Kaspersky Fraud Prevention

Cyberfraud report based on Kaspersky Fraud Prevention data

kaspersky BRING ON THE FUTURE

For more information, please visit kfp.kaspersky.com

Contents

General fraud statistics & trends of 2021

Looking back…

More of the same?

In the Kaspersky Fraud Prevention Report 2020[1], we discussed how the forced digitisation induced by the pandemic benefited fraudsters and cybercriminals worldwide. We detailed the prominent types of fraud, with increased cyber-fraud, social engineering – with particular emphasis on phishing scams and IVR fraud – as well as money laundering and ecommerce fraud in general. 2021 was no different: whilst life is slowly getting back to normal for individuals and businesses, it is also unfortunately getting back to normal for fraudsters and cyber-criminals. Whilst the initial pandemic shock wave as a world event has died down, COVID-19 remained the most popular lure in social engineering attacks, and fraudsters continued to exploit its long-lasting effects. They capitalised on the need for information (e.g. disease tracking, new variants, financial assistance, etc.) and the shift towards hybrid working models, as evidenced by the rise in the number of cyber-attacks targeting business through their remote employees[2][3]. Indeed, never has the attack surface been so wide, with an ever-increasing digital presence, a general move towards cloud-based solutions, growing inter-connectivity and a rapidly evolving technology landscape.

What were the attacks?

As cybercriminals continued to exploit the various stages of the pandemic, they kept in tune with related developments[4] for financial gain (e.g. vaccination lures, tracking apps, fake vaccine certificates, fake cures, etc.). They also took advantage of the global accelerated digitisation, and exploited **working-from-home technologies**, all too often hastily deployed by organisations trying to keep afloat – focusing on attacking old, unpatched and newly discovered vulnerabilities as well as gaining initial access through social engineering and/or compromised credentials. This is turn led to a surge in **Authorised Push Payment Fraud** (APP), and in the UK alone, this increased by 71% in the first half of 2021[5].

It is also undeniable that **ransomware** became one of the greatest threats faced by organisations in any sector today, ranking it as a national security priority[6]. In fact, ransomware is so lucrative that some criminal groups shifted attack modes altogether, as observed with FIN11 who switched operations from Point-Of-Sale (POS) campaigns to targeted ransomware[7]. In fact, ransomware groups are no longer only opportunistic in targeting SMEs with immature security postures, and increasingly target bigger organisations that could potentially pay higher ransoms.

In addition, criminals capitalised on the accelerated **adoption of cloud infrastructures** to cater for new working patterns and behaviours. Indeed, compromised external cloud assets were more common than on-premises assets in both incidents and breaches[8], and those that were breached were generally found to be poorly secured and/ or not having deployed multi-factor authentication[9].

Cloud adoption also led to many forms of ransomware, from attacks on container environments to steal credentials and leak information, leading businesses to face not only public exposure and regulatory scrutiny, but also crippling operational downtime, lest a ransom be paid. Ransomware payments doubled in 2021[10], and in the UK alone, ransomware attacks doubled in a year[11], despite increase enforcement action worldwide[12][13](leading to criminals switching from Bitcoin to Monero, a less traceable crypto-currency, as their payment of choice).

As criminals were successful in extorting payments from their victims, they needed to convert their cryptocurrency into money, leading ransomware groups to establish sophisticated operations, often cooperating with other criminal groups (e.g. affiliates) and using crypto payment facilities (e.g. mixers, exchanges, etc.) to launder their illicit gains. Countering **money laundering** has become a top priority for governments and businesses alike in the last two years[14].

[1] https://kfp.kaspersky.com/wp-content/uploads/2021/01/Kaspersky-Fraud-Report-English-2020.pdf

[2] https://venturebeat.com/2021/10/14/battling-new-cyberthreats-in-your-hybrid-work-environment-vb-live/

[3] https://digit.fyi/mobile-cyber-attacks-two-thirds-of-uk-workers-risk/

[4] https://www.pwc.co.uk/issues/cyber-security-services/insights/five-cyber-threat-trends-to-prepare-for-in-2021.html

[5] https://www.ukfinance.org.uk/press/press-releases/government-coordinated-action-needed-fraud-losses-rise-30-cent

[6] https://www.reuters.com/world/russia-excluded-30-country-meeting-fight-ransomware-cyber-crime-2021-10-13/

[7] https://content.fireeye.com/m-trends/rpt-m-trends-2021

[8] https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf

[9] https://www.verizon.com/business/resources/reports/dbir/

[10] https://www.wsj.com/articles/suspected-ransomware-payments-for-first-half-of-2021-total-590-million-11634308503

[11] https://www.theguardian.com/uk-news/2021/oct/25/ransomware-attacks-in-uk-have-doubled-in-a-year-says-gchq-boss

[12] https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

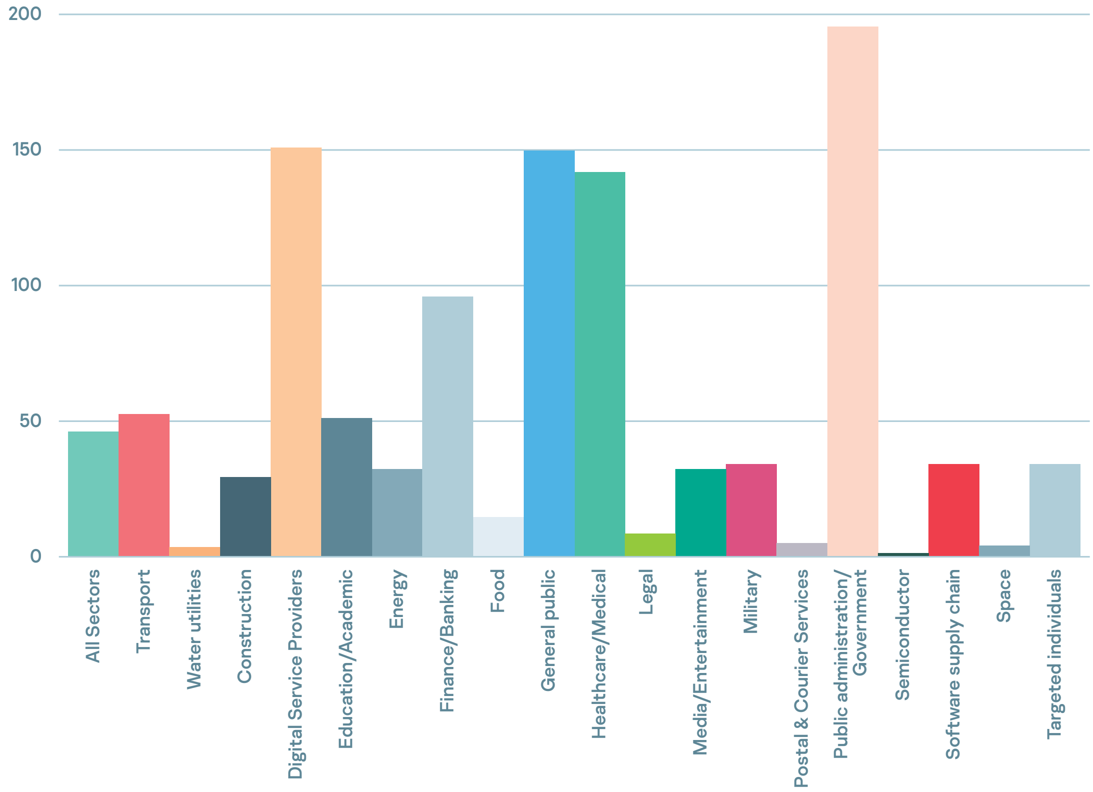
[13] https://www.cnbc.com/2021/11/08/revil-ransomware-2-arrested-for-international-cyberattacks.html

[14] https://duo.com/decipher/fincen-warns-of-evolving-ransomware-money-laundering-efforts

1

Who were the victims?

The most attacked industries/individuals' categories.



ENISA Threat Landscape 2021

Digital Services Providers were most targeted because of their horizontal supply model, and we saw many supply-chain attacks during 2021. It will also not come as a surprise that the healthcare/ medical sector was particularly hit, predominantly with targeted ransomware attacks, mostly on small and medium-sized hospitals and clinics which could ill-afford the impact of the disruption. Significantly during this period, the general public was in the top three most targeted segments, confirming that changing working patterns and digital behaviours – and the supporting technologies - continue to present a risk for businesses and attractive opportunities for fraudsters. And as in previous years, the Financial Services sector remains in the top four, as after all, criminals continue to "follow the money".

2

Did we invest more in cybersecurity?

Cybersecurity spending increased by 12% overall in 2021, according to Gartner[15], and spending generally increased in all areas:

Market Segment	2020	2021	Growth (%)
Application Security	3.333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2.981	3,505	17.5
Identity Access Management	12.036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4.859	5,473	12.6
Network Security Equipment	15.626	17.020	8.9
Other Information Security Software	2.306	2,527	9.6
Security Services	65.070	72.497	11.4
Consumer Security Software	6.507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Gartner 2021 CIO Agenda Survey

[15] https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Unsurprisingly, the biggest share of investment goes to security services (41%), infrastructure protection (16%) and network security equipment (11%). Given the massive increase in cloud services adoption in general, it will also not come as a shock that cloud security showed the biggest increase in spending by far (41.2%), but this doesn't compensate for the worrying lack of investment in the area as total spending only amounted to 0.5% of total in 2021. This is even more worrying as in 2020 and 2021, Enisa[16] observed a spike in "non-malicious incidents", as the COVID-19 pandemic became a multiplier for human errors and system misconfigurations, mostly affecting cloud environments. But maybe we can see a light at the end of the tunnel, as spending in Identity Access Management, a key building block for curbing fraud and cybercrime, increased by 15.6% overall, representing 9% of total spend.

[16] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

General statistics based on Kaspersky Fraud Prevention data

General statistics based on Kaspersky Fraud Prevention data

The Kaspersky Fraud Prevention Report is based on cyberincidents and data received by Kaspersky Fraud Prevention.

This report provides examples of the main threats encountered by companies, analyzes current cyberfraud trends with a focus on cybersecurity issues in the banking sector and e-commerce, and presents our main conclusions.

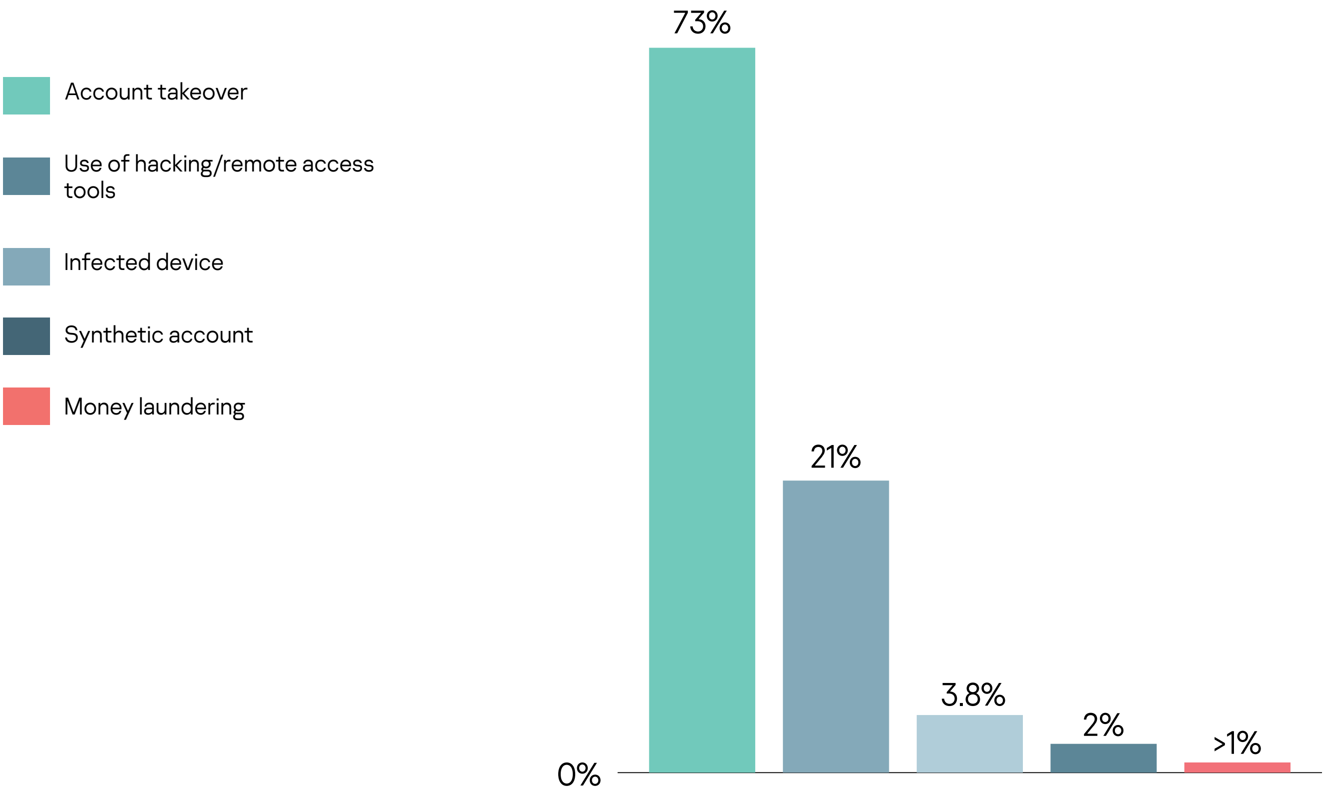
Kaspersky Fraud Prevention analyzes traffic in real time according to the following parameters:

3

Parameter	Average number of unique units per day
User	4.1 mln
Device	4.8 mln
Session	9.5 mln
Event	197 mln

4

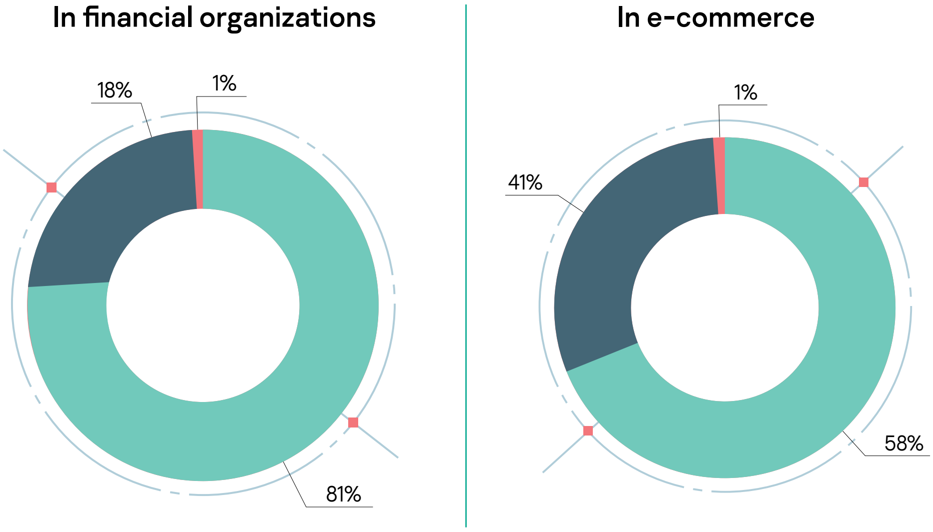
Incidents generated by Kaspersky Fraud Prevention



5

Risk-Based Authentication eliminates the need for additional authentication steps for legitimate users, allowing them to log in without excessive verification. By constantly analyzing hundreds of different indicators in real time, a dynamic assessment of the level of risk is formed. It allows a decision to be made with a high degree of confidence regarding the level of access to a personal account.

Annual average ratio of online user session risk-level verdicts



🟩 Legitimate user

🟥 High risk of fraud

⬛ Insufficient information, moderate risk of fraud

Analysis of user session events using Kaspersky Fraud Prevention technologies:

- **Analysis of a device and its environment**
  Leverages the advantages of Kaspersky's global presence to identify "good" devices and utilize this data for user authentication. Based on the global reputation of devices, IP addresses, location indicators and other data, any attribute that has been involved in fraudulent activity is proactively detected and marked as suspicious or associated with fraud.

- **Behavioral analysis**
  Tracks user activity during login and throughout the session, analyzes typical navigation attributes, time indicators, account activity and clicks, and much more. This lets you generate a profile of normal, legitimate behavior of a client and then detect any anomalous or suspicious activity during login attempts.

- **Behavioral biometrics**
  Analyzes various types of user interactions with a device, such as mouse movements, clicks, scrolls, touches, screen swipes and more to recognize when the device is being used by a legitimate user or by a cybercriminal, whether human or machine. This technology also lets you detect bots, remote administration tools, and account takeover activities.

- **Malware detection**
  Lets you determine whether a user device is infected with malware without installing additional components. Data on potential infection is used for risk-based authentication (RBA) and for determining the legitimacy of transactions.

Social engineering in 2021

How social engineering techniques evolved during the height of the 2020 pandemic and how they are changing now

Hackers have never missed an opportunity to take advantage of past crises to attack entrepreneurs, government officials and ordinary people who were temporarily overwhelmed and/or confused by these new situations. The COVID-19 pandemic was no exception. As soon as the World Health Organization (WHO) declared an emergency over the COVID-19 epidemic, cybercriminals immediately started planning and conducting malicious attack campaigns that took advantage of local events and news. The WHO itself was not immune to attacks either.

Google and Microsoft conducted extensive research on how the pandemic impacted the cyberthreat landscape and concluded that cybercriminals exploited the desire of people and organizations to obtain more information about the crisis as it gained momentum.

The global trends of cyberattacks went unchanged overall. Cybercriminals simply adapted their lures and malware to current local conditions. For instance, the beginning of March showed a rapid growth in the number of attacks that exploited the up-to-the-minute breaking news related to the COVID-19 topic. However, after a while it became more and more difficult to catch people off-guard with the emerging situations, and COVID-19 became just another pretext among many others used for deception. By employing social engineering techniques, cybercriminals were able inject malicious code, hack corporate infrastructures and obtain user account credentials of employees, which provided new opportunities for subsequent attacks. Some industries suffered more than others.

The pandemic also set the stage for the expansion of financial fraud. Based on data from IBM X-Force, financial organizations and insurance companies have been at the top of this rating for the fifth year in a row. Experian called COVID-19 an "open door for scammers" and highlighted the five following threats as the most common cyberthreats of 2020:

- Coercion of victims to make payments (or bank transfers) by hacking corporate email or an individual email account (BEC/EAC)
- Theft of account credentials
- Opening of accounts based on fake documents
- Fraud when conducting transactions
- Fraud using fictitious or artificial identities

With potentially malicious programs already idly embedded in vulnerable systems, the security of many companies had already been compromised long before COVID-19. The pandemic simply provided the right conditions for launching overt attacks. The rapid development of digital services and the migration of many companies to the cloud have boosted the number of attacks against organizations and individual users who were unable to put enough emphasis on security during their attempts to get through the crisis.

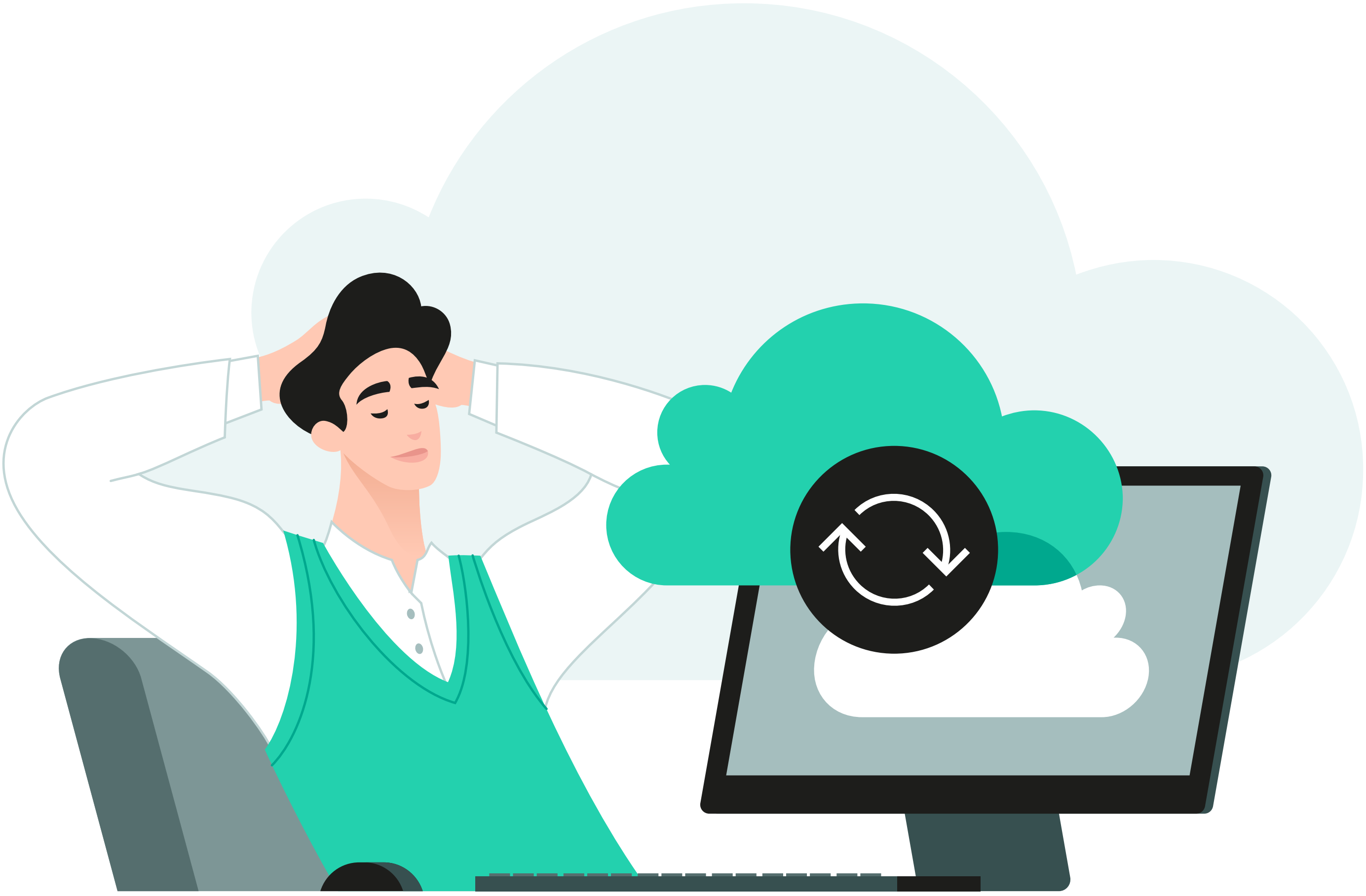
Companies are finally beginning to recover and are transitioning from mere survival back to sustainable development. The work process is returning to normal, and people are encouraged by the gradual ending of lockdowns. However, only one thing is certain: our past way of life is gone forever. Future development poses some serious tasks, one of which is the inevitable transition to digital technologies. To retain the trust of customers and partners, a business must not only provide convenient service but also reliably secure their infrastructure.

Investments and national assets

An opportunity for quick profit with minimal effort remains one of the most widespread forms of fraud. In the second quarter of this year, cybercriminals decided to diversify their assortment of techniques for getting easy money. Email recipients were offered the opportunity to invest funds into natural resources (oil, gas, etc.) or cryptocurrency secured by those resources. The subject of natural gas also popped up in the more traditional scams involving compensation. The cybercriminals even used the brands of major companies to make their offers seem more trustworthy. However, the websites receiving these investments quickly disappeared together with whatever money the scammers were able to steal from their victims while the page was active.

For the more distrustful victims, the cybercriminals created a platform in which the "Anti-fraud Department" promised to compensate the victims of cybercriminals, who were actually employees of the company. The cybercriminals assured the victims that compensation will be paid to those who gave the scammers more than 800 dollars. The scammers most likely assumed that many users would be curious as to whether or not they personally would receive compensation, so these attacks were not specifically targeted. Of course, the services of these so-called anti-fraud saviors were not free of charge, despite the free consultation they advertised. Any customer who filled out a questionnaire was asked to pay a small fee for the return of their money. After this fee was paid, these "consultants" just disappeared.

Another profitable scam was advertised as an opportunity for customer payouts. Using the logotype of a bank, the scammers offered active banking users the opportunity to receive dividends from investors with no strings attached. After filling out a questionnaire requiring their name, phone number and email address, the potential victim saw a message stating that a specific amount was ready to be paid. Although the cybercriminals emphasized that they do not take any commission for facilitating these payments, the user was required to provide their bank card details or deposit a small amount supposedly to verify that their account details were entered correctly. In other words, it all turned out to be the usual scam.

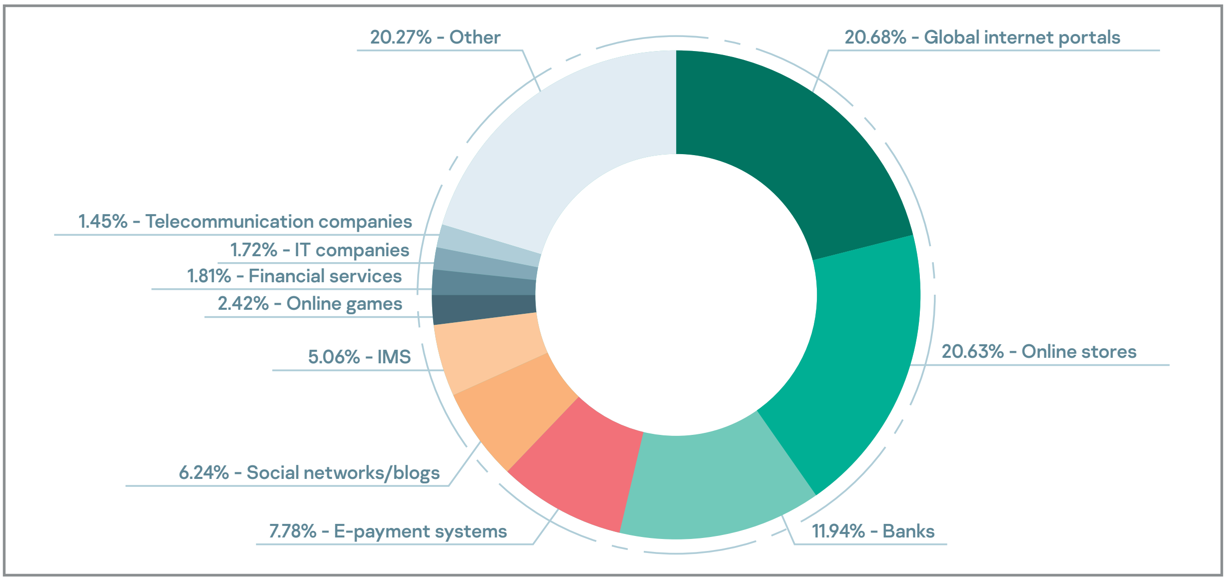


Organizations under attack

The rating of organizations hit by phishing attacks is based on detections registered by Kaspersky's Anti-Phishing component on users' computers. This component detects all pages containing phishing content that a user attempts to open by clicking links in an email or on the web, provided that these links are listed in Kaspersky databases.

Among organizations whose brands were most frequently used by cybercriminals as lures in their attacks, global internet portals are in the lead (20.68%). Online stores (20.63%) are very close behind in second place. Banks (11.94%) are in third place, while payment systems (7.78%) come in fourth. Fifth and sixth place are occupied by social networks/blogs with 6.24% and messengers (IMS) with 5.06%, respectively[17].

6



Screen Sharing

One of the most prevalent social engineering techniques still employed by cybercriminals is to persuade an unsuspecting user to allow the scammer to remotely control the user's Android device.

Standard remote administration tools such as TeamViewer and Anydesk were popular among scammers for a long time because they were legally distributed and therefore not detected by antivirus software (in contrast to malware).

However, the relatively small number of these tools meant that anti-fraud systems were able to easily reinforce their security against them.

As a result, this year showed a trend of scammers switching to screen sharing tools for their scams. These tools are provided by most communication applications such as Skype, Zoom, and Discord, which are so popular that their availability on a device and even their use during a session would not be identified as a definite threat.

This way, scammers are able to capture passwords and authorization codes, and directly control the actions of a user over the phone. These scammers are probably overjoyed by users who store their account data in text files (especially those who store all of their banking data in one file).

Some Android applications can be specifically identified when sharing your screen. For others, you can only determine whether or not it is running.

Screen sharing detection is aided by experience accumulated in iOS, in which the use of screen sharing tools has already been the most popular technique for remote intervention for a long time. However, screen sharing may also be indicated by extending your desktop to a TV or by other innocent activities.

By conducting a comprehensive analysis of session parameters, screen sharing settings and device data, the technologies for counteracting this threat can also be improved.

[17] https://securelist.com/spam-and-phishing-in-q3-2021/104741/

Overview of international requirements in finance, security and confidentiality

Three years after implementation of the international standards known as PSD2 and GDPR, just how effective are they?

Of all standards that we analyzed, none had such a large public resonance as the European Union's General Data Protection Regulation (GDPR).
The controversy surrounding its implementation in May of 2018 was debated on an international scale. However, the three most substantial takeaways from the implementation of GDPR are as follows:

- This specific regulation was responsible for public consciousness of a clearly defined concept of data privacy.
- It provides extensive and indisputable rights to private individuals.
- Last but not least, it extends beyond any specific territory or jurisdiction.

Three years have already passed since the implementation of GDPR and it is generally understood that this regulation was a true pioneer in the regulatory domain. Moreover, it has influenced many countries to follow the example of others, at least to some extent.

Without a doubt, GDPR and other international regulations have improved global awareness of data protection issues. This means that organizations need to pay attention to the latest trends in incident response and data disclosure prevention to avoid criticism for lack of transparency, and thereby avoid losing the trust of their customers.

As noted earlier, the behavior of consumers has changed. Now data protection issues are on everyone's mind, and business representatives should take notice. While previous security requirements had created difficulties for users and were viewed as obstacles on the path to innovation, now they are perceived as true allies of users. Nowadays, when cybercrime is on the rise, data protection is more relevant than ever and requires strict authentication in all possible forms. For payments, the 3D Secure protocol is an excellent example of this strict authentication.

Indeed, two decades ago, the first version of 3D Secure had been an important anti-fraud tool but was most often perceived as the main reason for failed purchases when used for e-commerce. Today's latest version of the protocol (3.2.2) leverages past user experience and keeps up with current trends in security (such as biometric data).

Most common bank-related scams in 2021

Evolution of the "Investor" social engineering scam

This scam, which was very popular in 2021, essentially involves convincing a bank customer that certain investments will be very profitable, asking them to take out a loan through the customer's online banking system and install special software such as cryptowallets, and offering to transfer the loan funds for a huge return of investment.

The main reasons for the enormous popularity of this scam were most likely the expansion of cryptocurrency exchanges and cryptowallets, and the lack of knowledge about this relatively new technology.

For banks, these scams were especially detrimental because they stole the bank's money instead of the private funds of the customer (which, according to legislation in many countries, the bank is not obligated to return if the customer actually provided their own passwords and codes). This increases the risk of unrecoverable loans.

Another especially popular social engineering technique employed this year was the relatively new "Police/FBI/government employee" scenario. According to this scenario, scammers introduce themselves as employees of law enforcement agencies and say that they need the victim's data (account number, balance, card number, text message code, etc.) to prevent or solve a crime.

This type of scam has better chances of success because it exploits the common fear people have when dealing with government and legal authorities.

Scammers also use the "double call" technique on victims. First they call and introduce themselves as a bank employee and attempt to scam the customer. If unsuccessful, they call again, but this time they introduce themselves as representatives of the police and say that they just detected potential fraud requiring police involvement for an investigation.

Offline fraud using bank cards with social engineering

1. A scammer may also call a bank customer and somehow persuade them to add funds to the scammer's card. To do so, the criminal has to convince the customer to tokenize the criminal's card on their own device and add money to it at the nearest ATM.

   In this case, the potential victims are fairly advanced users because they would have to be capable of tokenizing a card on their device.

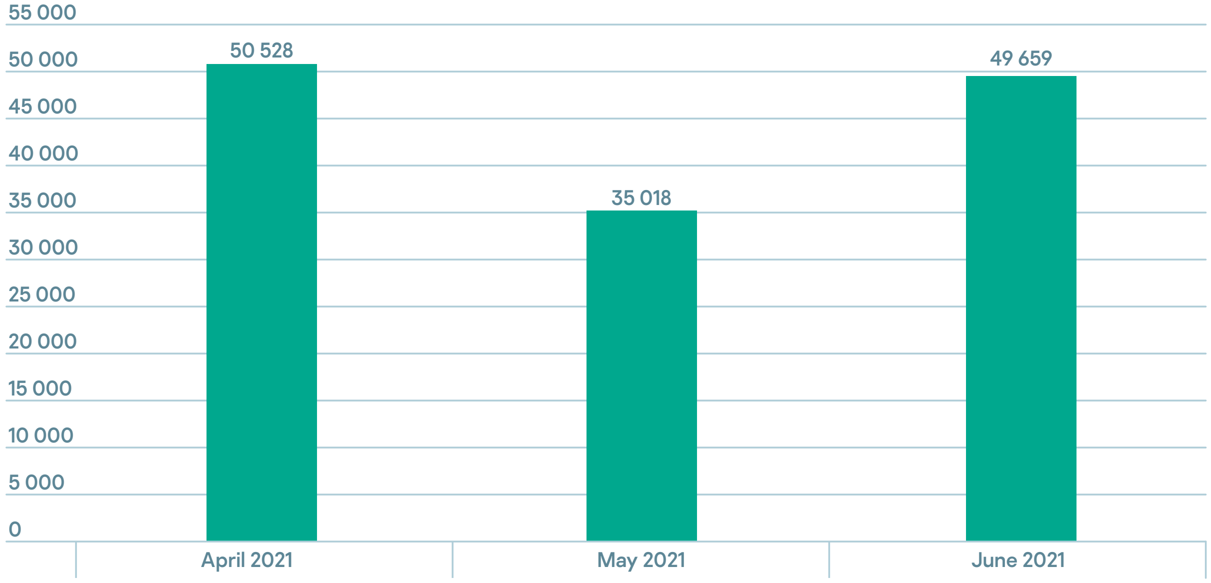
2. Bank accounts and cards issued to minors may be especially vulnerable to this scam. Despite the fact that young customers often do not have access to a bank account, they are still capable of withdrawing money and paying for services and products online. Scammers with social engineering skills can still extract some form of profit from even limited accounts with restricted functionality.

3. Voice assistants (also known as IVR systems) in banking apps can also be used to obtain data that is useful for social engineering purposes. A scammer just has to call the voice assistant of a bank (bot), introduce themselves as a bank customer and simply ask for their card number, account number, and amount of available funds while pretending that they forgot this information. After the voice assistant provides this information, the scammer can call the customer/victim and conduct their scam very convincingly by confirming the customer's bank account number, card number (or last 4 digits), and the amount of available funds.

Financial threat statistics

In the second quarter of 2021, Kaspersky solutions prevented the startup of malicious programs (one or more) designed to steal money from bank accounts on the computers of 119,252 unique users.

7



Source: https://securelist.com/it-threat-evolution-in-q2-2021-pcstatistics/103607/

Phishing in the banking sector

In 2021, one of the many financial organizations using Kaspersky Fraud Prevention detected a group of scammers that were creating phishing pages that spoofed pages of the bank's official website.

One page imitated the bank login page, including the text boxes for entering account credentials. After this data was entered, the user was prompted for the second authentication factor (text message code), then a different phone number was linked to the account.

This spoofed page (and its subsequent copies) also utilized masking for certain IP addresses. These types of phishing pages were blocked by the efforts of Kaspersky. A week and a half after being blocked, the scammer group created a new, almost identical page.

To detect the activity of this scammer group, Kaspersky Fraud Prevention applied new rules for detecting suspicious activity.

The following was detected:

- Use of a new device
- Linking of a new phone number
- Change in the device environment

In combination, these parameters helped accurately identify a fraudulent digital fingerprint of a device. Fraudulent devices were added to the denylist that is provided by Kaspersky Fraud Prevention functionality.

The Kaspersky Fraud Prevention team had assumed that these were cloud devices, but this was not actually confirmed. The ports of this financial organization were also scanned, but remote administration tools (RAT) were not detected.

The scammer group most likely used several of their own devices to implement this scam based on the fact that the cookies were not cleared and the device environment did not change. Then new devices appeared but the environment stayed the same.

Captcha is obsolete

For many years, it seemed like the only tool for combating bots was CAPTCHA, which is a mechanism that is supposed to help determine whether a program (bot) or an actual human is requesting a web service. It is still used by many websites, including online banking systems, pages of loyalty programs, and other websites that let you log in to a personal dashboard.

However, scammers have their own ways to bypass Captcha. One of them relies on so-called click farms. This process looks very simple. A large number of hired people click on a specific link, log in again, click the link again, and so on, indefinitely. This type of work is paid at the lowest possible rates. It used to be handled by bots, but it has required the involvement of real living people ever since the anti-fraud algorithms learned to detect bot activity.

A click farm employee is tasked with things like selecting fire hydrants as quickly as possible, deciphering some text, solving equations, or whatever task was designed by the creators of the specific Captcha to distinguish between a human and a robot.

Of course, not all cybercriminals can afford the services of click farms, so it would seem advisable to continue using Captcha at least as an added level of security. It's not quite that simple though. Users never considered the Captcha mechanism to be a convenient tool. It always left a lot of room for mistakes. For instance, a person could inadvertently click the wrong thing, fail to make out all the characters, or forget to switch their keyboard language layout. Even if a person enters everything correctly, Captcha is still perceived as an excessive obstacle that negatively affects the user experience (UX) when interacting with the resource.

Ultimately, Captcha not only fails to protect against cybercriminals, but also annoys and drives away legitimate customers. Therefore, it certainly seems like the right time to discard this obsolete security mechanism.

Fortunately, Captcha is not the only way to determine whether a human or machine is attempting to access a system. There are more state-of-the-art techniques that can be used. For example, Kaspersky Fraud Prevention has a technology called Advanced Authentication, which lets you avoid excessive authentication steps and makes things more convenient for legitimate users.

Basically, this technology analyzes hundreds of parameters that characterize the behavior of a user, including passive biometric indicators, information about the device being used for the authentication attempt, the device environment, and many other parameters. The machine learning technologies of Advanced Authentication enable a quick and accurate decision on whether or not to allow a user to log in, require additional verification, or restrict the user's access. This technology also lets you accurately determine whether a human or machine has requested a service[18].

Over the past two years, we have seen a multitude of personal data leaks, including multiple leaks from major companies.

The Dark Web has an extensive market for information about citizens of various countries with enough data to open a bank account, and this data can be obtained at a relatively cheap price. Therefore, it is economically feasible for cybercriminals to utilize the data of an unsuspecting person to open a new bank account for the purpose of transferring even a relatively small amount of money.

How to combat the use of money laundering mules

For any kind of bank fraud, criminals need to somehow transfer the funds to legitimate bank accounts or otherwise launder the money into "clean" cash. To cover their tracks, they use so-called money mules, which are people who receive the unlawfully acquired money in their own bank accounts and then transfer it further down the line.

Previously, scammers primarily used the accounts of ordinary bank customers for their money laundering purposes. Now, cybercriminals frequently open accounts specifically for money laundering, and these accounts are getting more and more numerous each day.

The pandemic dealt a huge blow to businesses throughout the entire world. Some companies were forced to close, and employees lost their jobs. Many countries are attempting to stabilize the situation by allocating funds to assist businesses and private individuals. Many banks have simplified the dispersement of loans for emergency use to help those who need it as quickly as possible.
Some also simplified the verification process for dispersement of "pre-approved loans" (provisional credit).

For sophisticated money laundering schemes, cybercriminals use some very intricate tricks that may include automation tools, proxy servers, remote administration tools, and the TOR network. This is all necessary to make new schemes sufficiently different from previously identified fraud and money laundering systems. To properly combat these types of advanced methods, you need specialized tools for rapid cross-channel detection of these schemes.

Their quest for more and more money has led to a significant increase in the number of so-called money mule accounts. Using that same leaked personal data, cybercriminals take out a loan, transfer the funds to a newly opened account, then withdraw the cash and disappear.

[18] https://www.kaspersky.com/blog/rsa2021-captcha-is-dead/40054/

These tools are provided by Kaspersky Fraud Prevention.
This solution analyzes information about devices that are used by cybercriminals to connect to mule accounts, registration patterns, and a multitude of other indicators that can be used to determine whether or not a customer is involved in an illegal scheme[19].

Peer-2-Peer payments

One of the main sources of user data for fraudulent P2P transfers is phishing. Hundreds of new phishing pages appear each day. Although some are quite unprofessionally done, others were created with such high quality that it can be very difficult to distinguish them from their spoofed web pages without a detailed analysis. Of course, we are talking about new designs and not just a copied payment page from some bank or aggregator, even if it's just an iframe on a search results page. A domain name that seems to imitate some official resource and an SSL certificate issued a few days or weeks ago by a free Certificate Authority should be enough red flags to tell you not to make any payments on these pages. Most enticement scams are designed to lure users who want to either save money or acquire some easy money. This could be a sale of trendy shoes with a discount, an offer for a better tax refund, a tempting get-rich-quick scheme, or a low-priced iPhone. The psychology of user behavior is closely linked to financial competence and knowledge of cybersecurity principles.

Other sources of user data are leaks and insider attacks. Leaks happen everywhere, including among payment providers. This information frequently contains not only bank card details but also phone numbers and/or email addresses. Scammers can obtain many different leaked databases from various sources. Even if the leaked data from a payment provider lacks phone information but has an email address, you can easily correlate other leaked databases to match an email address to a phone number. You should also consider potential insider leaks from banks, which unfortunately happen from time to time. Although they are not quite as common as other leaks, the quality and detail of user information in these cases is more relevant and fruitful for fraud.

In contrast to traditional cases of carding, P2P schemes have a recipient that can be used for subsequent transit of funds to target accounts.

In the third quarter of 2021, the Kaspersky Anti-Phishing system stopped 46,340,156 attempts to open phishing links. Approximately 3.56% of Kaspersky users encountered this threat.

Source:
https://securelist.com/spam-and-phishing-in-q3-2021/104741/

Drop cards are used in most cases. Scammers normally obtain these cards by duping individuals with low financial and/or legal knowledge, or through the help of people knowingly participating in these schemes. A victim or accomplice is asked to apply for a debit card using their own identification information, and then give that debit card to a third party. If you don't understand the risk posed by this activity, this request may actually seem tempting because it doesn't cost anything to register a card and you will receive some type of compensation from the third parties who will use your card. However, if that card receives a money transfer that is later determined to be fraudulent, the card owner will be criminally liable as an accomplice. Recruiters for this scheme often search social networks to find people experiencing financial difficulties.

Another variant of this scheme is to recruit willing "account mules" who make their bank accounts available for money laundering. Instead of giving their bank card to third parties for a card drop scam, these mules agree to accept transfers from time to time and get to keep a small portion of those transfers. The recipient's compensation in this case is a commission instead of a one-time reward. These account mules are recruited in the same way as drop mules.

The basic scenario for a fraudulent P2P transfer using social engineering occurs as follows. Scammers can obtain user bank card details and phone numbers in several ways, including through phishing, insiders within banks, and data leaks. During this type of attack, the scammer attempts to transfer a specific amount from the user's card to a drop card or mule account. Social engineering in this case can include various scenarios, whether it is a call from a bank's security department, police officer, or employee of the Central Bank from a spoofed phone number.

The likelihood of a successful attack under this scenario strongly depends on how much the scammer knows about the user's bank account, and this knowledge is more reliable if the scammer received the data from a bank insider. In all other cases, everything depends on the financial greed of the scammer and their level of preparation. After all, even successfully employed social engineering techniques by a The second type of scheme is more difficult to implement and utilizes a well-prepared platform with a phishing resource. If the platform attempts to directly interact with the payment gateway of the acquiring bank, bots are used to complete the P2P payment, or information on this gateway's API is used to facilitate the payment.

[19] https://www.kaspersky.com/blog/rsa2021-detecting-money-mules/40083/

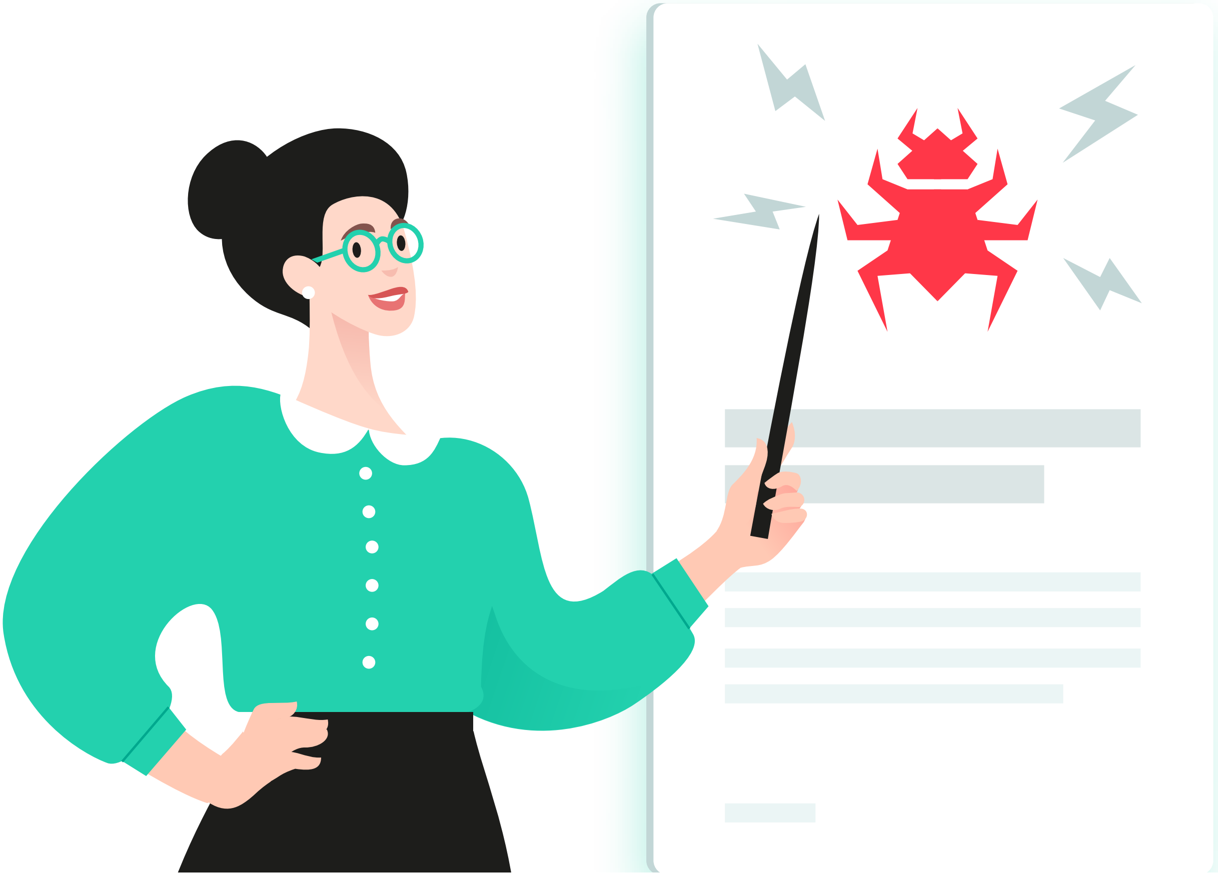
Acquiring banks and major payment aggregators (such as Yoomoney, Qiwi, and ChronoPay) are currently not servicing various high-risk resources (including scam resources) due to current Central Bank requirements. However, aggregators/facilitators (which are terms with a flexible interpretation in this context) can connect to acquiring banks and to our payment aggregators and make payments through them if they reside outside of our national jurisdiction. Although their trustworthiness is fair to middling, our acquiring banks/aggregators are more than happy to make some money off commission.

A user who falls for the latest link with a tempting offer will end up on a page that sells a product at an unbelievably low price while offering cash back from the bank for utilizing its services or a tax deduction. If card details are entered to purchase the item, the funds will be debited from the card. If cash back or a tax deduction was selected, a message will inform the user that the specified card will be credited.

After a user has entered their data and clicked the "Submit payment" button, the phishing resource uses a bot or API facilitator to send the request to the payment gateway. However, the request is actually for a P2P transfer from the user's card to the scammer's card. Then the user is redirected to a page that requires entry of a one-time password to successfully complete 3DS. The user enters their one-time password and money is debited from their card, Of course, they don't actually receive the item, cash back, or tax deduction.

For fraud monitoring systems at acquiring banks that evaluate the financial indicators of operations, this type of payment may look like a transfer to a recipient in an external bank from a new card of an external issuer for this P2P service. According to the latest recommendations of the Central Bank, a risk assessment must be conducted on the recipient's card based on the size and frequency of the credited amounts.

When bots are used and the acquiring bank carrying out the payment has a session data analysis system installed in addition to a transactional fraud monitoring system, this type of payment may be marked as suspicious based on a user session analysis that detects distinct attributes indicating an elevated risk of the operation. Such attributes include the use of anonymizing tools and an attempt to conceal one's actual location on the network, an attempt to manipulate a device fingerprint, bot activity, anomalous behavior of a user on the page, and an unreliable reputation of the IP address, among many others.



Fraud beyond finance

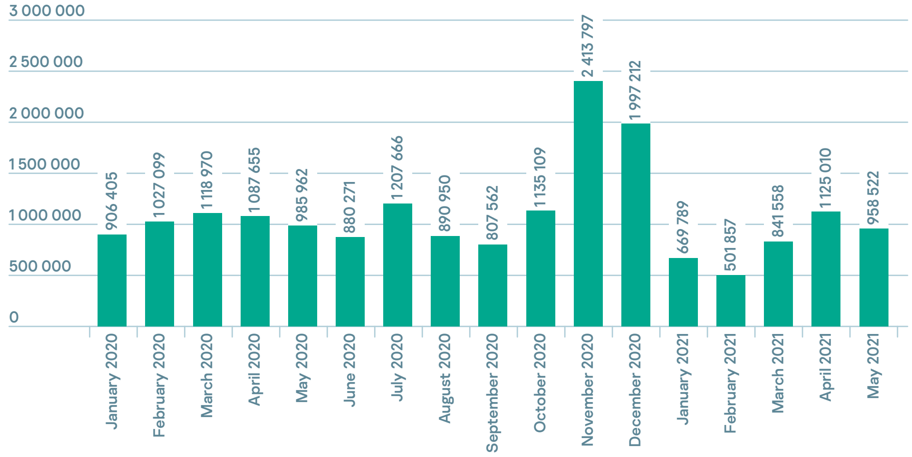
We previously found that the migration to remote work-from-home systems resulted in a more than 50% increase in the number of attempts to open malicious websites that exploit a user's interest in gaming. A year after publication of our preceding report, we once again studied the landscape of threats aimed at gamers and the gaming industry.

Quarantine and video games

The number of gaming enthusiasts is steadily growing each year, which is confirmed by the statistics of active players on the Steam platform. After the spike in May of 2020, which we discussed in our last report, the number of active Steam users has slightly decreased but still has not returned to pre-Covid levels.

Accordingly, cybercriminals continue to attack gamers. The statistics of Web Anti-Virus detections on websites whose names are generally associated with the gaming theme (for example, the website name contains the name of a popular video game or gaming platform) show a very noticeable spike in November-December of 2020. People involved with the gaming scene generally think that this spike was related to the release of Cyberpunk 2077, when cybercriminals were actively exploiting this hot topic and trying to scam impatient gamers any way they could.

8



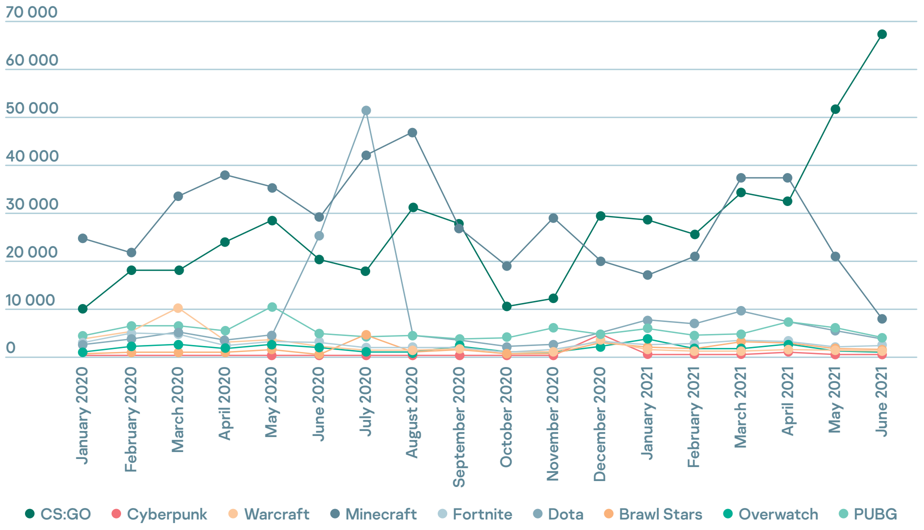
Number of web attacks exploiting the gaming theme from January of 2020 through May of 2021. Source: Kaspersky Security Network (KSN)

Gaming-related phishing scams are distinguished by their impressive diversity. Right now we are seeing more and more online events related to gaming, which enables cybercriminals to continually try new scenarios to obtain user data.

Source: https://securelist.com/game-related-cyberthreats/103675/

Quarterly dynamics show that the number of users who were victims of gaming-themed cyberattacks increased at the beginning of the pandemic but decreased in the first and second quarters of 2021 compared to the first and second quarters of 2020 when more users were trying to play games for free during lockdown. A different trend is being observed for threats related to mobile games. The number of attacked mobile users at the beginning of the pandemic increased by 185% and only decreased by 10% in the second quarter of 2021. This means that cybercriminals are still actively exploiting mobile threats.

9



Number of web attacks exploiting the gaming theme from January of 2020 through May of 2021. Source: Kaspersky Security Network (KSN)

To avoid becoming the victim of cybercriminals, gamers should be vigilant. Do not always trust emails that were supposedly sent from gaming services, do not enter your account credentials on suspicious resources, and download games only from official sources[20].

Dating apps

The pandemic and its resultant restrictions led to an increase in popularity of dating apps. For example, in Tinder, the total number of swipes during the past year increased by 11%, while the daily number of swipes reached 3 billion for the first time in March of 2020. This is not surprising when considering that a significant percentage of places where you could hang out and meet new people were locked down multiple times in 2020 and in the beginning of 2021.

Unfortunately, the increased activity of users in dating apps could also increase their associated risks. Users could encounter the following threats in particular:

- Identification of a user by third parties. Unauthorized individuals could obtain access to the personal data of a user, including their real name, actual residence, work location or place of study, and later use this information for stalking or doxing.
- Data theft for account takeover.
- Fraud. The most popular scams include requests to transfer money for various reasons, requests to send nude pics, which would then be used for blackmail, and forwarding of links to phishing websites containing a form to enter bank card details.

The likelihood of becoming a victim of these threats largely depends on the security measures that are implemented in the specific application and its vulnerabilities.

The developers of dating apps are beginning to put more focus on the security of user data. After finding out that third parties were able to intercept user messages in four out of nine of the apps that we analyzed in 2017, we are encouraged by the fact that all nine of those dating apps are using secure data transfer protocols in 2021.

If developers continue in this direction, sooner or later the online dating scene will become much safer than it is right now.

In regard to the current situation, we offer the following recommendations on how to secure yourself when meeting people online:

- Do not publish detailed information about yourself (last name, workplace, pics with friends, political views, etc.).
- Manually indicate your general location if possible.
- Use two-factor authentication.
- Delete or hide your profile if you no longer use the dating app[21].

If a user allows their relative distance to be displayed, it is not difficult to calculate their location in most services through triangulation and location spoofing programs.

Out of the four studied dating apps that require your location data, only two (Tinder and Bumble) have countermeasures against the use of these programs.

Source:
https://www.kaspersky.com/blog/mwc21-online-dating-apps/40628/

[20] https://securelist.com/do-cybercriminals-play-cyber-games-in-quarantine-a-look-one-year-later/103031/

[21] https://securelist.com/dating-apps-report-2021/103000/

Brute-force attacks and bonuses

Bonuses and other benefits of loyalty programs provide a lot of opportunities for scammers. They can accumulate these benefits for resale or use them to make purchases that can then be resold or kept for their own personal use. Kaspersky Fraud Prevention has previously detected a lot of these situations, which even included a massive purchase of diapers from an online store.

Now, when analyzing logs in a session, Kaspersky Fraud Prevention frequently detects blatant attempts to hack accounts by using brute-force attacks, which sometimes reach up to 30 unsuccessful login attempts. Scammers try all the possible variants of passwords and user names to hack accounts either manually or by using bots.

Attacks on online stores. Promo codes and multiple accounts

In one of the largest online stores, multiple forms of fraud were detected at the same time:

1. Attempts to brute-force promo codes by using an algorithm to try all possible combinations (you should pay special attention when the number of attempts exceeds 10).

2. Use of multiple accounts to research and later resell this data on the web.

There are often multiple accounts on the same device, but this is not necessarily evidence of fraud. However, there are users who have multiple accounts and use them for a long time without making any purchases. These accounts are most often used to view the prices and quantity of items in stock. This information is valuable for competitors and can actually be sold on the Internet. However, this information is usually collected with the aid of bots and algorithms because it takes too much time to collect this data manually.

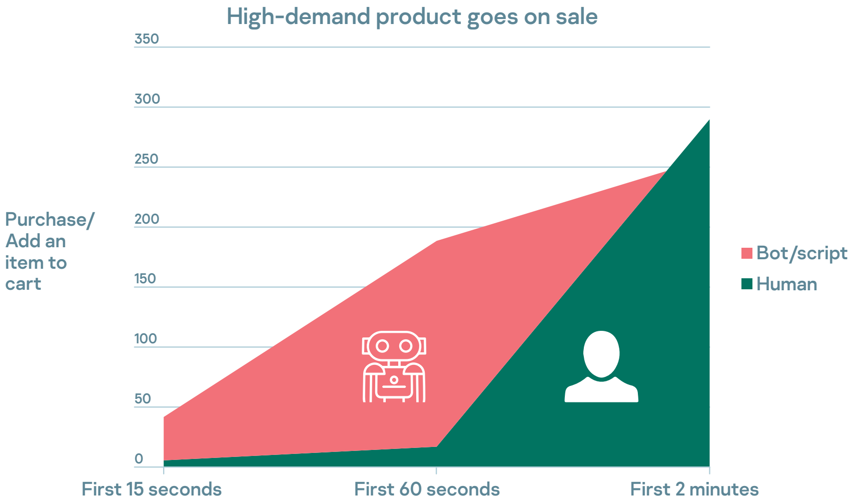
Fraud in online auctions

Online auctions, bidding procedures, and online sales with limited resources and tight deadlines to reserve those resources provide conditions that are ripe for fraudulent activity.

One example is the online sale of a high-demand, low-supply item such as brand-name athletic shoes. They are put up for sale at 00:00, and by 00:02 they are all sold out. Systems like Kaspersky Fraud Prevention let you identify bot activity and algorithms that make lightning-fast purchases.

This activity is identified based on predefined rules for detecting bots. One of the main parameters for these rules are clicks:

10



Passive biometrics for detecting fraud

Scammers are continually improving their tools to counteract detection technologies. Fraud detection methods that are based on any fixed set of attributes (signatures) will work only until those attributes are exposed.

The same is true for user behavior in a session, which is basically a sequence of discrete actions that can be deduced by a fairly diligent cybercriminal who can then use that information to confuse anomaly detection algorithms.

Therefore it is not surprising that anti-fraud systems are now resorting to more sophisticated sources of data associated with the specific control signals of a user. On a web resource, this data essentially consists of mouse movements, clicks, and keyboard inputs, which provide the capability to create specialized technologies that help identify remote control activity, for example. Unfortunately, however, mouse movement simulation tools are also being developed. In some cases, they are virtually indistinguishable from the movements of a real user.

Anti-fraud systems on mobile devices have significantly more capabilities. Nowadays, the standard set of sensors includes touchscreen sensors, accelerometers, gyroscopes (for angular rotation), proximity, illumination, and rarer sensors such as a magnet meter. Even if it is possible to simulate the readings of these sensors, cybercriminals are still having an extremely difficult time figuring out how to do this.

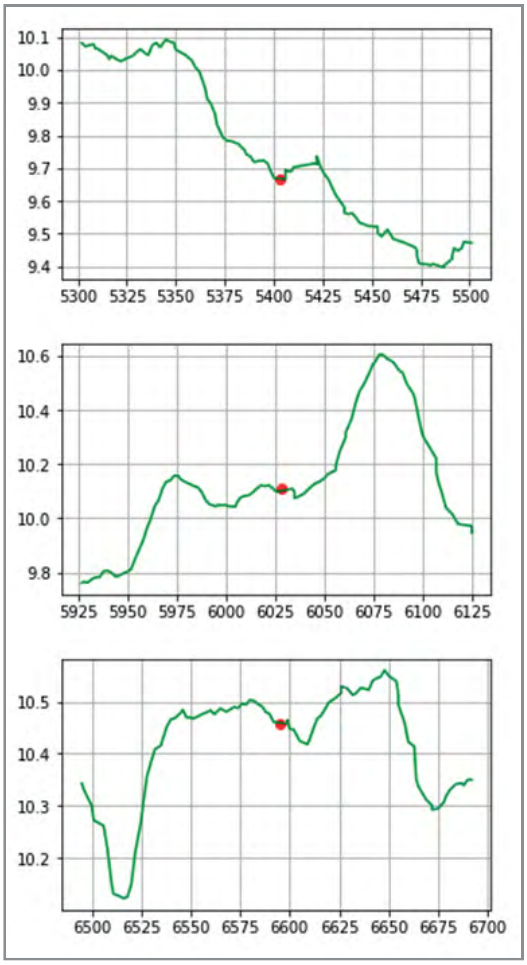
The availability of a multitude of sensors enables the implementation of passive biometrics technologies, which identify a user based on background activities. This is different from active biometrics, which require a specific action for identification, such as a fingerprint scanner or facial recognition.

The potential applications of this technology are quite extensive. For example, you can use it to distinguish a human from automation and remote control tools, accurately identify a specific person, and even distinguish phone movement patterns that are typical for anomalous scenarios (as one of the detection factors used together with other technologies). On the other hand, this technology is difficult to develop and implement due to the substantial differences between device sensors, the need to process large amounts of data and use machine learning technologies, and the need to minimize its impact on device performance.

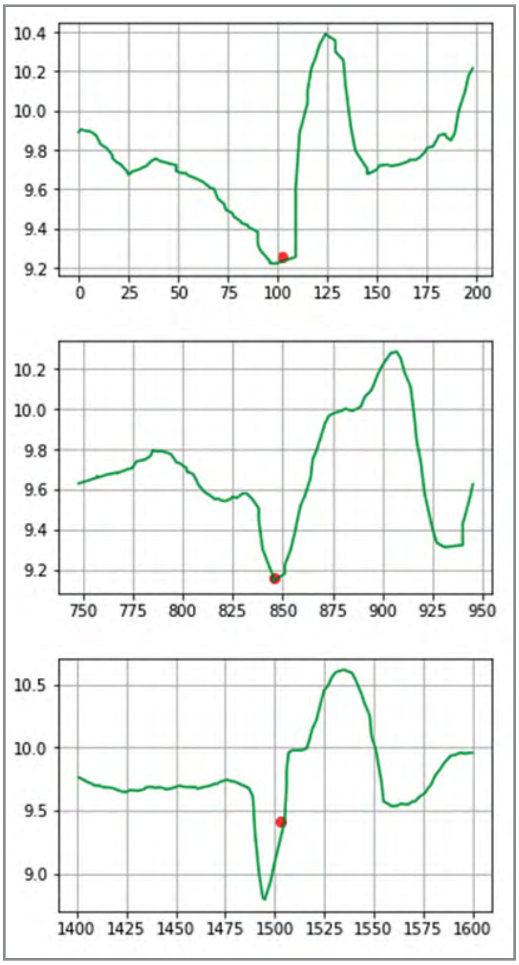
Real-world use of our product has demonstrated good results from combining passive biometrics techniques with analysis of data on the specific device and its environment.

For example, a fairly common social engineering scenario involves asking the victim to install a remote administration tool. In this case, the Kaspersky solution would analyze the call (duration of the call, reputation of the phone number) simultaneously while searching for biometric anomalies.

11



Pattern of user activity



Remote control event based on an analysis of mobile phone sensors

Looking ahead…

Emerging threats

Criminals will continue targeting technologies that support **remote and hybrid working** patterns - specifically VPN and remote access services - as businesses continue to rely on these services. These are low hanging fruits for unsecure environments as successful attacks give criminals remote access to their victims without having to deploy any malware. And as people slowly return to the office, this may leave these supporting technologies unattended, potentially giving criminals further opportunities. In a similar vein, attacks against **cloud** environments will likely continue and have a greater impact as more organisations move towards "Cloud-First" strategies. The operational pressures caused by cloud downtime will likely cause enough pressure to force companies into paying ransoms. And as the digital supply chain continues to expand, criminals will continue to target it for bigger payloads (e.g. attacks on Managed Services Providers or digital services suppliers).

We can also expect **more elaborate ransomware** attacks involving the active recruitment of employees to help with ransomware campaign[23], rendering insider threat management a priority for the foreseeable future.

COVID-19 will also continue to present opportunities, and we can expect that government deployed applications (e.g. tracking, travel, identity), which hold a lot of valuable and sensitive data, will increasingly be targeted. Successful attacks will result in data becoming accessible to criminals in underground markets, with the likely cascading effect of more phishing and ransomware campaigns.

As Increased collaboration and professionalisation of criminal operations continues, **money laundering** schemes are likely to further develop over the coming years.

On the road to success

Whilst the attacks that were observed in 2021 were in themselves not new, the way in which they were conducted is worrying: the increased cooperation and professionalism of criminals, enabling them to deploy efficient "operational" processes is something to watch out for, and learn from. As the fraudsters' ultimate aim is to monetise the proceeds of their crime, in response, governments and businesses should aim for effective international coordination of law-enforcement, regulations and cooperation with the private sector to be able to investigate money trails. Only then will they have a fighting chance to disrupt, at least, ransomware operations.

As for more recommendations for businesses, these will be no different to those given in previous years: implementing security fundamentals, such as multi-factor authentication, patch and vulnerability management, hardening of systems and applications, classification and protection of data, and of course employee education, will go a long way.

[23] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

IT Security News:
www.kaspersky.com/blog
Cyber Threats News:
www.securelist.com

@KasperskyFP

www.kaspersky.com

TOP 100

Kaspersky Fraud Prevention is among the top 100 best inventions of 2017 according to Rospatent: https://kas.pr/100best

Kaspersky Fraud Prevention Automated Fraud Analytics [156555] included in the Register by Order of the Ministry of Communications of the Russian Federation dated November 19, 2019 No. 742, Appendix 1, No. 72, registry number 5954

Kaspersky Fraud Prevention Advanced Authentication [156556] included in the Register by Order of the Ministry of Communications of the Russian Federation dated November 19, 2019 No. 742, Appendix 1, No. 73, registry number 5955

WORLD BRANDING AWARDS
BRAND OF THE YEAR