kaspersky

Financial Cyberthreats in 2019

16.04.2020

Methodology

Financial cyberthreats are malicious programs that target users of services such as online banking, e-money, and cryptocurrency, or that attempt to gain access to financial organizations and their infrastructure. These threats are usually accompanied by spam and phishing activities, with malicious users creating fake financial-themed pages and emails to steal victims' credentials.

In order to study the threat landscape of the financial sector, our researchers analyzed malicious activity on the devices of individual users of Kaspersky's security solutions. Statistics for corporate users were collected from corporate security solutions, after the customers agreed to share their data with Kaspersky.

Introduction and key findings

In 2019, we witnessed a number of significant changes in the cyberthreat landscape. Cybercriminals started to lose interest in malicious cryptocurrency mining and turned their attention to the broader topic of digital trust and privacy issues.

How did all those changes affect financial security around the world? As our report for the first half of 2019 demonstrated, there is no room for complacency – cyberthreats that aim to steal money are still out there.

Although the financial industry did not witness any major cases in 2019, the statistics show that particular categories of users and businesses are still being targeted by criminals. We have prepared this report to provide a more detailed picture of the situation.

This publication continues our series of Kaspersky reports (see here, here, and here) providing 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.

Phishing:

In 2019, the share of financial phishing increased from 44.7% of all phishing detections to 51.4%.

Almost every third attempt to visit a phishing page blocked by Kaspersky products is related to banking phishing (27% share).

The share of phishing-related attacks on payment systems and online stores accounted for almost 17% and over 7.5% respectively in 2019. This is more or less the same as 2018 levels.

The share of financial phishing encountered by Mac users fell slightly from 57.6%, accounting for 54%.

Banking malware (Windows):

In 2019, the number of users attacked with banking Trojans was 773,943 – a decrease compared to the 889,452 attacked in 2018.

1% of users attacked with banking malware were corporate users – an increase from 24.1% in 2018.

Users in Russia, Germany, and China were attacked most frequently by banking malware.

Just four banking malware (ZBot, RTM, Emotet, CliptoShuffler) families accounted for attacks on the vast majority of users (around 87%).

Android banking malware:

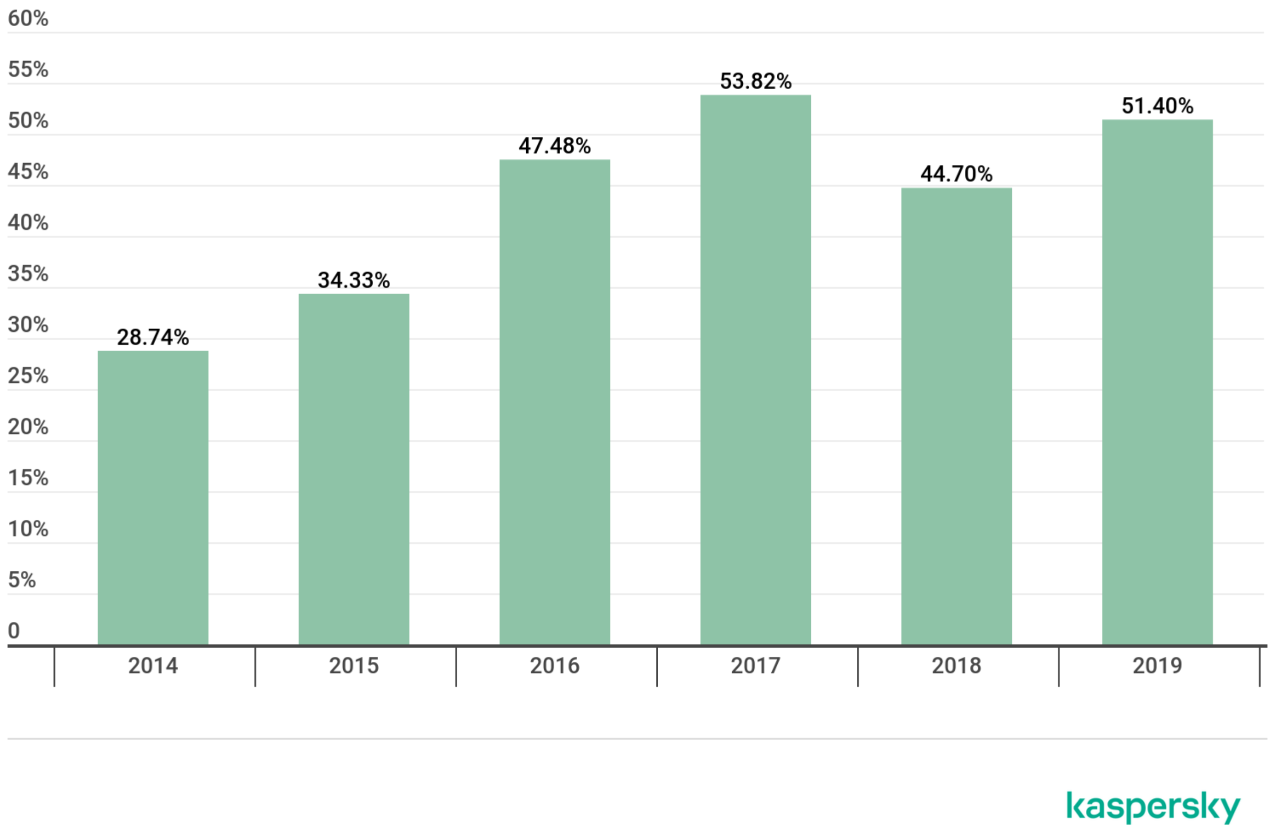
In 2019, the number of users that encountered Android banking malware dropped to just over 675,000 from around 1.8 million.

Russia, South Africa, and Australia were the countries with the highest percentage of users attacked by Android banking malware.

Financial phishing

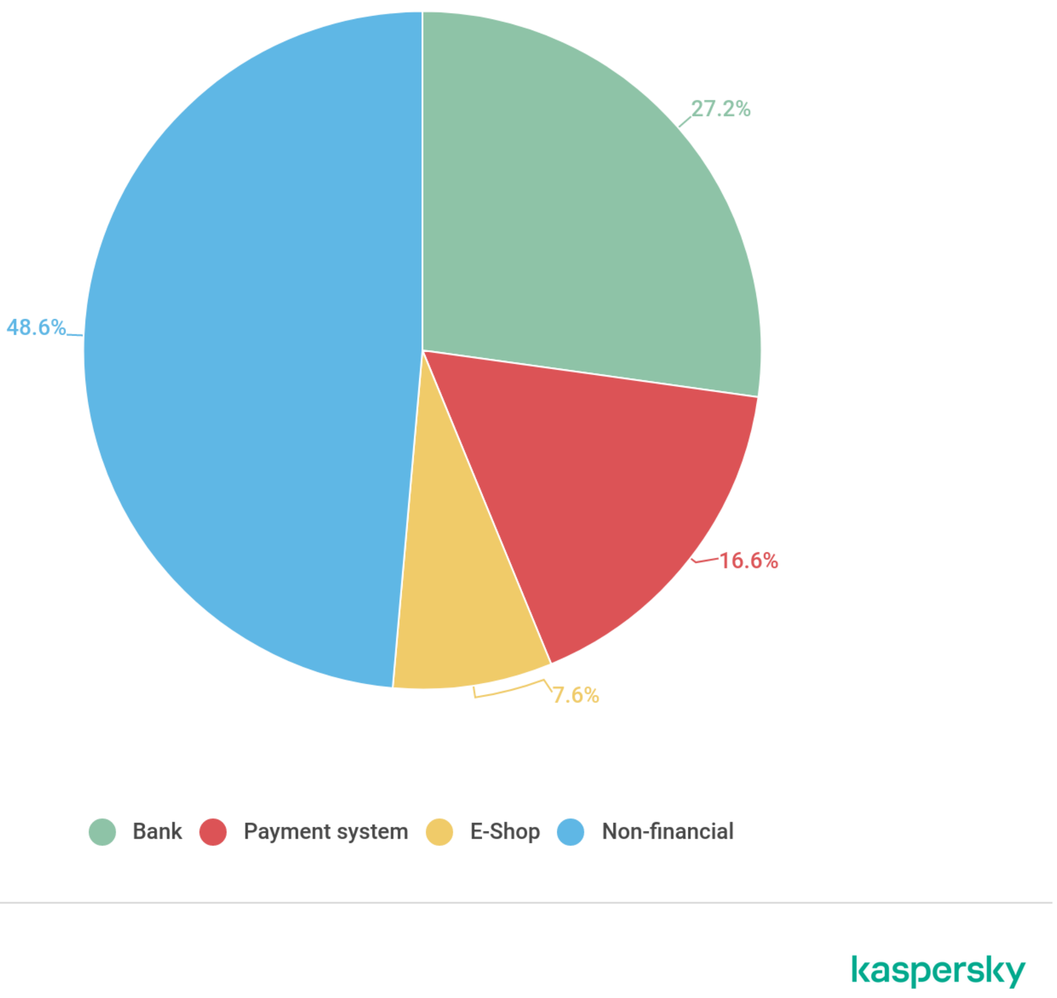
Financial phishing is one of the most popular ways for criminals to make money. It doesn't require a lot of investment but if the criminals get the victim's credentials, they can either be used to steal money or sold.

As our telemetry systems show, this type of activity has accounted for around half of all phishing attacks on Windows users in recent years.



The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky, 2014-2019 (download)

In 2019, the overall number of phishing detections stood at 467,188,119. 51.4% of those were finance-related attacks. That is the second-highest share ever registered by Kaspersky; the highest proportion of financial phishing was 53.8% in 2017.



The distribution of different types of financial phishing detected by Kaspersky in 2019 (download)

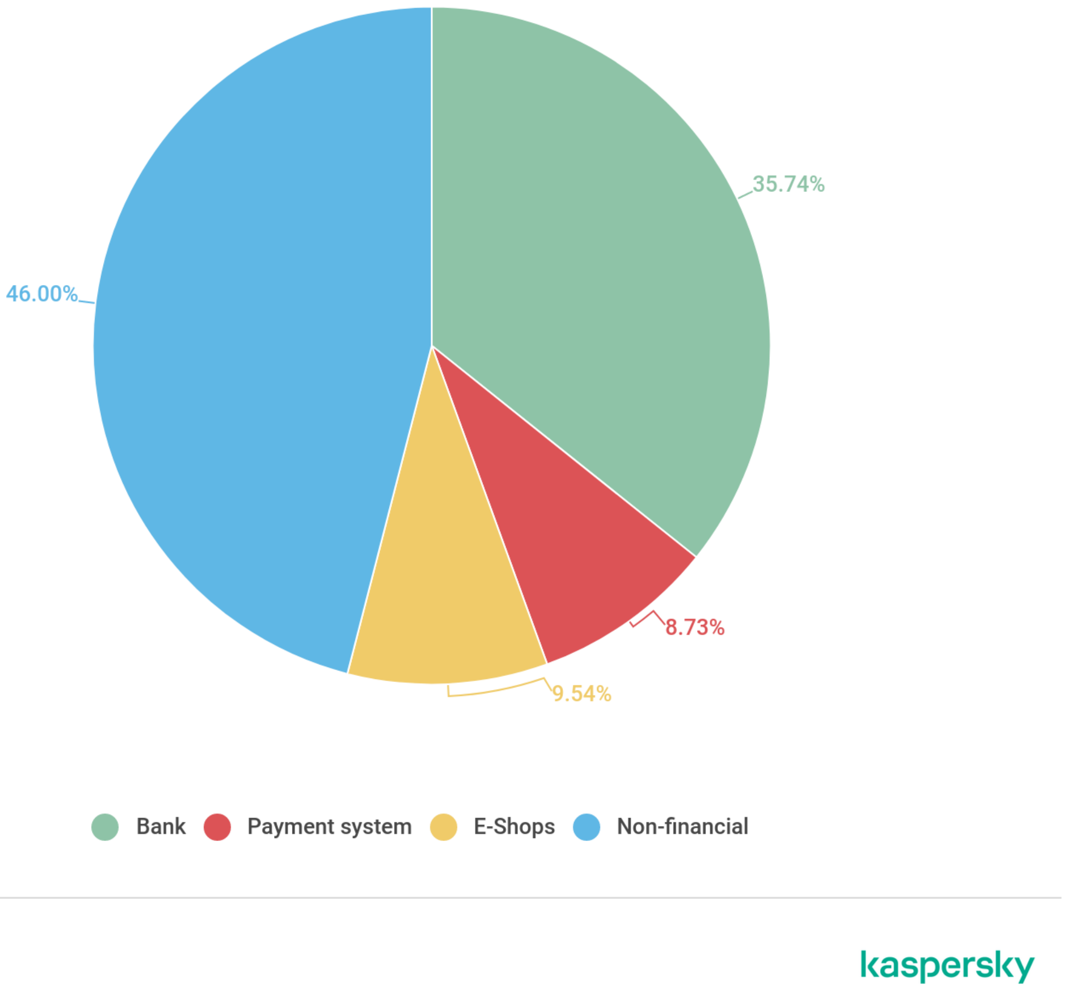
Compared to the previous year, bank-related phishing grew from a share of 21.7% to almost 30% in 2019. The other two main finance categories remained more or less at the same level.

Financial phishing on Mac

As is now customary, we also compare the above statistics with those for MacOS: while the latter has traditionally been considered a relatively secure platform when it comes to cybersecurity, nobody knows where the latest threats may strike. Moreover, phishing is an OS-agnostic activity – it is all about social engineering.

In 2018, 57.6% of phishing attacks against Mac users attempted to steal financial data. A third of those were bank-related attacks. In 2019, the overall level was slightly less – just over 54%.

In 2019, the breakdown of categories was as follows:



The distribution of different types of financial phishing detected by Kaspersky on Macs in 2019 (download)

The share of bank phishing actually grew by around 6% compared to 2018. At the same, the E-shop category's share dropped from around 18% to around 8%. The Payment systems category remained more or less unchanged. Overall, our data shows that the financial share of phishing attacks on Macs is also quite substantial – like that for Windows. Let's take a closer look at both categories.

Mac vs Windows

In 2017, we discovered an interesting twist when Apple became the most frequently used brand name in the online shopping category both in the MacOS and Windows statistics, pushing Amazon down to second place for the latter platform. Even more interesting is that in 2018 Apple maintained its position in the Windows statistics, but Amazon led the MacOS statistics for the first time since we started tracking this activity. In 2019, the situation was as follows:

	Mac	Windows
1	Apple	Apple
2	Amazon.com: Online Shopping	Amazon.com: Online Shopping
3	eBay	eBay
4	groupon	Steam
5	Steam	Americanas
6	ASOS	groupon
7	Americanas	MercadoLibre
8	Shopify	Alibaba Group
9	Alibaba Group	Allegro

The most frequently used brands in the E-shop category of financial phishing activity, 2019

What is most interesting in the table above is that the top three places appear to be OS agnostic and are the same for both Mac and Windows.

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

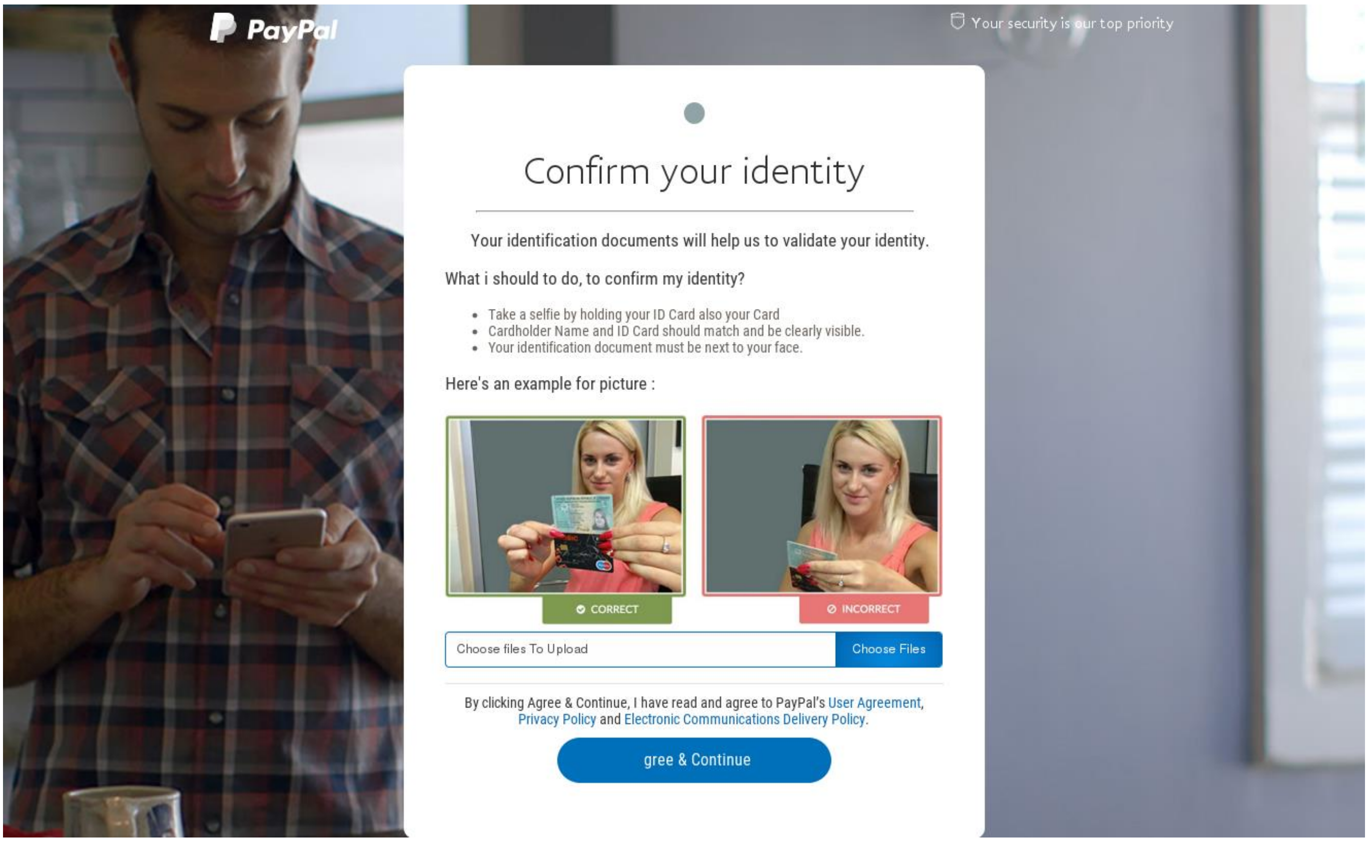
	Mac	Windows
1	PayPal	Visa Inc.
2	MasterCard International	PayPal
3	American Express	MasterCard International
4	Visa Inc.	American Express
5	Authorize.Net	Cielo S.A.
6	Stripe	Stripe
7	Cielo S.A.	Authorize.Net
8	adyen payment system	adyen payment system
9	Neteller	Alipay

The most frequently used brands in the Payment systems category of financial phishing activity, 2019

The data above can be viewed as a warning to users of the corresponding systems: they illustrate to what extent malicious users exploit these well-known names to fraudulently obtain payment card details as well as online banking and payment system credentials.

Phishing campaign themes

The list of 2019 phishing campaigns covered below includes the usual suspects: fake versions of online banking and payment systems or web pages mimicking internet stores.



Confirm your identity

Your identification documents will help us to validate your identity.

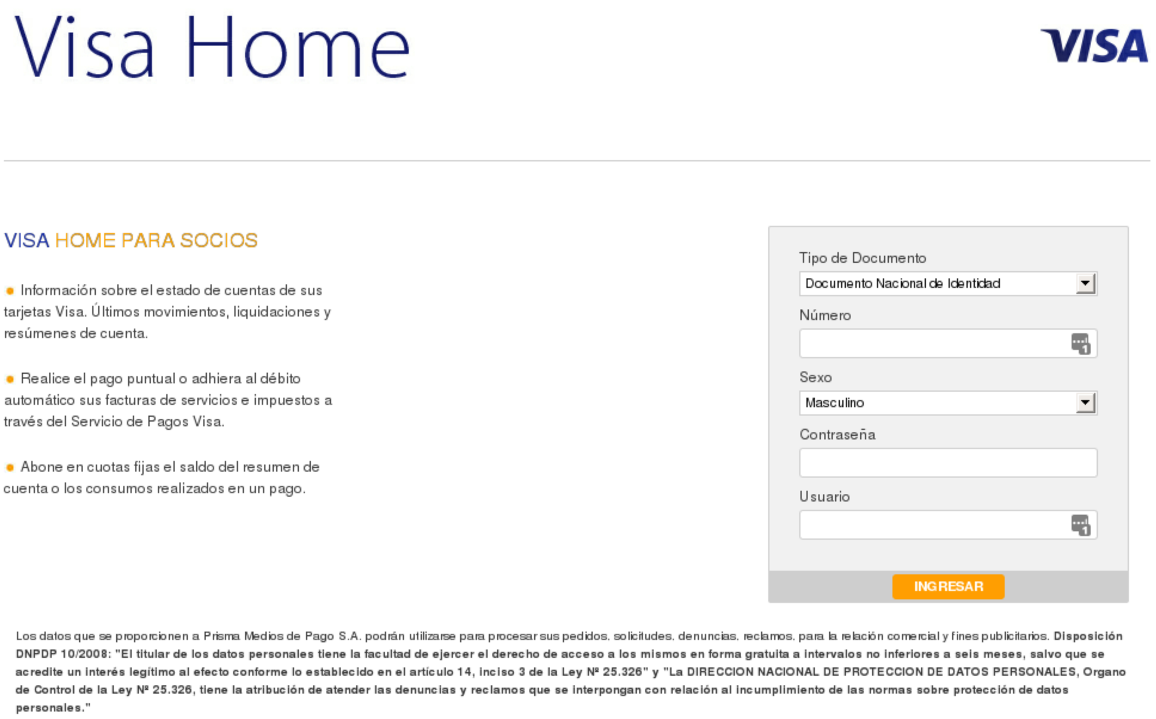
What i should to do, to confirm my identity?

- Take a selfie by holding your ID Card also your Card
- Cardholder Name and ID Card should match and be clearly visible.
- Your identification document must be next to your face.

Here's an example for picture :

By clicking Agree & Continue, I have read and agree to PayPal's User Agreement, Privacy Policy and Electronic Communications Delivery Policy.

A phishing page masquerading as a payment service



Visa Home

VISA HOME PARA SOCIOS

- Información sobre el estado de cuentas de sus tarjetas Visa. Últimos movimientos, liquidaciones y resúmenes de cuenta.
- Realice el pago puntual o adhiera al débito automático sus facturas de servicios e impuestos a través del Servicio de Pagos Visa.
- Abone en cuotas fijas el saldo del resumen de cuenta o los consumos realizados en un pago.

Tipo de Documento

Documento Nacional de Identidad

Número

Sexo

Masculino

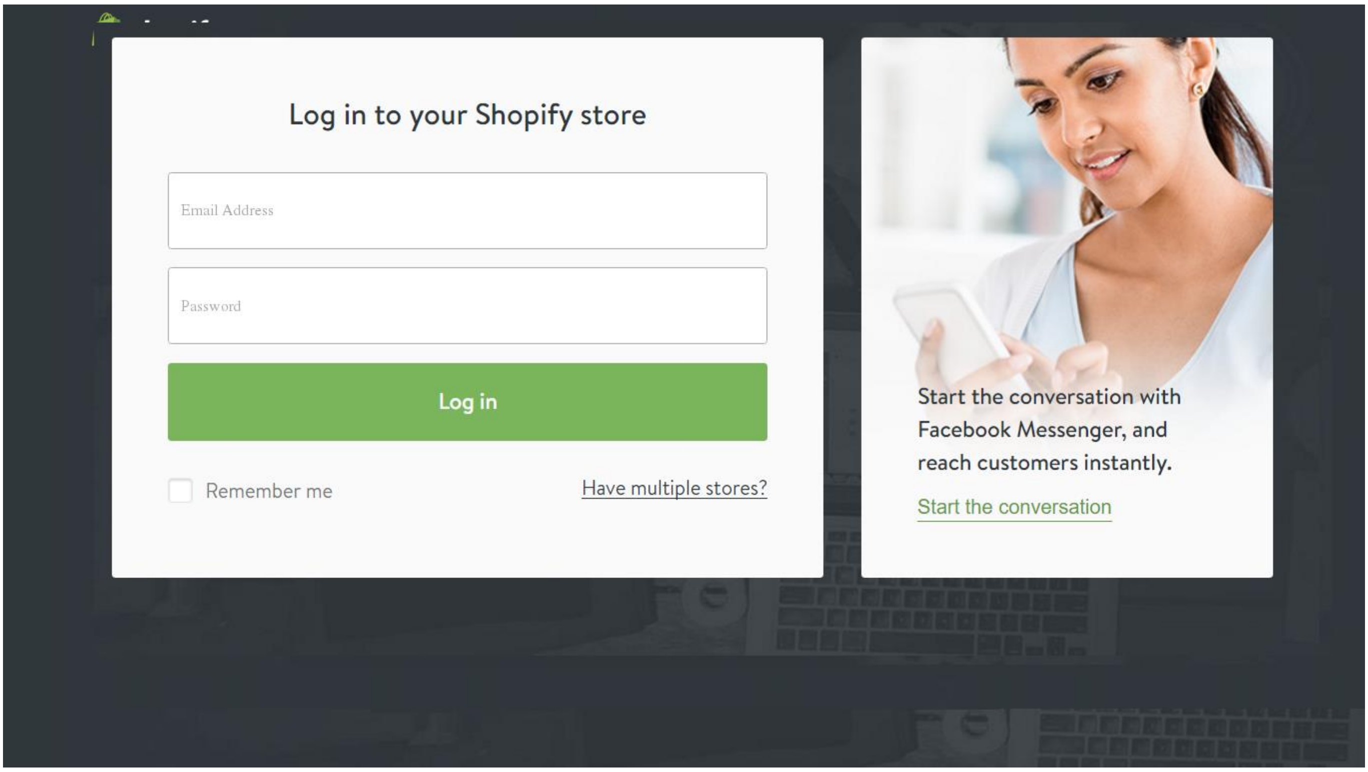
Contraseña

Usuario

INGRESAR

Los datos que se proporcionen a Prisma Medios de Pago S.A. podrán utilizarse para procesar sus pedidos, solicitudes, denuncias, reclamos, para la relación comercial y fines publicitarios. **Disposición DNPDP 10/2008: "El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 de la Ley Nº 25.326" y "La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Organo de Control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales."**

Phishing pages masquerading as payment service pages



Log in to your Shopify store

Email Address

Password

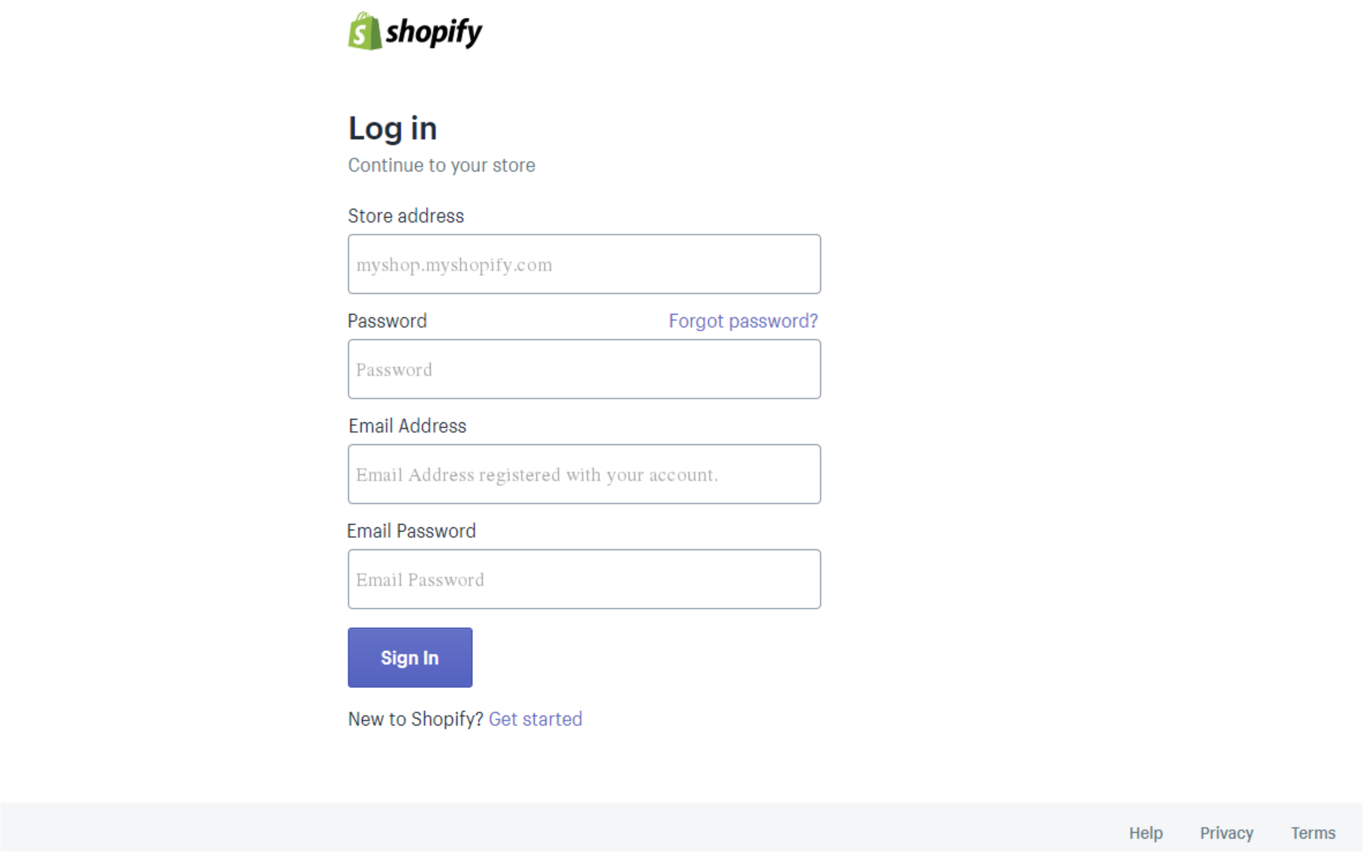
Log in

□ Remember me

Have multiple stores?

Start the conversation with Facebook Messenger, and reach customers instantly.

Start the conversation



shopify

Log in

Continue to your store

Store address

myshop.myshopify.com

Password

Forgot password?

Password

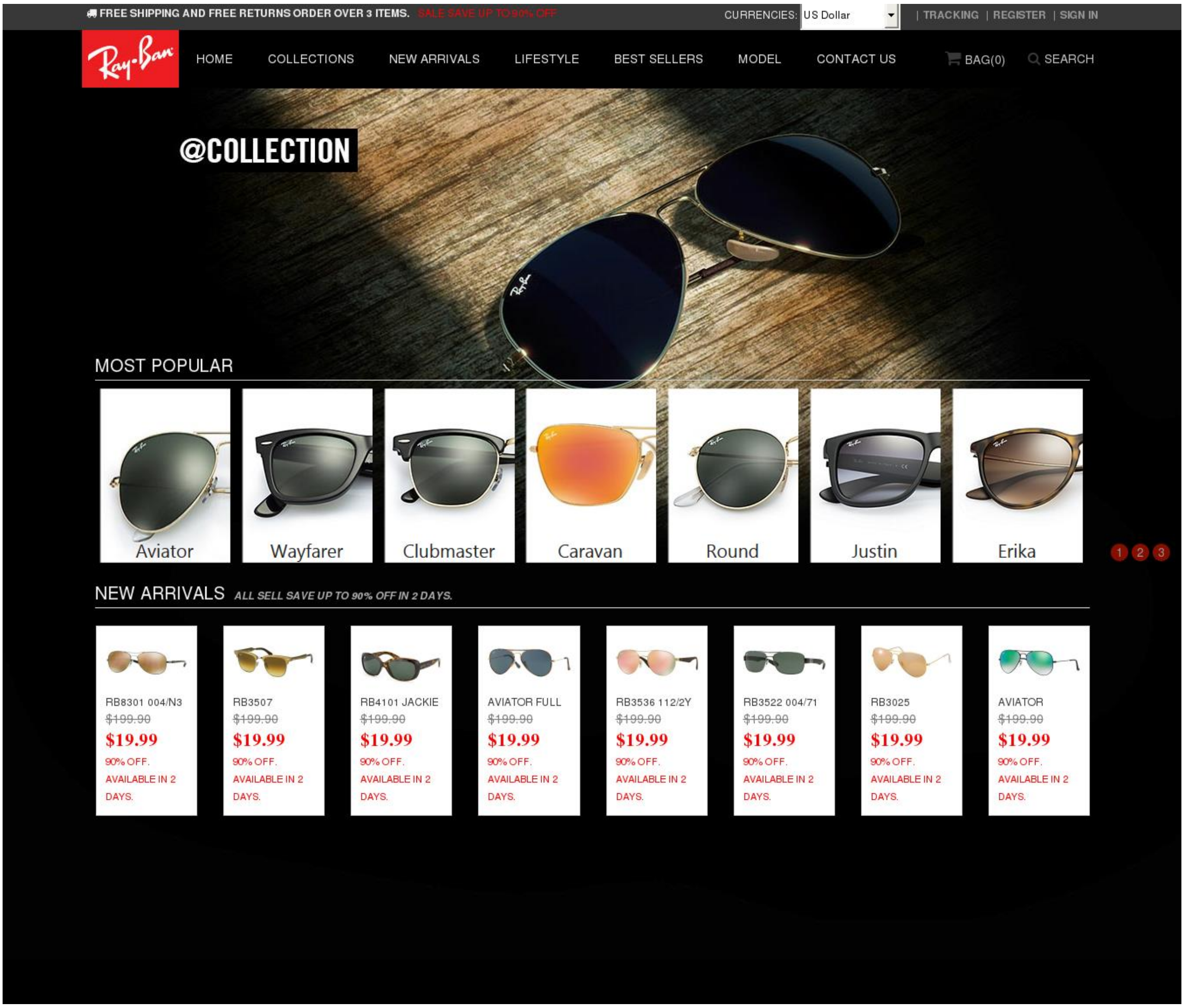
Email Address

Email Address registered with your account.

Email Password

Email Password

New to Shopify? Get started


FREE SHIPPING AND FREE RETURNS ORDER OVER 3 ITEMS. SALE SAVE UP TO 90% OFF
CURRENCIES: US Dollar
| TRACKING | REGISTER | SIGN IN
Ray-Ban
HOME
COLLECTIONS
NEW ARRIVALS
LIFESTYLE
BEST SELLERS
MODEL
CONTACT US
BAG(0)
SEARCH
@COLLECTION
MOST POPULAR
Aviator
Wayfarer
Clubmaster
Caravan
Round
Justin
Erika
1 2 3
NEW ARRIVALS ALL SELL SAVE UP TO 90% OFF IN 2 DAYS.
RB8301 004/N3 $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
RB3507 $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
RB4101 JACKIE $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
AVIATOR FULL $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
RB3536 112/2Y $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
RB3522 004/71 $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
RB3025 $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.
AVIATOR $199.90 $19.99 90% OFF. AVAILABLE IN 2 DAYS.

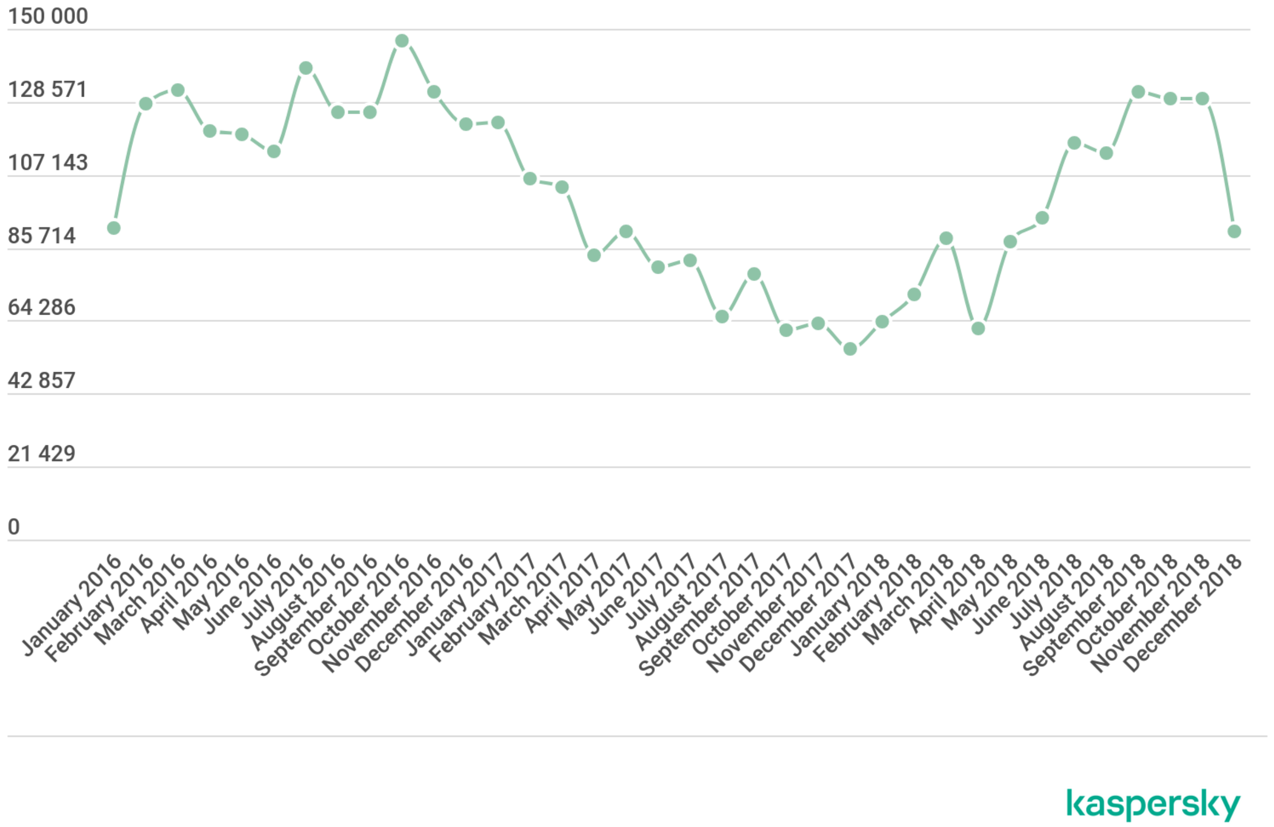
Phishing pages masquerading as an e-store pages

Of course, by clicking a link or entering credentials on pages like these, a user will not be accessing their account – they will be passing on important personal information to the fraudsters.

Some of the most common scams used to trick users include messages that refer to the hacking or blocking of an account or offers of incredible bargains.

Banking malware on PCs

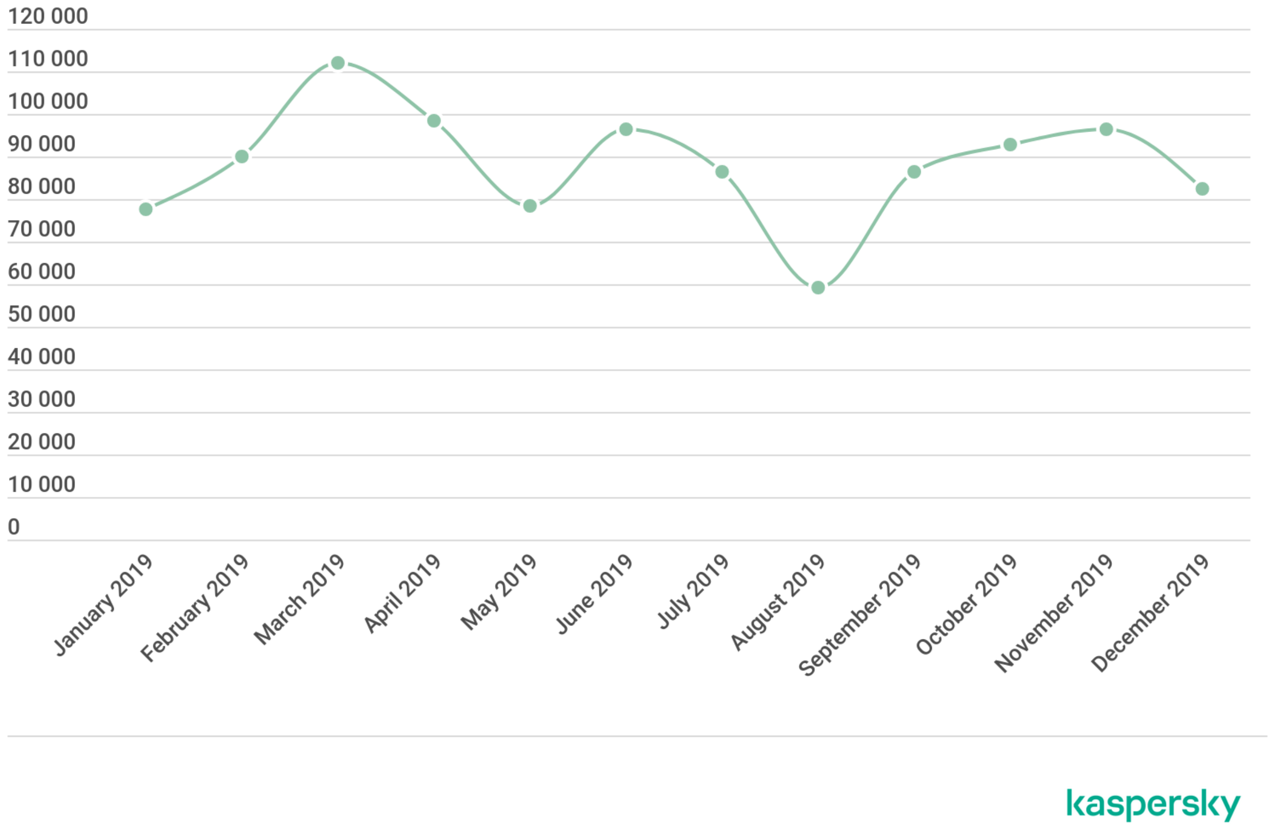
For clarity, when discussing financial malware in this paper we mean typical banking Trojans designed to steal the credentials used to access online banking or payment system accounts and to intercept one-time passwords. Kaspersky has been monitoring this particular type of malware for a number of years:



The number of users attacked with banking malware, 2016-2018 (download)

As we can see, throughout 2016 there was a steady growth in the number of users attacked with bankers – following downward trends in 2014 and 2015. 2017 and the first half of 2018 saw a return to a downward trend. The number of attacked users worldwide fell from 1,088,933 in 2016 to 767,072 in 2017 – a decline of almost 30%.

Below are the figures for 2019.

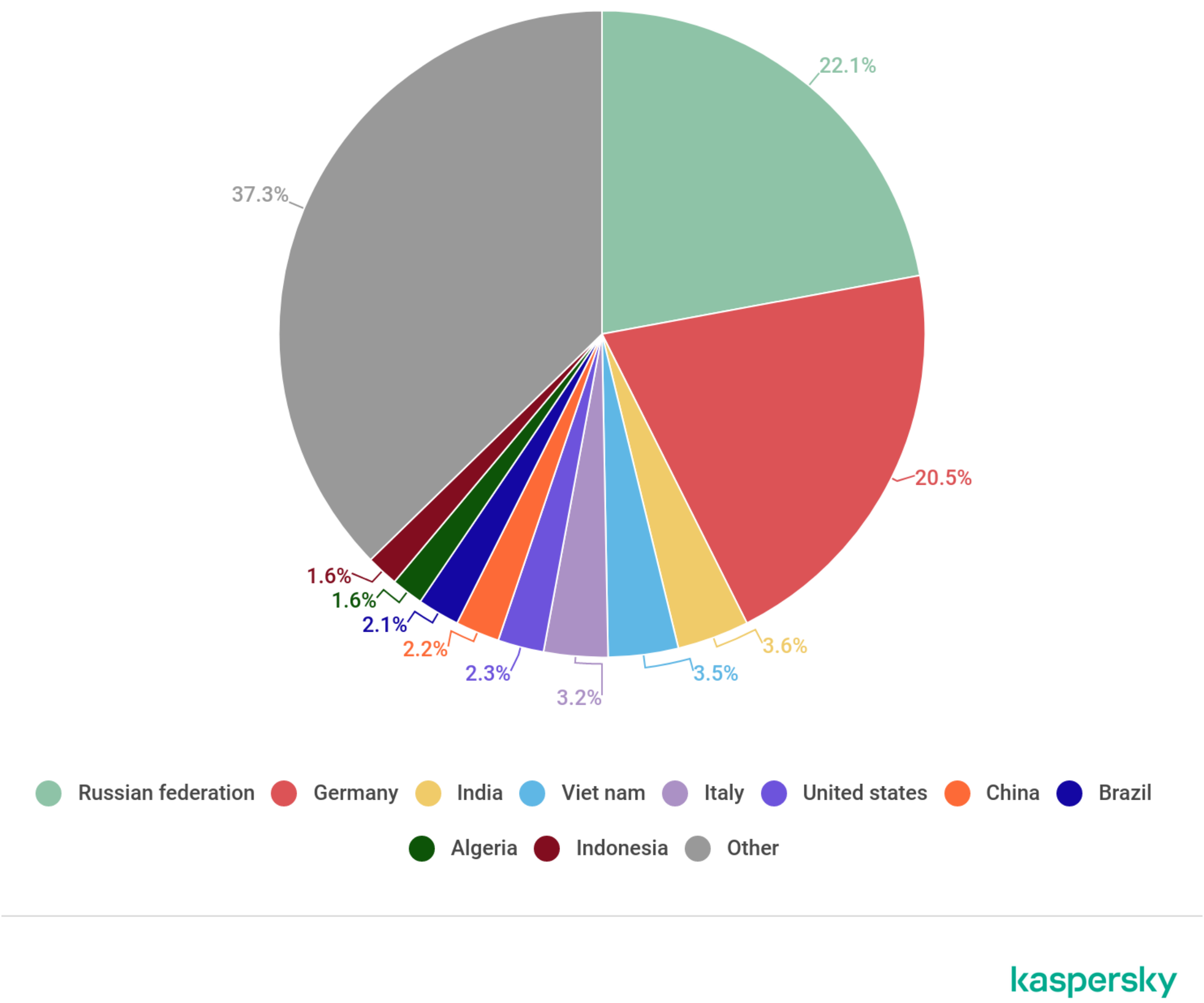


The number of users attacked with banking malware 2019 (download)

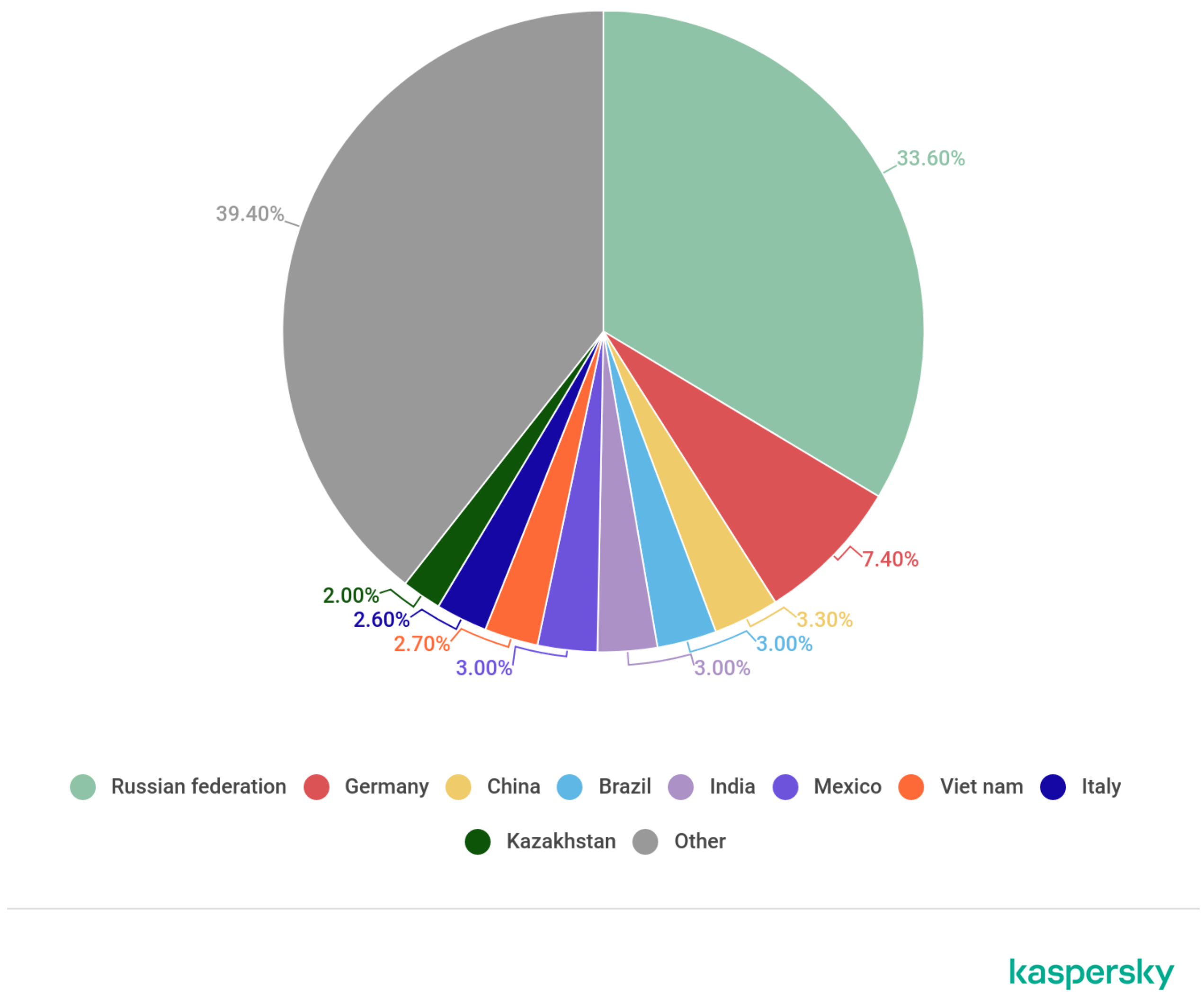
In 2019, the number of users attacked with banking Trojans stood at 773,943 – a slight decrease compared to 889,452 in 2018.

The geography of attacked users

As shown in the charts below, more than half of all users attacked with banking malware in 2018 and 2019 were located in just 10 countries.



***The geographic distribution of users attacked with banking malware in 2018** (download)*

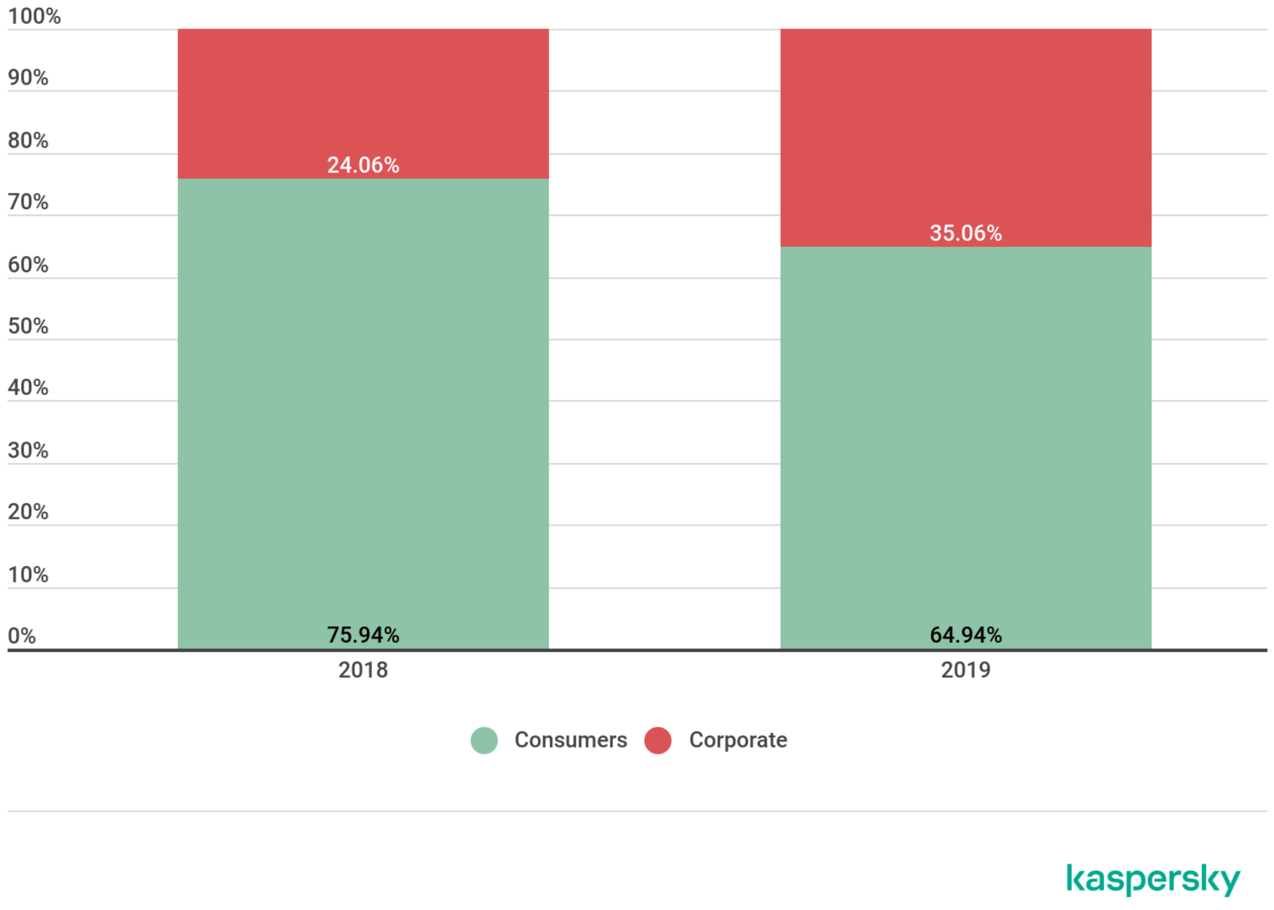


The geographic distribution of users attacked with banking malware in 2019 (download)

In 2019, Russia’s share increased and accounted for over one-third of attacks. Germany remained in second place, while China ended the year in third place.

The type of users attacked

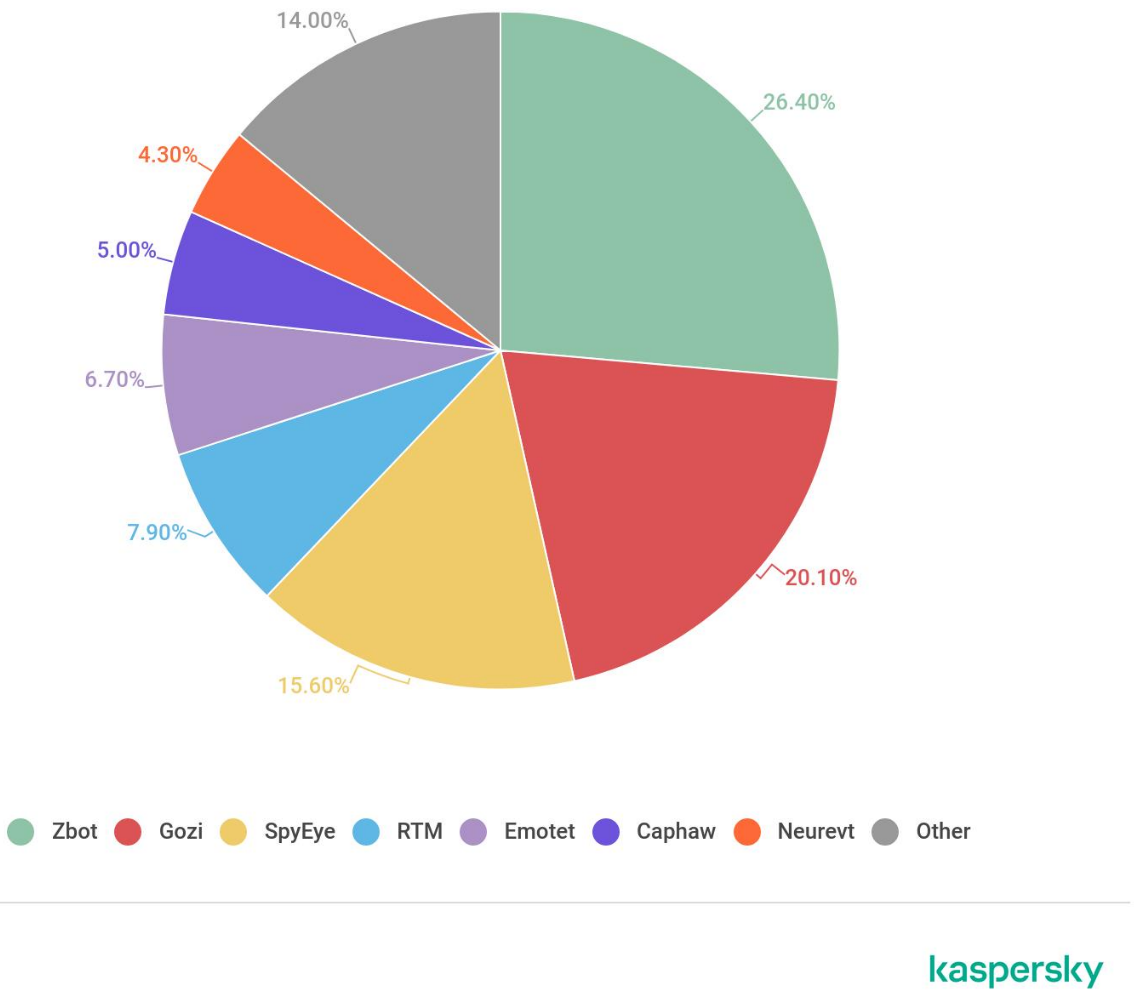
It is also interesting to look at the consumer/corporate split in victimology.



The distribution of attacked users by type in 2018-2019 (download)

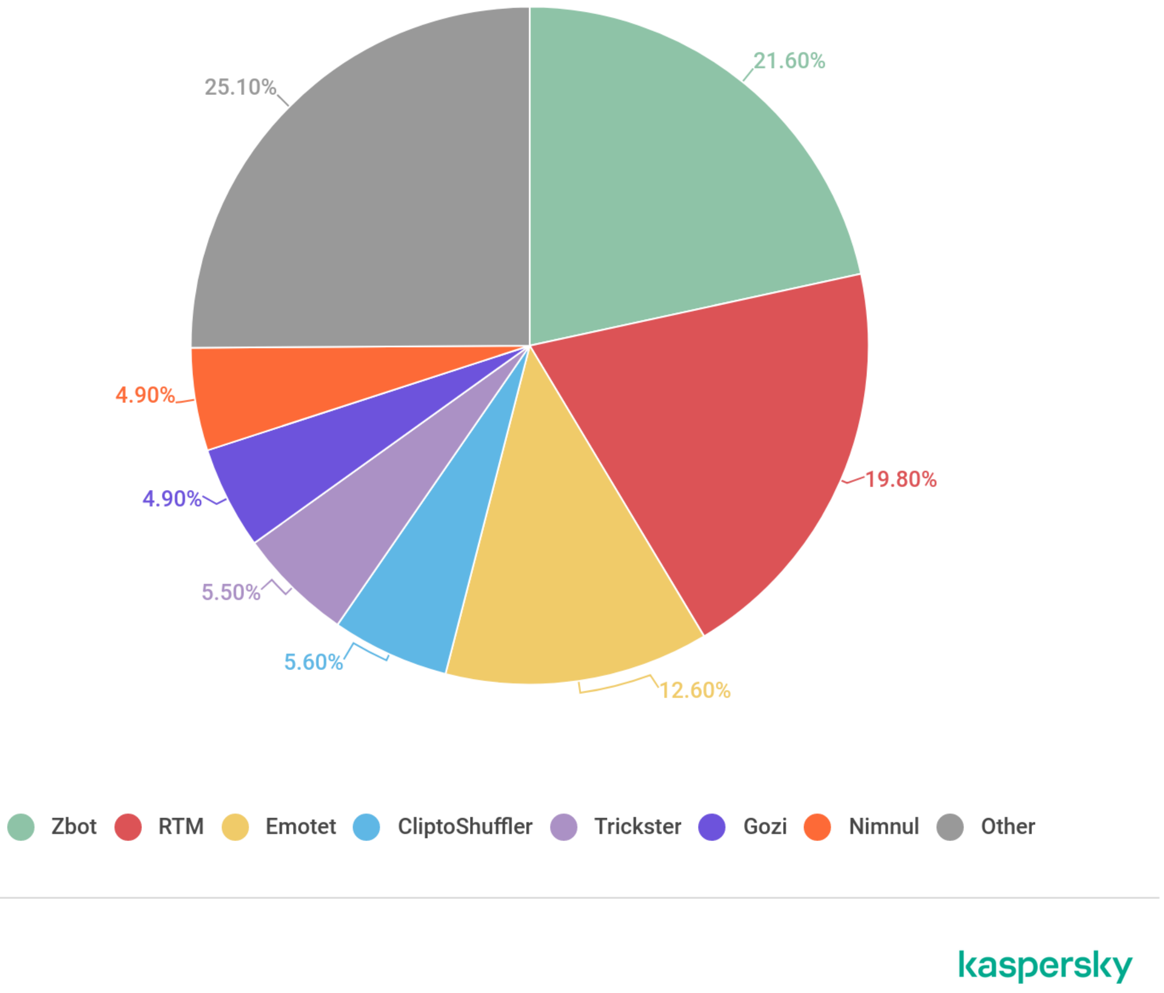
The main actors and developments

For years, the banking malware landscape has been dominated by several major players.



The distribution of the most widespread banking malware families in 2018 (download)

In 2018, we saw the major players decreasing their attacks – Zbot fell to 26.4% and Gozi to a little over 20%. 2019 produced the following situation.

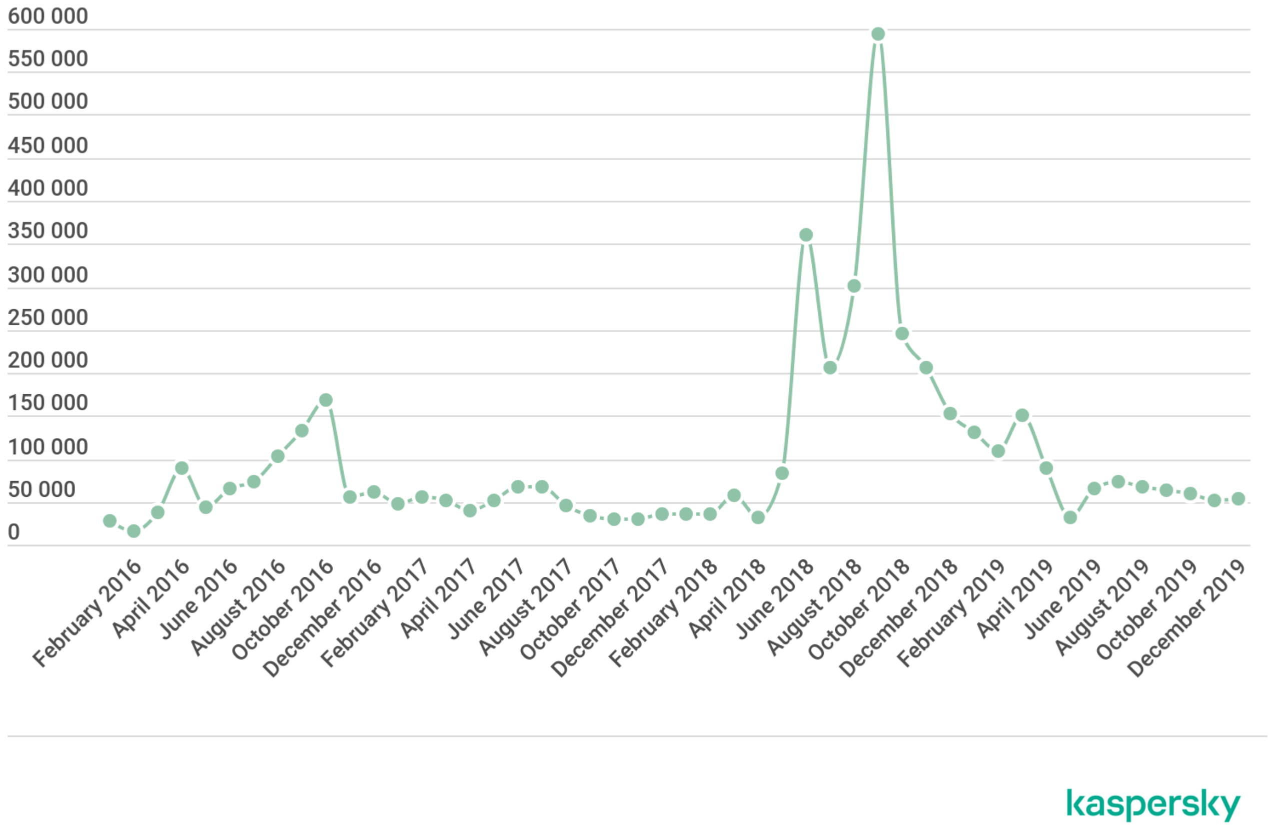


The distribution of the most widespread banking malware families in 2019 (download)

Zbot is still the most widespread malware, while second and the third places are occupied by RTM and Emotet. Gozi dropped out of the top three, ending the year in sixth place.

Mobile banking malware

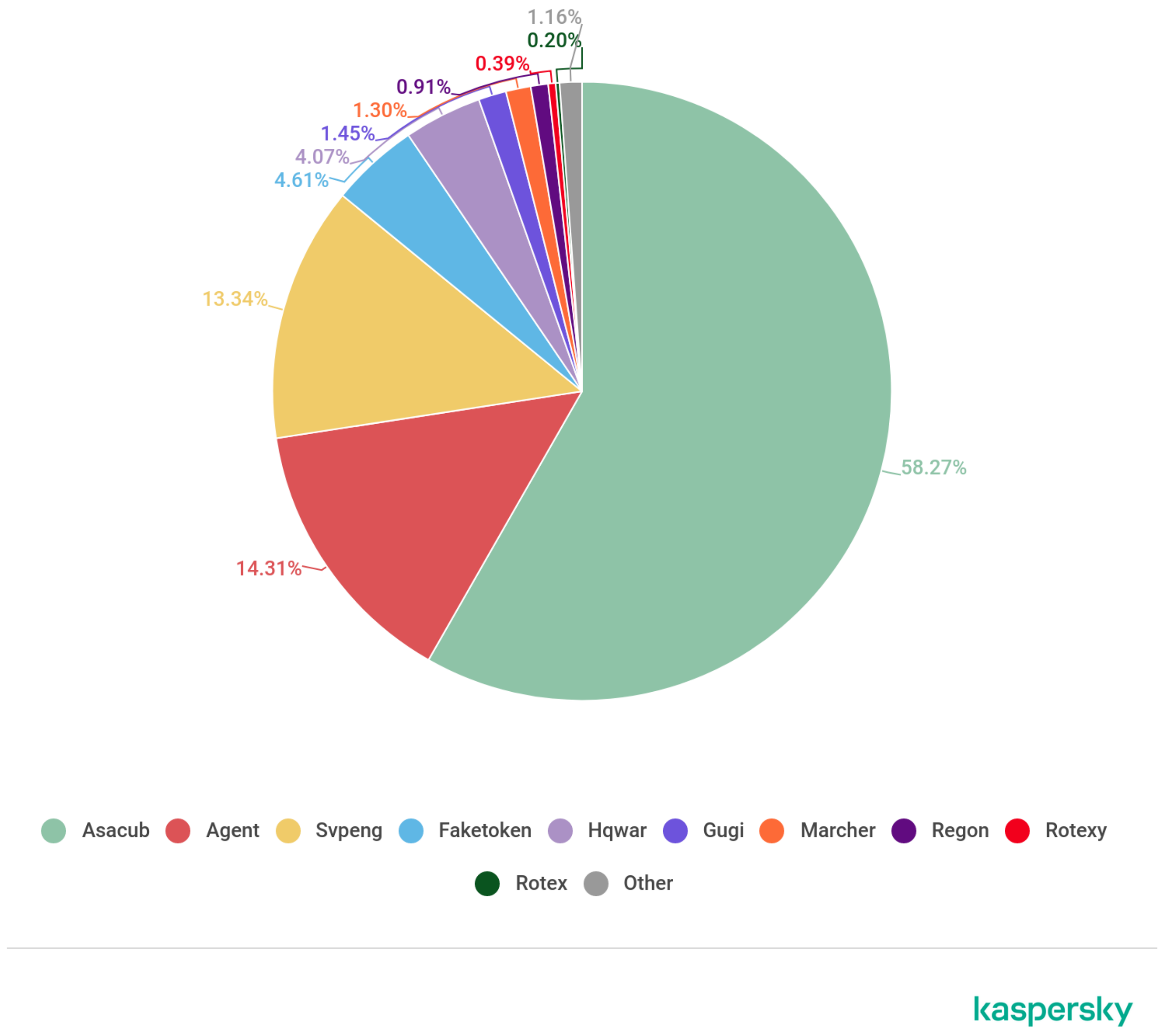
In 2018, we reviewed the methodology behind the mobile section of this report. We had previously analyzed Android banking malware statistics using KSN data sent by the Kaspersky Internet Security for Android solution. But as Kaspersky developed new mobile security solutions and technologies, the statistics gathered from one product alone became less relevant. That is why we decided to shift to expanded data, gathered from multiple mobile solutions. The data for 2016 and 2017 in this report was recalculated using the new methodology.



The change in the number of users attacked with Android banking malware, 2016-2019 (download)

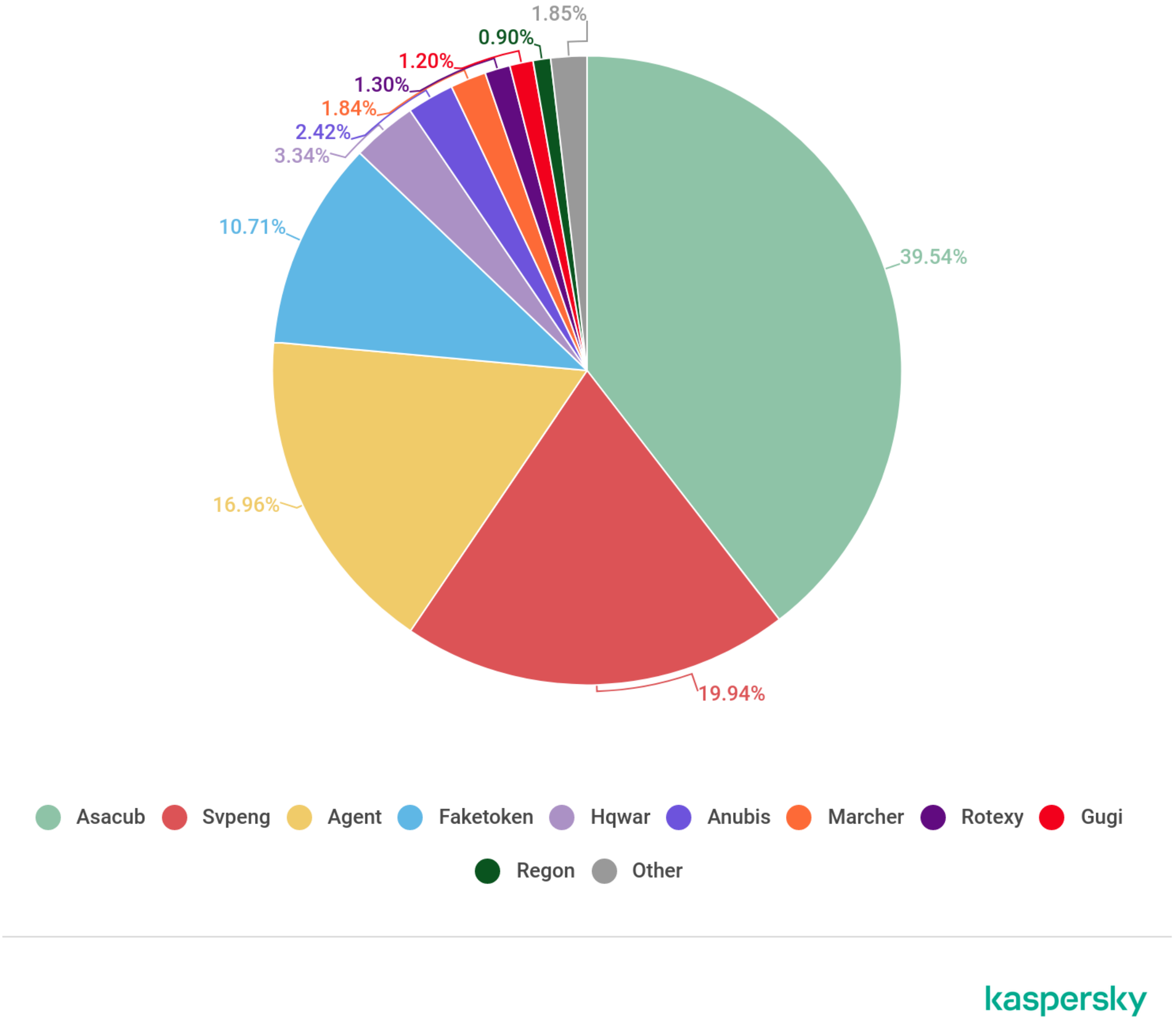
In 2019 the number of users that encountered Android banking malware dropped to 675,000 from around 1.8 million in 2018.

To get a clearer picture of what is behind these dramatic changes we took a closer look at the landscape and reviewed the most widespread families across the year. In 2018, the situation was as follows:



The most widespread Android banking malware in 2018 (download)

Asacub's share more than doubled YoY to almost 60%, followed by Agent (14.28%) and Svpeng (13.31%). All three experienced explosive growth in 2018, especially Asacub as it peaked from 146,532 attacked users in 2017 to 1,125,258.



The most widespread Android banking malware in 2019 (download)

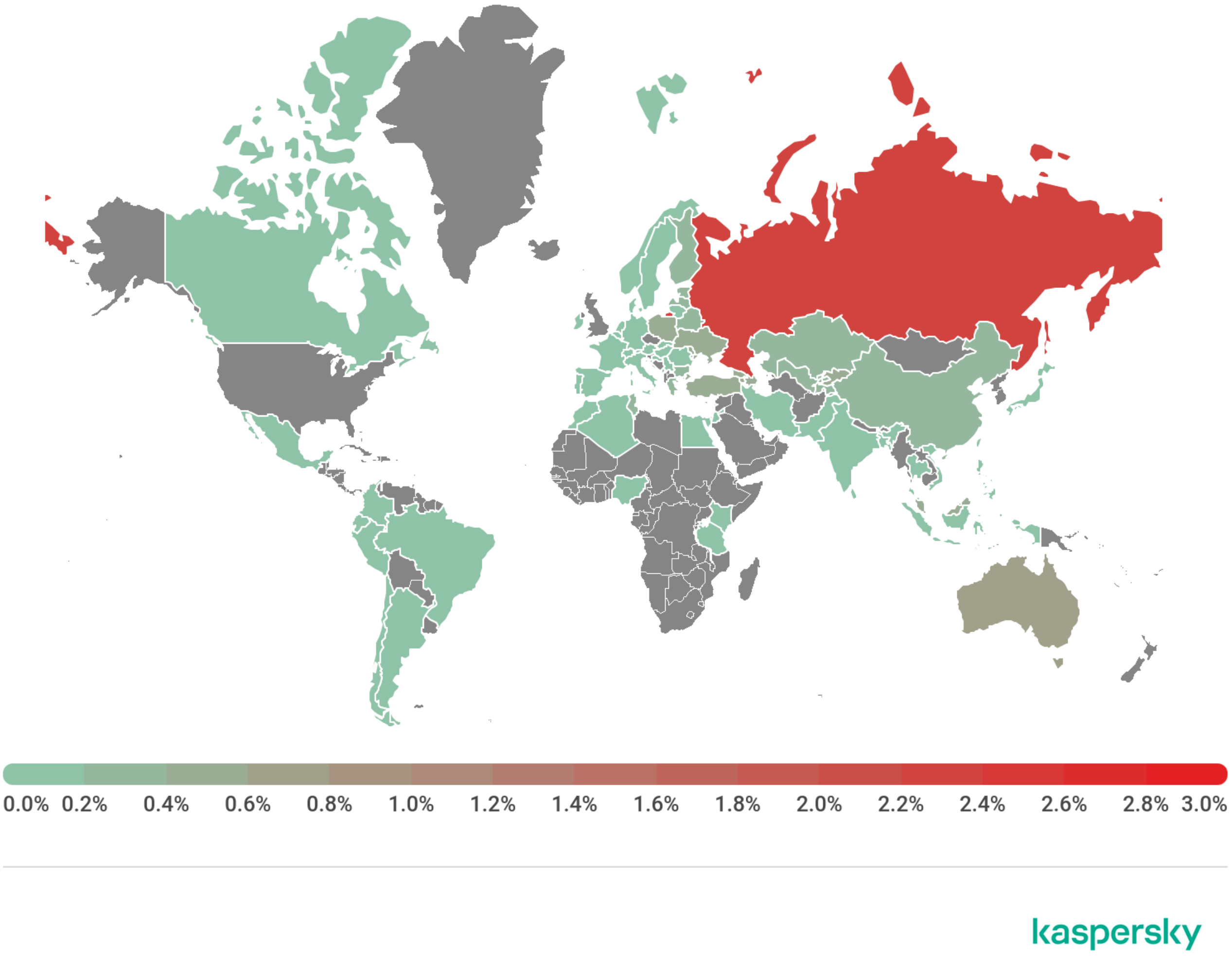
In 2019, there was almost no change among the most widespread families. The Asacub family was the only exception – it conceded some of its share to its nearest competitors. However, it still accounted for almost half of all attacks.

Geography of attacked users

In previous reports, we calculated the distribution of users attacked with Android banking Trojans by comparing the overall number of unique users attacked by this type of malware with the overall number of users in a region. There was always one problem – the majority of detections in Russia traditionally came from this malicious software due to the prevalence of SMS banking in the region, which allowed attackers to steal money with a simple text message if an infection was successful. Previously, the same was true for SMS Trojans, but after regulative measures, criminals found a new way to capitalize on victims in Russia.

In 2018, we decided to change the methodology and replaced the overall number of attacked unique users with the share of unique users that faced this threat from the overall number of users registered in the respective region.

The picture for 2018 was as follows:



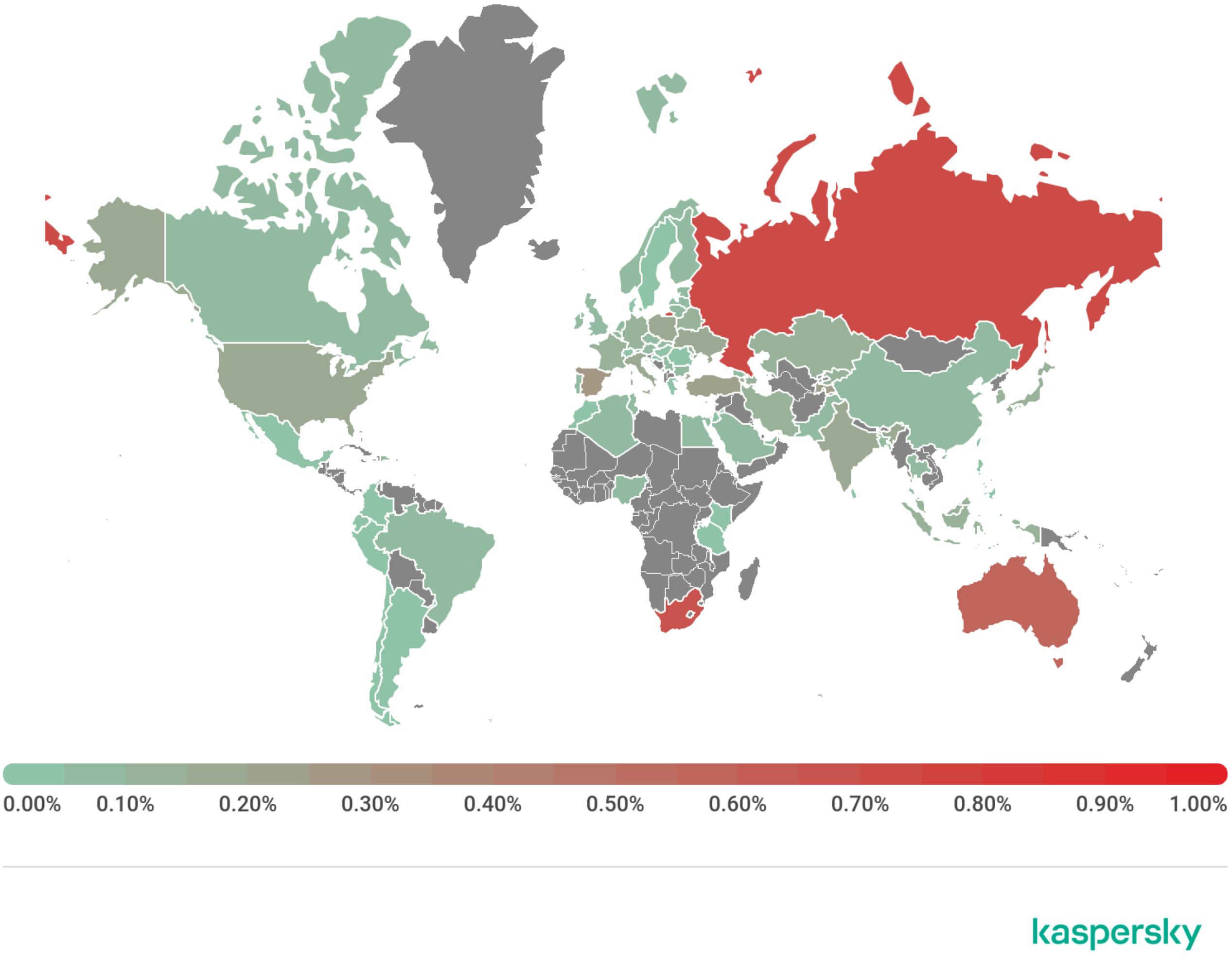
Percentage of Android users who encountered banking malware by country, 2018 ***(download)***

The top 10 countries with the highest percentage of users that encountered Android banking malware in 2018:

Russia	2.32%
South Africa	1.27%
US	0.82%
Australia	0.71%
Armenia	0.51%
Poland	0.46%

Moldova	0.44%
Kyrgyzstan	0.43%
Azerbaijan	0.43%
Georgia	0.42%

In 2019 it changed to:



Percentage of Android users who encountered banking malware by country, 2019 (download)

The top 10 countries with the highest percentage of users that encountered Android banking malware in 2019:

Russian Federation	0.72%
South Africa	0.66%

Australia	0.59%
Spain	0.29%
Tajikistan	0.21%
Turkey	0.20%
US	0.18%
Italy	0.17%
Ukraine	0.17%
Armenia	0.16%

Australia replaced the US in the top three. Also of interest is the fact that the average percentage fell for all countries – sometimes 2-digit decrease can be seen.

Major changes to the Android banking malware landscape

While the figures tell their own story, there are many more ways to explore the changes and developments in the threat landscape. Our key method is the analysis of actual malware found in the wild.

As this analysis shows, 2019 was a relatively stable year when it comes to malicious mobile software. One point of interest, however, may be a new technique that we recently observed with Ginp and Cerberus Trojans.

At the very beginning of 2020, we found a new version of the Ginp banking Trojan that was first discovered by a Kaspersky analyst in 2019. Apart from the standard functions of an Android banker – the ability to intercept and send text messages, and perform window overlays – the new version involves a highly unconventional function to insert fake text messages in the inbox of a standard SMS app.

These messages are made to look like notifications from reputable app vendors informing users about an undesirable event (blocked account access, for example). In order to resolve the issue, the user is requested to open the application. Once the victim does that, the Trojan overlays the original window and asks the user to enter their credit card or bank account details, which then end up in the hands of cybercriminals.

We subsequently detected a rise in a technique used by the infamous Cerberus banker on Android devices. This malware increasingly produces fake push notifications to users on behalf of several banking applications. The detected messages urge Polish-speaking targets to open applications and check their cards and bank accounts by entering their login credentials. This technique is on the rise with more fake notifications being produced on behalf of more and more banking applications.

Conclusion and advice

2019 has demonstrated that cybercriminals continue to update their malware with new features, investing resources in new distribution methods and techniques to avoid detection. The increase in banking Trojan activity targeting corporate users is also of concern as such attacks could bring more problems than attacks on ordinary users.

This all means that malicious users are still gaining financially from their activities.

As the above threat data shows, there is still plenty of motivation for financial fraud operations involving phishing and specialized banking malware. At the same time, mobile malware regained its ability to jeopardize users across the world.

To avoid losing money as a result of a cyberattack, Kaspersky experts advise the following.

To protect against financial threats, Kaspersky recommends that users:

Only install applications from trusted sources such as official stores;

Check what access rights and permissions the application requests – if they do not correspond to what the program is designed to do, then it should be questioned;

Do not follow links in spam messages and do not open documents attached to them;

Install a reliable security solution – such as Kaspersky Security Cloud – that protects against a wide range of threats. The service also incorporates the Permission Checker feature for Android that allows users to see which applications have access to a device's camera, microphone, location and other private information and restrict them if necessary.

To protect your business from financial malware, Kaspersky security specialists recommend:

Introducing cybersecurity awareness training for your employees, particularly those who are responsible for accounting, to teach them how to distinguish phishing attacks: do not open attachments or click on links from unknown or suspicious addresses;

Explaining to users the risk of installing programs from unknown sources. For critical user profiles, such as those in financial departments, switch on default-deny mode for web resources to ensure they can only access legitimate sites;

Installing the latest updates and patches for all the software you use;

Enabling protection at the level of internet gateways as it shields from many financial and other threats even before they reach employee endpoints. Kaspersky Security for Internet Gateways protects all devices in the corporate network from phishing, banking Trojans and other malicious payloads;

Using mobile protection solutions or corporate internet traffic protection to ensure employee devices are not exposed to financial and other threats. The latter helps protect even those devices for which antivirus is unavailable;

Implementing an EDR solution such as Kaspersky Endpoint Detection and Response for endpoint level detection, investigation and timely remediation of incidents. It can even catch unknown banking malware;

Integrating Threat Intelligence into your SIEM and security controls in order to access the most relevant and up-to-date threat data.

kaspersky

www.kaspersky.com/
www.securelist.com