Financial Cyberthreats in 2020

securelist.com/financial-cyberthreats-in-2020/101638/

Authors

Expert Kaspersky

2020 was challenging for everyone: companies, regulators, individuals. Due to the limitations imposed by the epidemiological situation, particular categories of users and businesses were increasingly targeted by cybercriminals. While we were adjusting to remote work and the rest of the new conditions, so were scammers. As a result, 2020 was extremely eventful in terms of digital threats, in particular those faced by financial institutions.

At the same time, some of the known APT (Advanced persistent threats) groups that are not generally targeting financial institutions have tried their hand at it. Existing at a special crossroads between APT and financial crime, the Lazarus group has already been among the most active ones in the financial sphere. In 2020, the group tried its hand at the big extortion game with the VHD ransomware family. Later on other groups, such as MuddyWater, followed suit.

Moreover, in 2020, we saw regional actors go global. A few Brazilian malware families expanded their operations to other continents, targeting victims in Europe and Asia. We have dubbed the first four families to have done this (Guildma, Javali, Melcoz, Grandoreiro) "the

Tétrade”. Later on the authors of Guildma also created the new banking malware Ghimob targeting users located in Brazil, Paraguay, Peru, Portugal, Germany, Angola, and Mozambique.

Of course, the known financial threats have remained, too. Thus, the year 2020 saw a surge in the use of Emotet, described by Interpol as “the world’s most dangerous malware”. In the beginning of 2021, law enforcement agencies all over the world joined their forces to disrupt the botnet’s infrastructure. According to Kaspersky experts, the operation will frustrate Emotet’s activities for at least several months. In the meantime, at least some of Emotet customers have switched to Trickbot.

Even though, in 2020, we have seen ever more sophisticated cyberattacks, the overall statistics look encouraging: the number of users hit by computer and mobile malware declines, so does financial phishing. Still, that does not mean that the cyber world has become a safer place – it means that the cybercriminals’ goals and tactics have undergone a number of changes. Despite the decreasing general statistics, we see that attacks have become more targeted and business-oriented. At the same time, we observe cybercriminals to skillfully adapt themselves to the global changes and benefit from the teleworking vulnerabilities and the rising popularity of online shopping. This report aims to shed a light on more details of financial cyberthreats in 2020.

This research is a continuation of our annual financial threat reports (2019, 2018 and 2017) providing an overview of the latest trends and key events across the financial threat landscape. Traditionally, the study covers the common phishing threats encountered by users, along with Windows and Android-based financial malware.

Methodology

In this research, by financial malware we mean several types of malevolent software. Firstly, we identify as financial the malware targeting users of financial services such as online banking, payment systems, e-money services, e-shops, and cryptocurrency services. Secondly, we use the term to define the malware attempting to gain access to financial organizations and their infrastructure. In most cases, financial malware attacks rely on spamming and phishing activities, such as creating and distributing fake finance themed web pages and emails to steal the victims’ payment info.

To examine the financial sector threat landscape, Kaspersky researchers have analyzed the malicious activities on devices owned by individuals using the Kaspersky security products, which they volunteered to make available to us through the Kaspersky Security Network. The corporate user statistics were collected from the enterprise security solutions, after our customers agreed to share their data with Kaspersky.

The data for 2020 was mostly compared against 2019 to monitor the malware development trends. However, in some parts, for better insight into the financial malware evolution, the study also refers to earlier times.

Key findings

Phishing:

- In 2020, the percentage of users hit by phishing declined slightly from 15.7% to 13.2%.
- This time around, e-shops became the target of choice for phishing attacks. Almost every fifth attempted visit to a phishing page blocked by Kaspersky products has been related to online store phishing.
- Phishing attacks against PayPal users soared from 26.8% in 2019 to 38.7% in 2020. The longtime leader of the category, Visa, dropped to the fourth place with 10.2% of phishing attacks against users of payment systems successfully prevented by Kaspersky in 2020.

PC:

- In 2020, 625,364 users were attacked by banking Trojans – 148,579 less from 773,943 in 2019.
- This year, users in Russia, Germany and Kazakhstan were the most frequent targets of financial malware.
- Zbot is still the most widespread banking malware (22.2 % of attacked users), the second place is now held by CliptoShuffler (15.3%), with Emotet (14.5%) in the third place as before.
- 36% of users hit by banking malware are corporate ones – an increase of one percentage point from the previous year.

Mobile:

- This year, the number of users attacked by Android banking malware rapidly dropped by more than 55%: from 675,772 in 2019 to 294,158 in 2020.
- Japan, Taiwan and Spain ended up with the highest percentage of users hit by Android banking malware.

Financial phishing

Financial phishing is one of the most popular tools used by cybercriminals to make money. Its prevalence is explained by the fact that it does not require much investment or technical expertise. In most cases, successful scammers win access either to the victim’s money or data that can be sold or otherwise monetized.

Percentage of financial phishing attacks (of the overall phishing attacks) detected by Kaspersky, 2016 – 2020 (download)

In 2020, Kaspersky anti-phishing technologies detected 434,898,635 attempted visits to various types of phishing pages. As can be seen from the graph above, 37.2% of those were related to financial phishing – 14.2 p.p. less than the figure registered in 2019 (51.4%). The lowest financial phishing percentage in the past five years.

By "financial phishing" we mean not banking phishing alone but several other types as well. For one, there are the 'payment systems', which include pages mimicking the well-known payment brands like PayPal, Visa, MasterCard, American Express and others. There are also the 'e-shops' which include online stores and auction sites like Amazon, Apple store, Steam, E-bay and others.

In 2019, the financial phishing cases detected by Kaspersky products were distributed as follows:

Distribution of financial phishing cases by type in 2019 (download)

Distribution of financial phishing cases by type in 2020 (download)

The year 2020 was definitely a unique one when it comes to financial phishing. One year back, we reported an increase in bank-related phishing from less than 22% to almost 30%. In 2020, banking phishing reached only 10.72 percent of the total. The e-shops, with 7.57% in 2019, on the contrary, almost tripled reaching 18.12%. Kaspersky experts connect these changes with the lockdown measures due to the pandemic – at home most of the time, people turned to online shopping and digital entertainment. Thus, growing demand from the users has led to increased "supply" from the cybercriminals. It should be noted that, while online shopping proved the most appealing field for scammers, payment systems were not that much of a lure – their share barely reaching 8.41%.

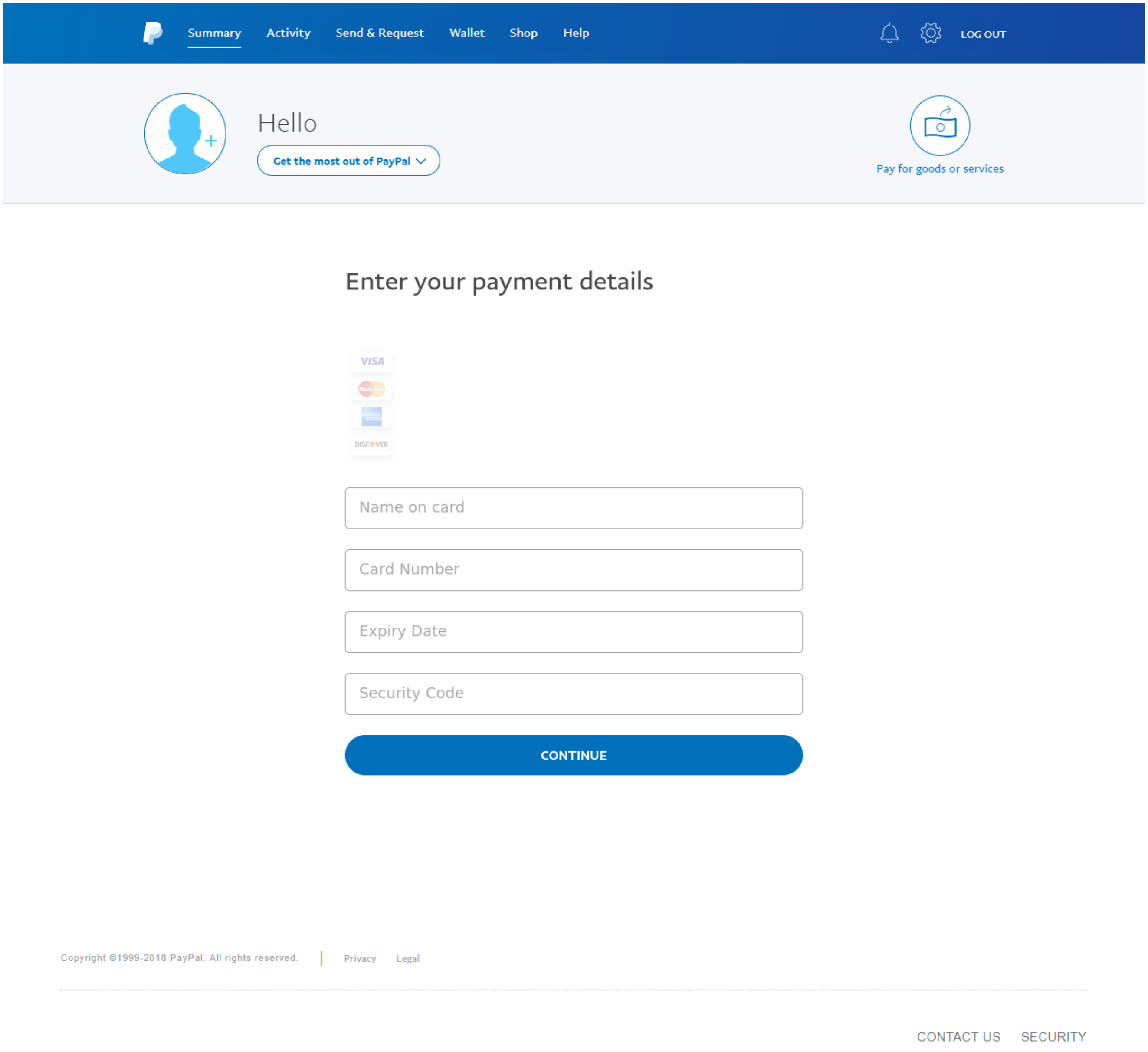
2019 statistics on payment systems:

The most frequently used brands in 'payment systems' financial phishing schemes in 2019 (download)

As can be observed from the graph above, the users of Visa Inc. (37.6%) were targeted the most in 2019. PayPal came in second with 26.8%, while MasterCard closed the top 3.

The most frequently used brands in 'payment systems' financial phishing schemes in 2020 (download)

In 2020, the PayPal brand name (38.7%) was used for scam more than those of any other popular payment system. Its share grew by 12 p.p.



Enter your payment details

Name on card

Card Number

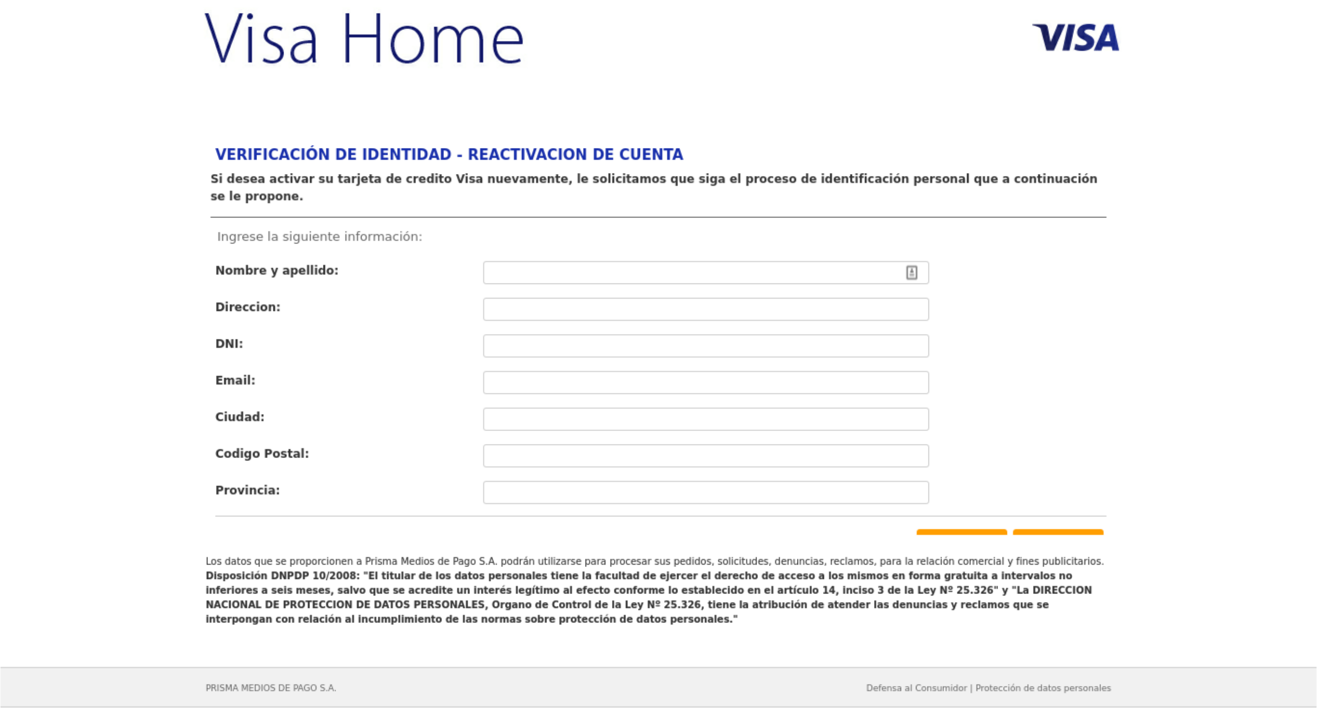
Expiry Date

Security Code

Copyright ©1999-2018 PayPal. All rights reserved.

Example of a phishing page targeting PayPal users

Mastercard made it to the second place slightly increasing its share from 16.3% to 17.5%. The third and the fourth places, with a tiny difference between them, were taken by American Express (10.6%) and Visa (10.2%). As was observed, in 2020, scammers mimicked Visa Inc. 3.5 times less than in 2019 (37.6%).



VERIFICACIÓN DE IDENTIDAD - REACTIVACION DE CUENTA

Si desea activar su tarjeta de credito Visa nuevamente, le solicitamos que siga el proceso de identificación personal que a continuación se le propone.

Ingrese la siguiente información:

Nombre y apellido:

Direccion:

DNI:

Email:

Ciudad:

Codigo Postal:

Provincia:

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."**

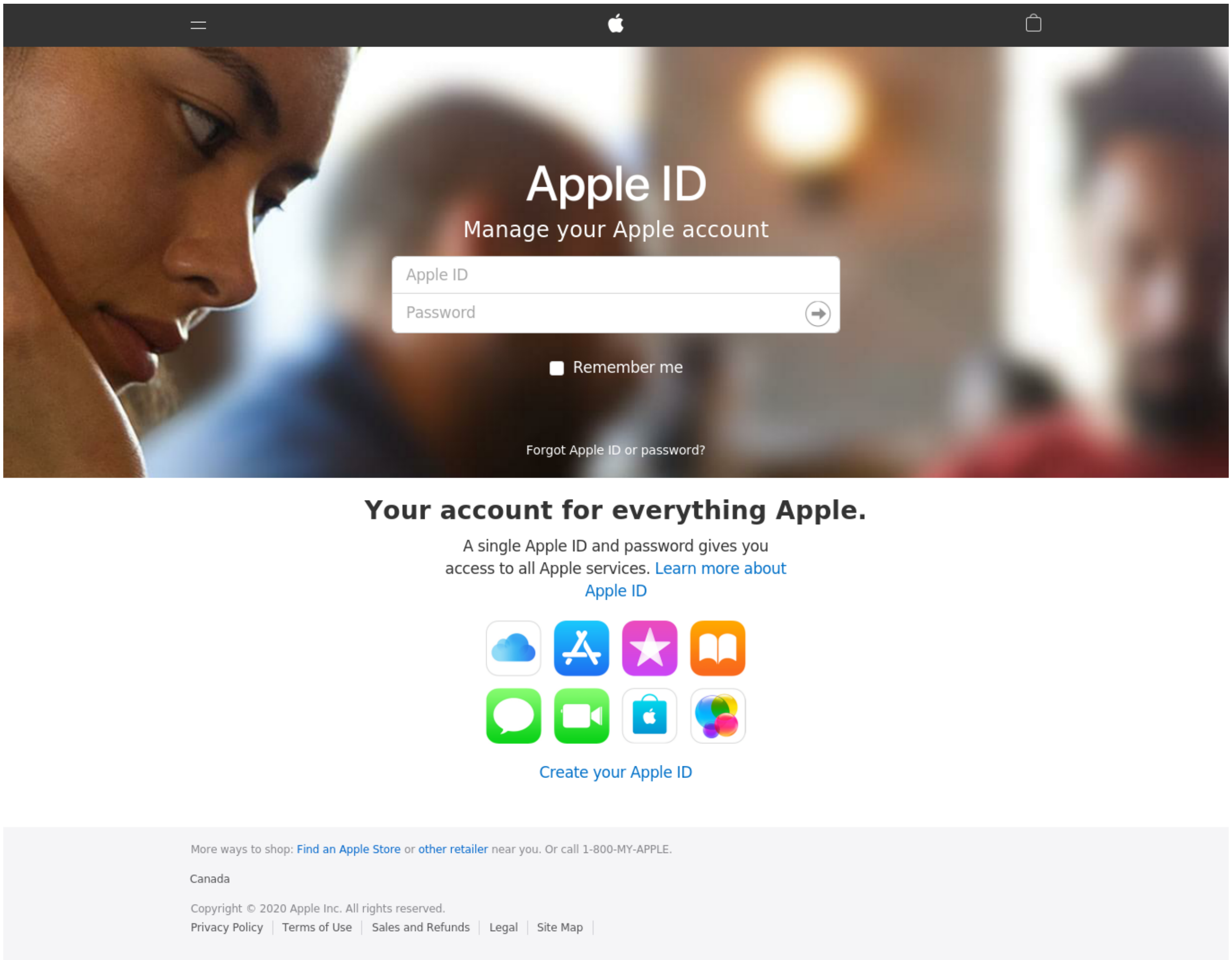
PRISMA MEDIOS DE PAGO S.A.

Defensa al Consumidor | Protección de datos personales

Example of a phishing page targeting Visa users

In 2019, we analyzed the ‘e- shop’ brands most frequently used by cybercriminals in financial phishing schemes. The results showed Apple (42.8%) to be the number one choice for scam. The online stores Amazon (23.6%) and eBay (14.2%) took the second and the third place respectively.

Brands most frequently used in ‘e-shop’ financial phishing schemes, 2019 (download)



Apple ID

Manage your Apple account

Apple ID

Password

□ Remember me

Forgot Apple ID or password?

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services. Learn more about Apple ID

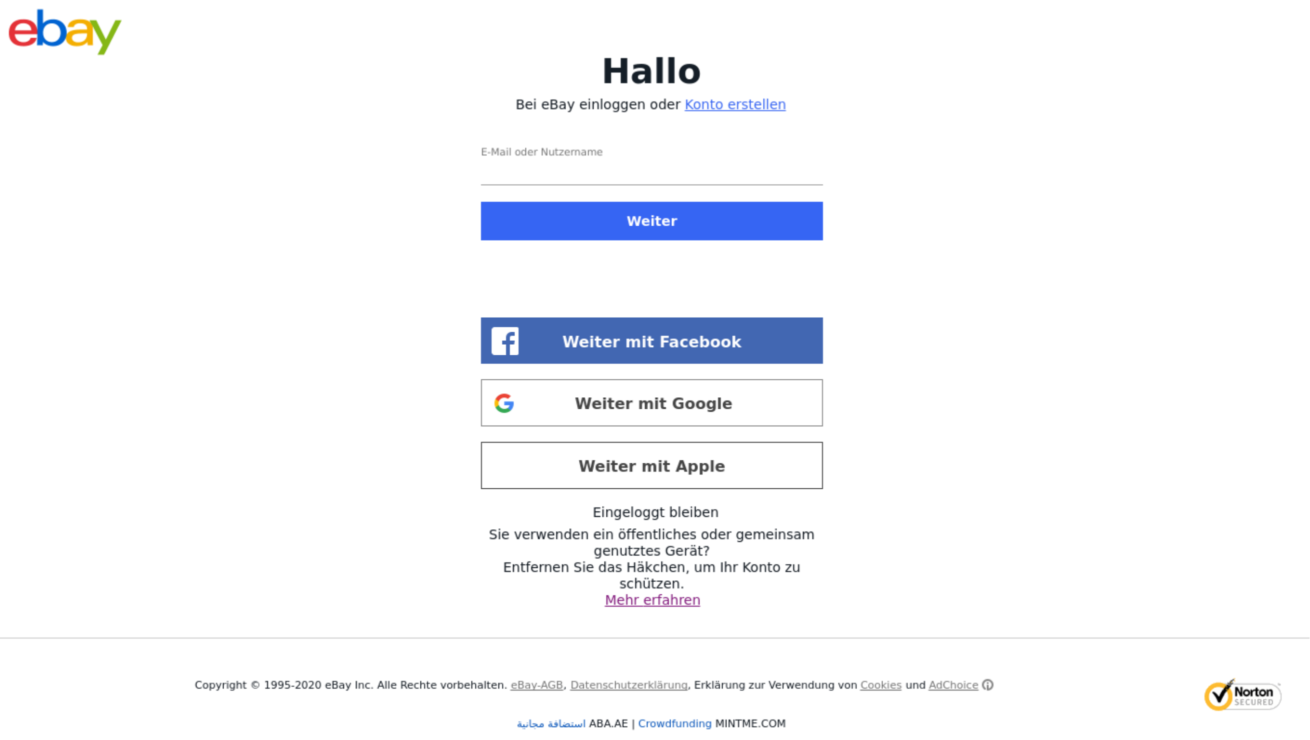
Create your Apple ID

More ways to shop: Find an Apple Store or other retailer near you. Or call 1-800-MY-APPLE.

Canada

Copyright © 2020 Apple Inc. All rights reserved.

Privacy Policy | Terms of Use | Sales and Refunds | Legal | Site Map |



Hallo

Bei eBay einloggen oder Konto erstellen

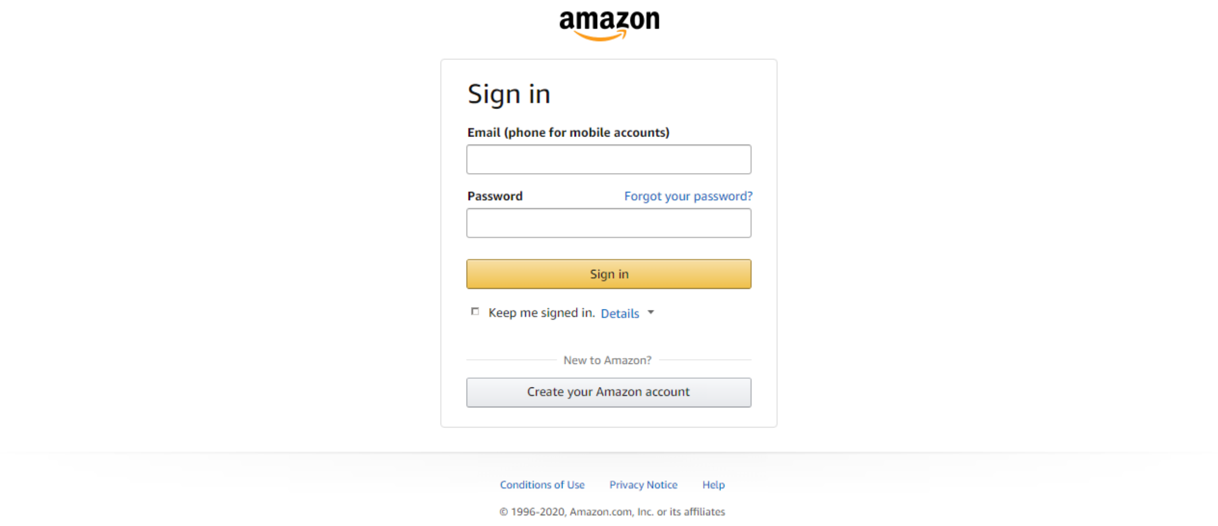
E-Mail oder Nutzername

Eingeloggt bleiben

Sie verwenden ein öffentliches oder gemeinsam genutztes Gerät?
Entfernen Sie das Häkchen, um Ihr Konto zu schützen.
Mehr erfahren

Copyright © 1995-2020 eBay Inc. Alle Rechte vorbehalten. eBay-AGB, Datenschutzerklärung, Erklärung zur Verwendung von Cookies und AdChoice

استضافة مجانية ABA.AE | Crowdfunding MINTME.COM


amazon
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Sign in
□ Keep me signed in. Details
New to Amazon?
Create your Amazon account
Conditions of Use
Privacy Notice
Help
© 1996-2020, Amazon.com, Inc. or its affiliates

Examples of phishing pages based on the online store brands most used by cybercriminals

In 2020, as the e-shop phishing continued to grow, Amazon made it to the first place with 27.84% of total. Challenged by the popular online store, Apple (27.07%) stepped down to the second place, its share reduced by 15 p.p. Steam and eBay swapped their positions – Steam (14.90%) finished third, and eBay (12.85%) fourth.

Brands most frequently used in 'e-shop' financial phishing schemes, 2020 (download)

Banking malware for PC

In this study, we analyze the banking malware that steals the credentials used to access online banking or payment system accounts and to intercept one-time passwords.

After an upsurge of malware activity in October 2016, when as many as 1,494,236 users were hit, we observed a gradual decline in the number of users attacked with banking malware. 2020 was no exception. The number of attacked users has declined from 773,943 in 2019 to 625,364 – almost a 20% drop.

The reduction can be explained by the fact that attacks are becoming more targeted – cybercriminals now prefer to attack large businesses. Yet common users and small entities continue to fall victim to cybercriminal groups such as Zbot, CliptoShuffler, Emotet, RTM and others.

Dynamic change in the number of unique users attacked with banking malware 2018 – 2020 (download)

The main actors

Every year we detect multiple families of banking malware: some of them become outdated, some, on the contrary, gain popularity among cybercriminals. Below is a list of top 10 most active banking malware families detected in 2019. The leading ones were Zbot (21.6%), RTM (19.8%), Emotet (12.6%), CliptoShuffler (5.6%) and Trickster (5.5%).

TOP 10 most widespread banking malware families in 2019 (download)

This year we continued tracking the most active banking malware families. It is quite noteworthy that only four of them (Zbot, CliptoShuffler, Emotet and RTM) account for more than one half of the attacked users. Below is a list of top 10 banking malware families we detected in 2020.

TOP 10 most widespread banking malware families in 2020 (download)

While Zbot (22.2%) still enjoys the status of the most used malware in the financial sphere, there were some changes in the list. RTM, with 10.5%, dropped from the second to the fourth place, while two other families, CliptoShuffler (15.3%) and Emotet (14.5%), both climbed higher in 2020. Notably, Gozi (3.3%), the second most active family just two years ago, was pushed out to the ninth place.

What is more, year 2020 has also been special for expansion of regional threat actors into the outside world. Thus, the four large Brazilian families we have called the Tétrade went global targeting not only Latin America but Asian and European countries as well.

Geography of attacked users

To assess and compare the degree of computer infection risk faced by users in different countries of the world, we have calculated for each country the proportion of Kaspersky product users faced by the threat during the period of report versus the total number of users attacked by financial malware.

Traditionally, more than half of all users hit with banking malware in 2019 and 2020 came from 10 countries. In 2019, the top 10 was as follows:

Russian Federation	33.6%
Germany	7.4%
China	3.3%
Brazil	3%

India	3%
Mexico	3%
Vietnam	2.70%
Italy	2.60%
Kazakhstan	2%
United States	2%

In 2019, Russia’s share reached 33.6% of the total, Germany finishing second with 7.4%, and China closing the top three with 3.3%.

In 2020, the situation was as follows:

Russian Federation	26.6%
Germany	4.5%
Kazakhstan	4.1%
Brazil	3.4%
China	3.4%
Italy	3.3%
India	3.1%
Mexico	2.8%
Vietnam	2.8%
Uzbekistan	2.3%

As can be seen from the chart, despite the decline Russia (26.6%) and Germany (4.5%) still hold the first and second places in the top 10. Notably, Russia’s figures always tend to be the highest due to the fact that most Kaspersky users are located in Russia. Kazakhstan, which used to be 9th with 2%, this year broke into the top three having added 2 more percentage points.

Types of users attacked

It can be noticed that financial malware becomes more corporate-oriented. This year we observed that 36% of users attacked by banking malware are corporate ones – one percentage point up from the previous year. This partly confirms our hypothesis about cybercriminals shifting their attention to the corporate sector. Still, the increase is relatively small, and we expect the redistribution of attacks between corporate and private users to clear up in the near future.

Corporate vs consumer product users, 2019–2020 (download)

All in all, in 2020, companies became more vulnerable due to the restrictions for onsite work and staff, coupled with increased number of employees using the corporate network remotely. The hasty transition to teleworking has affected the corporate security – most businesses were not ready to go online. Some of them lacked the devices, so employees had to use their home computers for work. Lack of online security training, default laptop configurations left as is, vulnerable remote access connections – together these factors have paved way to all sorts of attacks, including banking malware scams.

Cryptocurrency related cyberthreats in 2020

Three years ago, in 2018, cryptocurrencies made the hottest topic and turned the eyes of the whole cybersecurity community to the new danger. We have analyzed the hidden mining software cybercriminals spread to coin money at the users' cost, and found that today the malicious activity is not that widespread.

Number of users attacked by mining malware in 2019 (download)

Number of users attacked by mining malware in 2020 (download)

Geography of mining attacks, 2020 (download)

Thus, in 2020, we continued to observe a downward trend for this type of threat. Yet by the end of the year the numbers reached a certain plateau, and we even saw local trend reversals. It is likely that the sharp increase in cryptocurrency prices at the end of 2020 may boost the threat in early 2021. Moreover, due to the COVID crisis, we may yet see some economies collapsing and local currencies plummeting in 2021, which would turn cryptomining a lot more attractive.

Mobile banking malware

Android banking malware is a well-known threat Kaspersky experts have been analyzing for years. Last year was a dramatic one in terms of mobile banking malware. As stated in our previous annual report, in 2019, the number of users hit by it dropped to just over 675 thousand from around 1.8 million in 2018.

Number of users attacked with Android banking malware, 2018 – 2019 (download)

In 2020, we observed a continuation of this trend as the number of attacked users decreased by more than 55% to 294,158.

Number of users attacked with Android banking malware, 2019 – 2020 (download)

To get a better view of the reasons behind these dramatic changes, Kaspersky experts took a closer look at the landscape and reviewed the most widespread families over the year. In 2019, the situation was as follows:

Most widespread Android banking malware in 2019 (download)

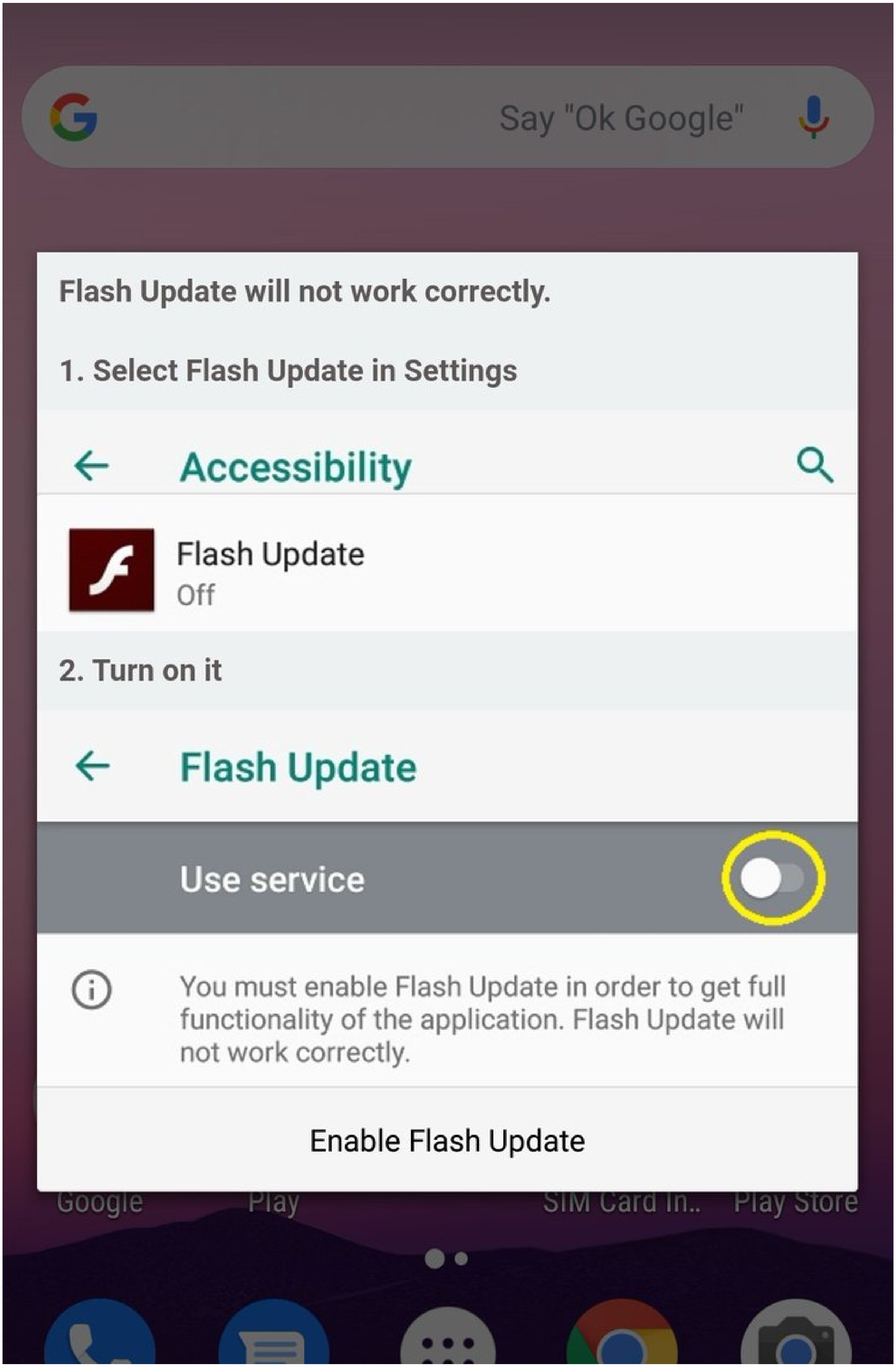
In 2020, Asacub's (25.6%) share is still the weightiest. Yet it shrank by 18.8 percentage points since 2019. Agent (18.0%) is still in the second position, although a bit lighter from the year before. Svpeng (12.8%), which mostly hunts for the administrator rights on the infected device, this year was challenged by Rotexy (17.9%), in which the banking Trojan's features are combined with those of a ransomware blocker.

Most widespread Android banking malware in 2020 (download)

All in all, 2020 was rich in new mobile banking malware. Let us give a brief overview of this year's major findings:

- **Trojan-Banker.AndroidOS.Ghimob.a**
  New banking malware from the Tétrade group that went global this year and attacked banks, exchanges, cryptocurrency exchangers and fintech organizations in Brazil, Paraguay, Peru, Portugal, Germany, Angola, and Mozambique. Ghimob was able to spy on a total of 153 mobile apps, which is impressive for a banking Trojan.
- **Trojan-Banker.AndroidOS.Gorgona.a**
  The malware mimics Google Play and uses the notification panel to attract the user's attention. It can make and redirect calls, execute USSD commands, install additional apps and block the device, if needed. If granted the permission to use Accessibility, it can get even more rights, for example, to receive and process text messages. Thus, it can gain control of the two-factor authentication. Uses TCP for C2 communication. Tends to target banks in Turkey.

- **Trojan-Banker.AndroidOS.Knobot.a**
  The new financial threat market player. Alongside phishing windows and interception of the two-factor authentication messages, the Trojan offers several features not typical of financial threats. For example, a mechanism for interception of device PIN code through Accessibility services.
  Ironically, it asks its victim to delegate the rights and even provides a small instruction on how to do it.



Flash Update will not work correctly.

1. Select Flash Update in Settings

Accessibility

Flash Update
Off

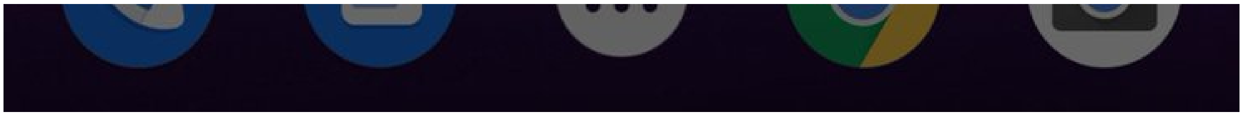
2. Turn on it

Flash Update

Use service

You must enable Flash Update in order to get full functionality of the application. Flash Update will not work correctly.

Enable Flash Update



A screenshot of Trojan-Banker.AndroidOS.Knobot.a on user’s phone

Geography of attacked users

Top 10 countries by percentage of users hit by 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%
United States	0.18%
Italy	0.17%
Ukraine	0.17%
Armenia	0.16%

Top 10 countries by percentage of users hit by Android banking malware in 2020:

Japan	2.83%
Taiwan (province of China)	0.87%
Spain	0.77%
Italy	0.71%
Turkey	0.60%
Korea	0.34%
Russian Federation	0.25%
Tajikistan	0.21%
Poland	0.17%

Australia	0.15%

As can be seen from the statistics, all the countries were completely reshuffled year on year. Russia from it top position in 2019 moved to the 7th place in 2020. Armenia, which used to close the 2019 chart, left it altogether. On the other hand, Japan (2.83%) and Taiwan (0.87%), not even mentioned in 2019, rapidly gained more users hit by Android banking malware and made it to the top. Meanwhile Spain (0.77%) ousted Australia from the third place with almost 3 thousand of affected users.

Conclusion

The year 2020 has shown that cybercriminals can easily adapt to new realities of the changing world. They keep updating their malware with new features and improving the detection avoidance techniques. The general statistics in all the areas we have analyzed (PC and mobile malware, phishing) is on the downward trend, which is a good sign.

We have observed that, in 2020, the phishing scammers have switched their attention from banks to e-shops. This trend is closely related to the pandemic, which has greatly changed the public’s attitude towards online shopping: criminals have marked its growing popularity and turned focus on it. We have registered a slight increase of the share of malware attacks against corporate users. The emerging trend of banking Trojans targeting corporate users is also of concern, as such attacks are likely to bring more problems than attacks on individuals. At the same time, the regional scam factories targeting financial organizations are increasingly reaching the global level, potentially resulting in more growth in 2021. Thus, even though the general statistics look positive, we have to consider the massive threat landscape still faced by financial organizations.

For protection against financial threats, Kaspersky recommends users to:

- Install only applications obtained from reliable sources, such as the official websites;
- Check the access rights and permissions requested by the application – do not grant them if they fail to match the app’s feature set;
- Never follow links from spam messages and never open documents attached to them;
- Install a trusted security solution, such as Kaspersky Security Cloud – it will protect you from a broad range of financial cyberthreats.

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

- Introduce cybersecurity awareness training for your employees, particularly those responsible for accounting, to teach them to detect phishing pages and improve the digital literacy of staff in general;
- For critical user profiles, such as those in financial departments, enable the default deny mode for web resources to ensure that only legitimate ones can be accessed;

- Install the latest updates and patches for all the software you use;
- For protection from complex threat and targeted attacks, install the anti-APT and EDR solutions for network threat detection, incident investigation and timely recovery action. Provide your SOC team with access to the latest threat intelligence and regular upskill training. All these are available within the Kaspersky Expert Security framework.

- Electronic Payments
- Financial malware
- Google Android
- Malware Statistics
- Microsoft Windows
- Phishing
- Trojan Banker

Authors

Kaspersky

Financial Cyberthreats in 2020

Your email address will not be published. Required fields are marked *