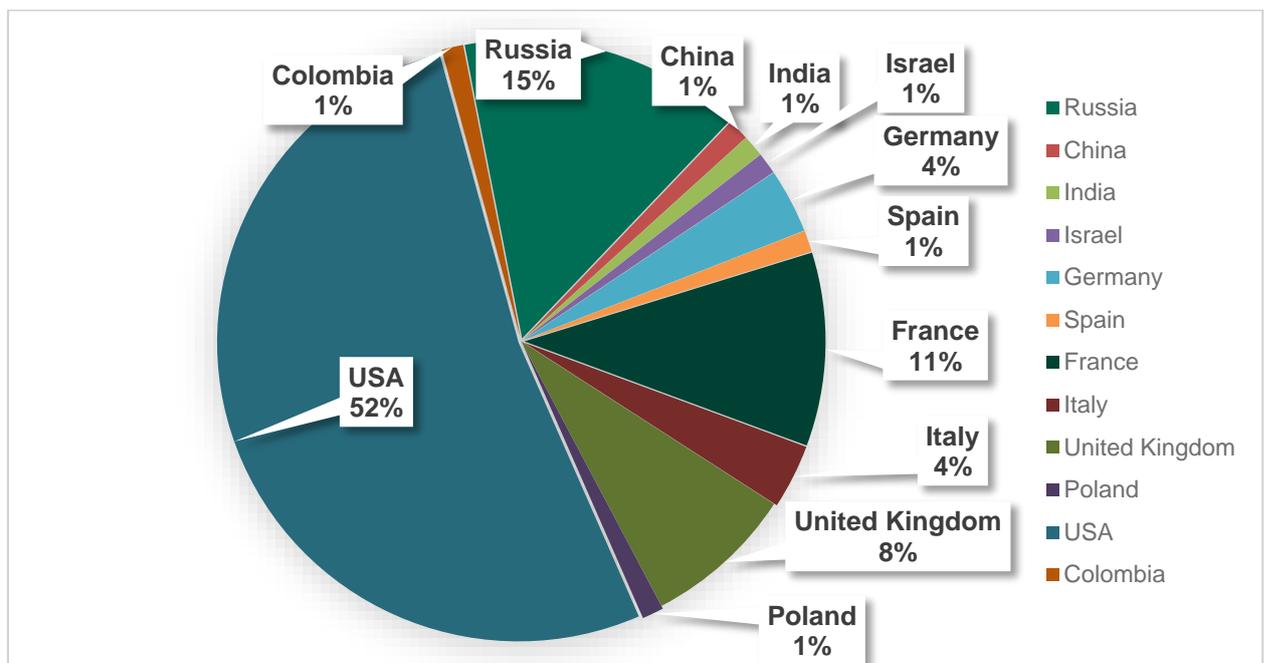


Fig. 35: Share of countries in the dark market world

It is plain to see that the United States took the leading position with half (52%) of all the

shops in dark market. America is followed by the Russian (15%) and French (11%) top markets. The share of other countries' markets is negligible [?], the United Kingdom (with its seven markets) and Italy (with its three markets) are still placed firmly in the dark segment, providing a few shops of high quality.

The offers on the markets can be divided into three vast categories, such as:

- fraud - including different types of personal information (accounts and ID) and on-going fraudulent schemes;
- software - containing offers of various malware;
- services - providing products for better and active social life (from traffic to spam) and malicious installs and loads for the contamination of victim devices.

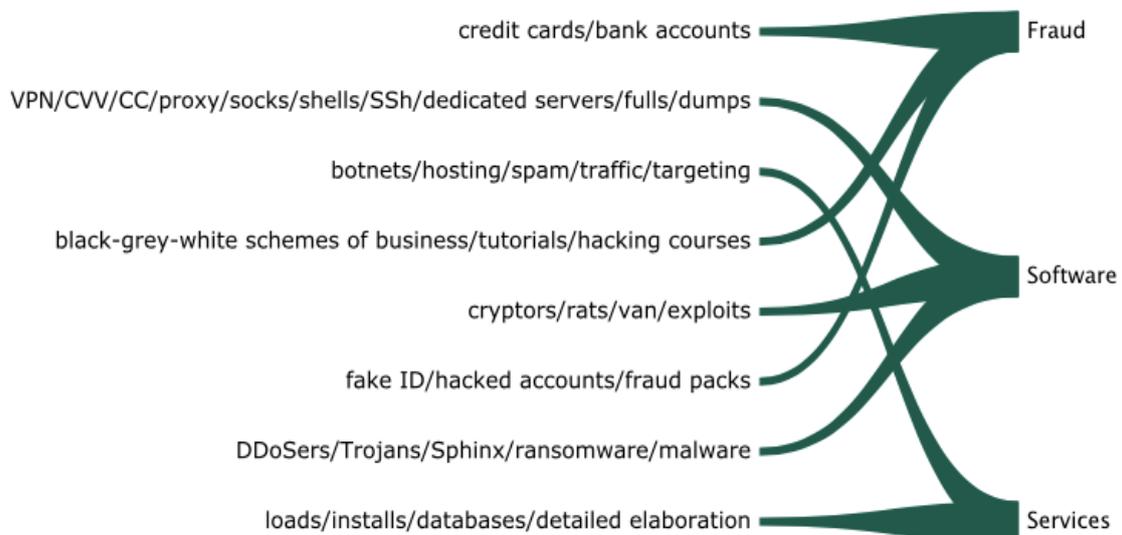


Fig. 36: The offers on the Darkmarkets

Within this paper, we will focus on the first and the second categories.

# Fraud

To start, we have decided to take a look at the prices of different sorts of fraud items, which are in abundance. The vast majority comprises online accounts of social networks and entertaining apps for any taste. The most abundant and, as a result, most popular, goods of any underground market are credit cards and bank accounts.

### BUY BANK LOGIN FROM HACKERS



**4318 USD** Digital

BUY BANK LOGIN FROM HACKERS - About Bank Login for sale We sell freshly spammed account and hacked bank login mostly any UK , EU and USA bank. If you need bank login, you write us and

Fig. 37: The offers on the dark markets

The most comprehensive list of bank accounts includes vendors from Russian markets. They can offer cards of different values for practically every leading bank in the world. For example, Russian Anonymous Marketplace buyers have the opportunity to choose from Russian, Ukrainian, English, American, and Canadian banks.

Other markets can even offer rare bank accounts from Europe and the UK, which are more valuable because of the following reasons:

- they often have a higher credit limit;
- they tend to be more secure (because of their PIN with signature system) than, for example, U.S. accounts;
- typically, there is a delay while processing a card in a foreign bank, so much more can be charged while the bank figures out the fraud.

Finally, to earn huge amounts of money, it's possible to check the shareware tutorials or proven black-market schemes of earning on the internet (from free of charge advice about how to cheat in E-bay, to cracking AliExpress accounts and qualified business tutorials with good income guaranteed). The prices of these items range from \$50 USD to over \$100 USD, depending on the plan's complexity and value of the monthly income.

## Malware

Open forums typically offer botnets, malware cryptors (created to defend malware against antivirus/anti-malware products), proxy, SOCKS (Socket Secure protocols that exchanges network packets between a client and a server through a proxy server), RATs, loads and installs, and also dedicated servers, including VDS (Virtual Dedicated Server), VPS (Virtual Private Server) and VNC (Virtual Network Computing - for the remote control of another computer).

Otherwise, professional black markets can provide powerful variations of worldwide famous malware. For example, '0day.su' sells DiamondFox (also known as Gorynych Botnet - a multipurpose botnet with capabilities ranging from credential stealing to the theft of credit card information from point of sale systems) for \$700. Meanwhile, Sphinx Trojan (high-powered banking malware based on the source code of the infamous Zeus banking Trojan) is available for \$800. T.chka offers Wincor ATM Malware (well-known malware that helps intruders to withdraw ATMs of their cash via "jackpotting" attacks with ease) for \$3975, GoldenEye Ransomware (a combination of Petya and MISCHA ransomware-types, which is distributed using a spam email message) for \$795, and Galileo (best hacking software that can spy the devices running on iOS, Android, Windows Mobile, BlackBerry, as well as Mac and Windows PC) for \$1760.

<p><b>CUTLET MAKER ATM CASHOUT MALWARE</b> <span>5 / 5</span></p>  <p><b>300 - 700 USD</b> <span>Digital</span></p> <p>I WILL SEND BAR PASS AFTER RELEASE OF COINS TO PREVENT SPREADING MALWARE AND SCAMS. These are 3 programs (Stimulator, Cutlet Maker, o0decalc and keygen) PROOF: Stimulator - Checking the</p>	<p><b>Selling Dumps Track with Pin ATM SKIMMER and MRS Machine for Cashout</b></p>  <p><b>700 - 1200 USD</b> <span>Mail</span></p> <p>Selling Dumps Track with Pin ATM SKIMMER and MRS Machine for Cashout _Wincor with keypad 700usd _Machine ATM Skimmer Wincor Nixdorf : 1200\$ Machine ATM Skimmer Wincor : 1200\$ Sell</p>
---	---

*Fig. 38: The offers on the dark markets*

The fact that offers exist for such prices points to the existence of demand for such goods: people are ready to spend huge amounts of money on fraud and cyber services.

Regarding bank accounts, the most widespread are from the US and Russia, as they have a lower rate of security than European or UK accounts, so they are much more easily hacked and put on the market. The minimum price on US bank accounts varies between \$13 and \$150. For Russian Credit Cards, it is from \$60 to \$400. The top border is shadowy, depending on a user's credit limit.

The UK and European accounts are less common and introduced only into a few markets from the reviewed list. Their lowest prices could be even less than those of the USA or Russian exemplars, still such accounts are unique offers due to their high limit and security, compared to the other samples offered.

Within hacking services, sophisticated vendors try to do their best, providing intruders with worldwide famous malware that has made a whole stink, and stolen good money. The big play costs big money, so to try DiamondFox or Sphinx Trojan, one must be prepared to pay at least \$700; but malware with renowned titles will cost not less than \$2000. The prices have been going up and the deals are risky, but the rewards are also great.

Thus, the ability to attack seems to outpace the ability to defend. Cybercriminals are likely to be in a better position since their aim is to know a single method of attack and to do it perfectly. Ordinary defenders, on the contrary, must know everything and be one-step ahead to prevent a disaster.

# Conclusion and advice

2017 showed that we all should stay vigilant. While the financial industry is working hard to make financial transactions online more secure, criminals are starting to exploit accessibility services. While the old malware families are resting in peace, their source code has been laid into the foundations of new families with devastating consequences.

Criminals 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 still get financial gain out of their activities.

As the above threat data shows, 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

- Don't click on suspicious links. They are mostly designed to download malware onto your device or lead you to phishing webpages, which intend to harvest your credentials.
- Never open or store unfamiliar files on your device as they could be malicious.
- Always stay vigilant when using public Wi-Fi networks as they can be insecure and unreliable, making hotspots a prime target for hackers to steal user information. To keep your confidential information safe, never use hotspots to make online payments or share financial information.
- Websites can be a front for cybercriminals, with the sole purpose of harvesting your data. To stop your confidential details from 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 compromising your credentials through a mobile banking application, make sure you use the official app for your financial services, and ensure it is not compromised. Download apps only from trusted sources and official application stores, and keep your apps updated.
- 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 have no boundaries, so your security needs to be just as widespread to minimize the risk of 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.
- If you use cloud email services, make sure you have installed a dedicated protection for your email – such as Kaspersky Security for Microsoft Office 365 – to strengthen your protection against business email compromise.
- Ensure all levels of your corporate infrastructure are protected, from core data centers to specialized systems in the case of banking infrastructure (such as ATMs), and leverage advanced detection and response technologies, which make it possible to catch even unknown banking malware.
- Use proven security solutions, equipped with behavioral based protection technologies, which make it possible to catch even unknown banking malware.
- To stay up-to-date and feed your SOC with info, subscribe to expert services: malware phishing data feeds and APT and financial reporting services.