BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 69(4), 2021, Article number: e137933
DOI: 10.24425/bpasts.2021.137933

SPECIAL SECTION

The impact of the COVID-19 pandemic on cybercrime

Agnieszka GRYSZCZYŃSKA *

Chair of Informatics Law, Faculty of Law and Administration, Cardinal Stefan Wyszyński University,
ul. Wóycickiego 1/3, bud. 17, 01-938 Warsaw, Poland

Abstract. The COVID-19 pandemic is accompanied by a cyber pandemic, involving changes in the modi operandi of perpetrators of various crimes, and an infodemic, associated with the spread of disinformation. The article analyses the impact of the COVID-19 pandemic on cybercrime and presents the latest research on the number of cybercrime cases in Poland and their growth dynamics. It determines the factors that contribute to the commission of a crime and prevent easy identification of criminals. It also suggests the legal and organisational changes that could reduce the number and effects of the most frequently recorded cyberattacks at a time of COVID-19. Particular attention is paid to legal problems of the growing phenomenon of identity theft, and the need to ensure better protection of users from phishing, including through education and proactive security measures consisting in blocking Internet domains used for fraudulent attempts to obtain data and financial resources.

Key words: cybersecurity, cybercrime, social engineering, phishing, identity theft, COVID-19.

1. INTRODUCTION

The COVID-19 pandemic is not just a medical problem; it is accompanied by other undesirable phenomena affecting our safety, health, or life. Actions aimed at limiting the spread of the virus have influenced working and learning methods as well as the implementation of public tasks. The sudden changes and the widespread use of remote working or learning have made cybersecurity problems more visible. The pandemic has also affected the way criminals act. For cybercriminals, the lockdown has been primarily an opportunity to increase the effectiveness of attacks based on social engineering. New attack vectors have appeared very quickly, and previously used scenarios have been adapted. Criminals have been using lockdown to attack large corporations, small businesses, public administration authorities, hospitals, or individuals. They have different motivations and distinct goals. Lockdown has increased the number of both cyber-dependent crimes and cyber-related crimes. Furthermore, criminals who used to commit crimes outside of cyberspace have changed their modus operandi due to restrictions of trade or movement and started to operate online, following their victims.

The analysis of the impact of the COVID-19 pandemic on the crime landscape includes the dynamics of changes in scenarios of attacks on online users, factors that make it easier for criminals to commit crimes, and factors that make it difficult to identify the attackers and bring them to justice.

2. MOST FREQUENT ATTACKS AMID COVID-19

The duration of the COVID-19 pandemic makes it possible to analyse the variability of attack scenarios, especially those aimed at monetisation and based on social engineering.

The analysis of reports concerning online security and information systems in Poland and worldwide shows a large number of incidents related to broadly taken computer frauds and distribution of malware [1–3]. In the early days of the pandemic, when a shortage of protective and hygiene measures was observed on the market, there were many frauds whose victims mismanaged their property because there were offered protective measures (including masks), hygienic products, pharmaceuticals, medications, fake corona home testing kits or even COVID-19 vaccines at online auctions or fake online shops. Paid orders were never delivered or customers would receive non-conforming, counterfeit, and/or sub-standard products [4]. National and international proceedings against such criminals are underway [5]. During the months that followed, with the balancing of supply of and demand for protective measures and hygienic products, the number of fake auctions or online shops still remained significantly high. Restrictions of movement and limits on the number of people who can stay in a shop at the same time have encouraged many to order products online. The number of fake online shops is invariably high, offering mainly electronics, children's toys, and branded clothing [6]. These offences can be classified as typical frauds under criminal law (Article 286 § 1 of the Polish Criminal Code) [7], only facilitated by the use of the Internet and information systems. Fraudulent fundraisers for the health sector, including financial support for hospitals and medical staff, to establish temporary hospitals, purchase ventilators or protective equipment, but also support patients and their families, should be considered as another type of typical fraud [8]. The same legal qualification will apply to the attacks referred to as Nigerian scams and Business Email Compromise (BEC) the scenarios of which have also been adapted to the current pandemic situation.

The analyses of criminal liability of people running fake online shops very often overlook three extremely important aspects: money laundering, unauthorised processing of personal data of victims, and commission of other additional crimes to

*e-mail: a.gryszczynska@uksw.edu.pl

Manuscript submitted 2020-12-31, revised 2021-05-04, initially accepted for publication 2021-06-06, published in August 2021

the detriment of victims. The majority of cybercrimes aiming at monetisation involve money laundering as the underlying offence. Studies carried out by the author of this article have shown that, in most of the examined fake online shops, the so-called money mule account was given to customers to make payments for purchased goods. An extensive set of tools necessary for laundering money from crimes includes a SIM card registered using the money mule's data, login credentials to electronic banking, and a selfie with an identification document. Some money launderers also need an ATM card. Criminals extensively exploit data obtained from money mules: they set up accounts on cryptocurrency exchange platforms or even open businesses. Those searching for people who would open bank accounts used in money laundering sell access to such accounts via the Internet to various criminal groups. Funds obtained from victims that are credited to the mule's account are then transferred to cryptocurrency exchange platforms, withdrawn in ATMs, and then deposited via Bitcoin ATMs. These activities make it considerably harder to track the money flows and identify their criminal source.

Another aspect that cannot be overlooked is the unauthorised processing of data of the people who shop in fake shops, and the use of such information by criminals to conceal their own identity. Criminals use the data of customers who set up accounts in fake shops to pose as such people. If the scope of the information collected by criminals is significant, buyers' data are used in fraudulent loans or credit applications. Furthermore, very often people who make purchases in a fake shop receive a link leading to a website claiming to be a billing agent or a bank where the customers are tricked into sharing their e-banking login credentials. An attack using the so-called "fake payment gateway" is one of the most frequent attack scenarios recorded in Poland in 2019 and 2020. Incidents included in this category have been detected since mid-2017, but since 2018 the number of domain names registered for this scenario has significantly increased: from a few per day to several dozen per month [9]. Thus far, different ways of persuading victims to enter a fake payment website have been observed. One of those includes publishing offers on classifieds websites or social networking sites to sell products at very attractive prices or give away various products for free. Another is creating websites of fake online shops that offer attractive prices (e.g. arya-toys.com, kidparadise.pl). People who made purchases there receive a message from criminals via e-mail, text, or instant messenger (e.g. Messenger) with the information regarding the payment and a link to a fake page posing as a website of a billing agent and then of a bank. The so-called "fake payment gateway" model has also used data from hacking into the customer database of the online shop Morele.net Sp. z o.o. (related domains: platnosci-morele.online, platnosc24.com) [10]. Hyperlinks leading to fake payment websites are also sent out in bulk without prior adjustments to recipients of the attack scenario. Criminals usually send text messages, saying that a surcharge is necessary for shipment, order, or electricity bill.

The criminals responsible for the "fake payment gateway" attacks have quickly adapted their social engineering techniques to the pandemic. As early as on 13 March 2020 (i.e. two days after the announcement of the Regulation restricting the operation of public and non-public educational facilities due to COVID-19 in Poland [11]), the following text messages were distributed: "We would like to inform you that, under the coronavirus special purpose law, funds on your bank account will be transferred as provisions to the National Bank of Poland. Log in to keep PLN 1000" and "According to the coronavirus special purpose law, all Polish citizens will be vaccinated. The vaccination cost after reimbursement is PLN 70. Pay to avoid queues." In both attacks, criminals used the domain name https://dpdoplata[.]org registered previously to send text messages asking for a shipping surcharge. The attack involving the scenario based on the mandatory COVID-19 vaccination also used the domain name posing as the National Health Fund (https://nfz582[.]com/1259). On 27 March 2020, criminals distributed information on arrears to the Tax Authority. This attack also took into account the current situation: on 26 March 2020, the Sejm received form no. 299, which is the Government's bill to amend the Law on special solutions to prevent, counteract and combat COVID-19 [12]. The page impersonating the gov.pl website, available at https://gov-24[.]com, redirected to another website posing as PayU S.A., available at https://paqu24[.]com. In April and May 2020, the most frequent scenarios that aimed at tricking customers into sharing their e-banking login credentials and authorisation codes involved criminals posing as entrepreneurs providing transport, shipping, or postal courier services, sending text messages with the information that a surcharge was necessary for parcel disinfection (sample domain names: eplatnosc.com, paczkadpd.com) [13]. If using e-banking login credentials, criminals establish that significant funds are available on the victim's bank account, they usually move to a SIM swap fraud. This attack requires obtaining a duplicate of the victim's SIM card in an unauthorised manner. Many procedures are completed on a remote basis during the pandemic and this has led to a drop in the level of security, in particular as regards the customer identity verification. This has made identity theft and extortion easier for cybercriminals.

Criminal groups tricking people to log on to social networking sites adapt their attack scenarios extremely quickly. Wanting to attract users to a fake login site, cybercriminals first create a website posing as an information website. There, they publish hair-raising news about kidnapping, rape, larceny, or car accident. Under the description of the alleged event, there is information that a surveillance video is available. Since the material is supposedly drastic and only intended for adults, it is necessary to verify age by logging on to the social networking site (Facebook.com) to watch the video. Once the victim's data have been intercepted, their account is used, among others, to intercept other accounts, publish fake recruitment information (for unauthorised collection of personal data or finding people involved in money laundering) and commit fraud. The most common scamming scenario involves a request sent to the victim's circle of friends, asking to borrow a small amount of money or pay for an order and provide a BLIK code for this purpose. With the introduction of restrictions related to the COVID-19 pandemic, the scenarios based on social engineering techniques used before have been replaced with websites

containing attention-grabbing information about the pandemic. Sample headlines include: "Doctor from a Warsaw hospital about the increasing number of infected people in Poland" or "Child kidnapped from a hospital for communicable diseases. [video]". Sample domains used in this attack scenario include efakty-koronawirus24[.]pl or koronainfo24[.]eu.

The COVID-19 pandemic has also given rise to disinformation about the epidemic, its causes, treatments, or resultant threats. The media and literature are increasingly referring to this phenomenon as infodemic [14]. Flooded with different messages and sensational reports, but also lacking access to reliable sources of information, Internet users have become susceptible to disinformation and fake news.

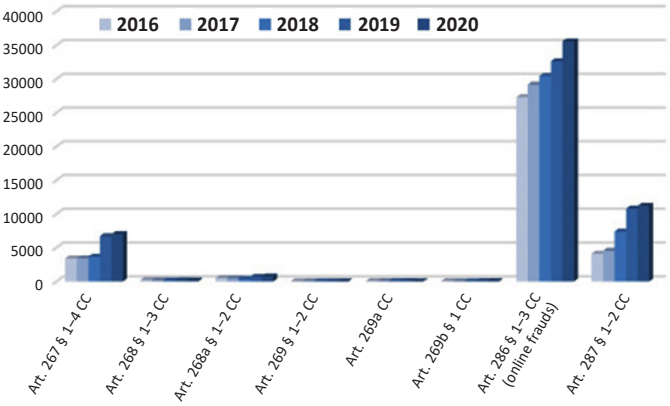
Since November 2020 when the COVID-19 vaccine became available, there has been a significant increase in the spread of disinformation about the vaccine's side effects, using shocking news about the vaccine and its negative effects to intercept credentials used to log in to social networking websites. In the attack scenarios observed in December 2020, users were encouraged to fill in a form to opt out of child's vaccination against COVID-19 and, to this end, provide their e-mail account login credentials.

Perpetrators of cyberattacks have various targets, including pharmaceutical companies, research laboratories, or supply chains used for vaccine deliveries. Some of them aim at gaining profits (e.g. ransomware attacks) [15], but other incidents are attributed to cyber-espionage groups being part of intelligence services. In July 2020, the United Kingdom's National Cyber Security Centre (NCSC) published a report detailing recent Tactics, Techniques and Procedures (TTPs) of the group APT29, which has targeted various organisations involved in COVID-19 vaccine development in Canada, the United States, and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines [16]. In December 2020, the European Medicines Agency reported a cyberattack and the possible access to documents relating to a COVID-19 vaccine [17].

It should be noted that, in connection with the pandemic, the outcomes of cyberattacks might be much more serious than they were before. Disinformation campaigns cause an increase in the level of social dissatisfaction and result not only in failure to abide by safety rules, but also cause physical attacks targeted at those who are sick or quarantined, and street riots. The COVID-19 has made organisations like hospitals, governments, and universities, more conscious about losing access to their systems and more motivated to pay the ransom. The heavy burden on healthcare makes the effects of ransomware attacks aimed at hospitals or research laboratories can become a direct threat to the life and health of many people. Given the status of the pandemic as well as the significant risks to patients' lives and well-being, the cyberattack on Brno University Hospital, was considered an attack on a critical infrastructure [18], whereas due to a patient's death in connection with a ransomware attack, German authorities are investigating the perpetrators on suspicion of negligent manslaughter [19].

It is extremely difficult to make quantitative analyses of cybercrime in Poland. Law enforcement authorities do not publish up-to-date statistical data showing the number of initiated proceedings or the number of acts identified for each legal qualification. The research is based on the data obtained from the National Police Headquarters. The data originate from police systems and can provide a basis for inference. It should be noted, however, that the legal qualification (the basis for initiating proceedings) is determined by the unit handling the case. A detailed analysis of descriptions of prohibited acts indicates that different units conducting the proceedings adopt different grounds for initiating proceedings in identical cases, which may result in slightly distorted statistics. Most of the analyses relating to the issue of cybercrime cover the acts committed under the articles of Chapter XXXIII of the Polish Criminal Code (CC), i.e. crimes against the protection of information (Articles 267 CC – 269 b CC) and Article 287 § 1 CC, i.e. computer fraud, which is a crime against property. As can be seen on the graph below (Fig. 1), the number of proceedings initiated under Articles 267 CC – 269 b CC is not significant. In 2020, the number of proceedings initiated for an act under Article 267 § 1–3 CC, i.e. the so-called computer hacking, amounted to 7017. A 106% increase in the number of initiated proceedings can be seen over 2016. An even more significant increase in the number of initiated proceedings, by 173%, can be observed with reference to initiated proceedings under Article 287 § 1–2 CC.

At the same time, in 2020 in Poland the number of proceedings initiated under Article 286 § 1–3 CC, i.e. frauds described in police databases as online frauds amounted to 35 566, which accounts for an increase of 9% compared to 2019 and of 30%



The legal basis for initiating proceedings	2016	2017	2018	2019	2020
Art. 267 § 1-4 CC	3401	3419	3676	6718	7017
Art. 268 § 1-3 CC	213	190	148	182	147
Art. 268a § 1-2 CC	499	464	382	686	764
Art. 269 § 1-2 CC	11	13	9	17	9
Art. 269a CC	44	39	51	37	33
Art. 269b § 1 CC	36	28	29	55	49
Art. 286 § 1-3 CC (online frauds)	27296	29161	30437	32627	35566
Art. 287 § 1-2 CC	4103	4554	7402	10793	11219

SOURCE: OWN STUDY BASED ON THE DATA FROM THE NATIONAL POLICE HEADQUARTERS

Fig. 1. Cybercrime in Poland including the legal basis for initiating proceedings

compared to 2016. With a total value of 83 822 proceedings initiated under Article 286 § 1–3 CC in 2020, frauds described in police databases as "online frauds" accounted for 42%. Hence, for most of the acts that could be considered cybercrimes, the proceedings were initiated under Article 286 CC.

The analysis of the data from the category of ascertained crimes provides slightly different values. The observed dynamics of the increase in the number of proceedings initiated under Articles 267 CC, 287 CC, and 286 CC (marked as online) indicates a steady increase in the number of cybercrimes. At the same time, no significant rise in cybercrimes was recorded in 2020 during the COVID-19 pandemic.

Quantitative analysis of proceedings initiated in cybercrime cases can be compared with data on the number of incidents classified by CSIRT/CERT teams. In Poland, security incidents are reported to three different teams: CSIRT NASK (for the private sector and part of the public sector), CSIRT GOV (for part of the public sector), and CSIRT MON (military sector, no publicly available data on incidents).

As Fig. 2 indicates, the number of incidents and observed cybercrimes is regularly increasing. In 2018, the CSIRT NASK team classified 3739 incidents, in 2019 – 6484 incidents, and in 2020 – 10,420 incidents. Between 2018 and 2019, the number of incidents, therefore, increased by 73%, and between 2019 and 2020 by 60.7%. Between 2018 and 2019, the number of incidents classified by the CSIRT GOV increased by 99% (from 6236 to 12405). The CSIRT GOV has not yet published data for 2020. At the same time, the number of proceedings initiated under Article 267 § 1–4 CC, Article 287 § 1–2 CC, and Article 286 § 1–3 CC (online frauds) increased between 2018 and 2019 by 20.8%, and between 2019 and 2020 by 7.3%.

It should be taken into account that multiple notifications may be considered as one incident in the CSIRT databases. At the same time, separate criminal proceedings may be conducted from the notification of each notifier. Notifications submitted in November and December 2020 may therefore have initiated criminal proceedings only in January 2021. That could distort the interpretation of the results. It must also be taken into account that the increased number of incidents was also caused by the increased number of notifications following the implementation of Directive 2016/1148. Undoubtedly, these studies need to be continued in 2021 and to be compared with post-pandemic statistics.

Research on the number of incidents and cybercrimes can also be contrasted with statistical data on the information society in Poland in 2020. According to research conducted by the Central Statistical Office (CSO) in 2020, 90.4% of households had access to the Internet at home (the indicator was 3.7% higher than in the previous year), 81.4% of persons aged 16–74 used the Internet regularly (in 2019 – 78.3%). As concerns the Internet in Poland, using an e-mail as well as reading online were the most common. In the same year, the share of e-mail users in the total population aged 16–74 amounted to 65.9%, while among Internet users 79.2%. In 2020, 60.9% of Poles purchased goods or services over the Internet, compared to 53.9% in 2019, 47.8% in 2018, 45% in 2017, and 41.9 in 2016. During the COVID-19 outbreak, 25% of working people aged 16–74 took advantage of remote working opportunities (most in ICT-related professions – 67.8%).

Research of the CSO in Poland shows that during lockdown there was a slight increase in the number of people using the Internet regularly (3.1%), only a decrease of 1.5% was seen in

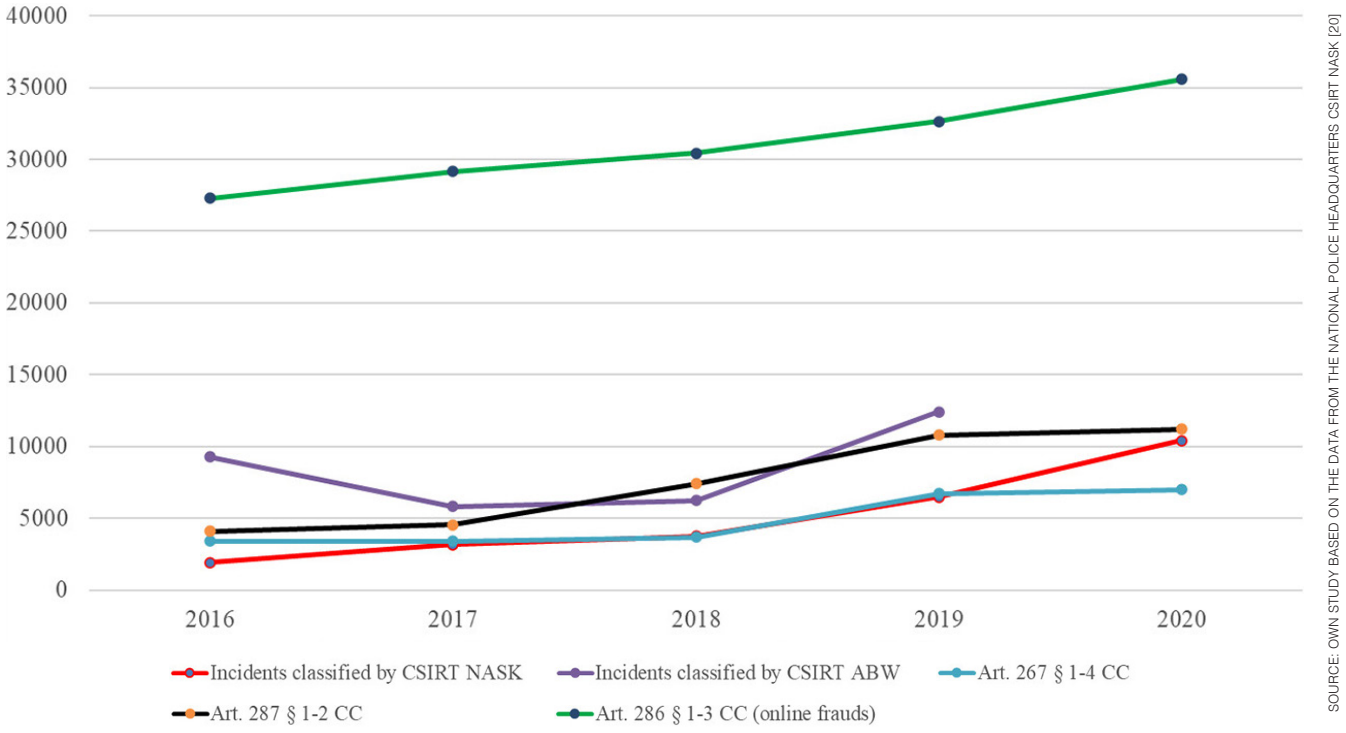
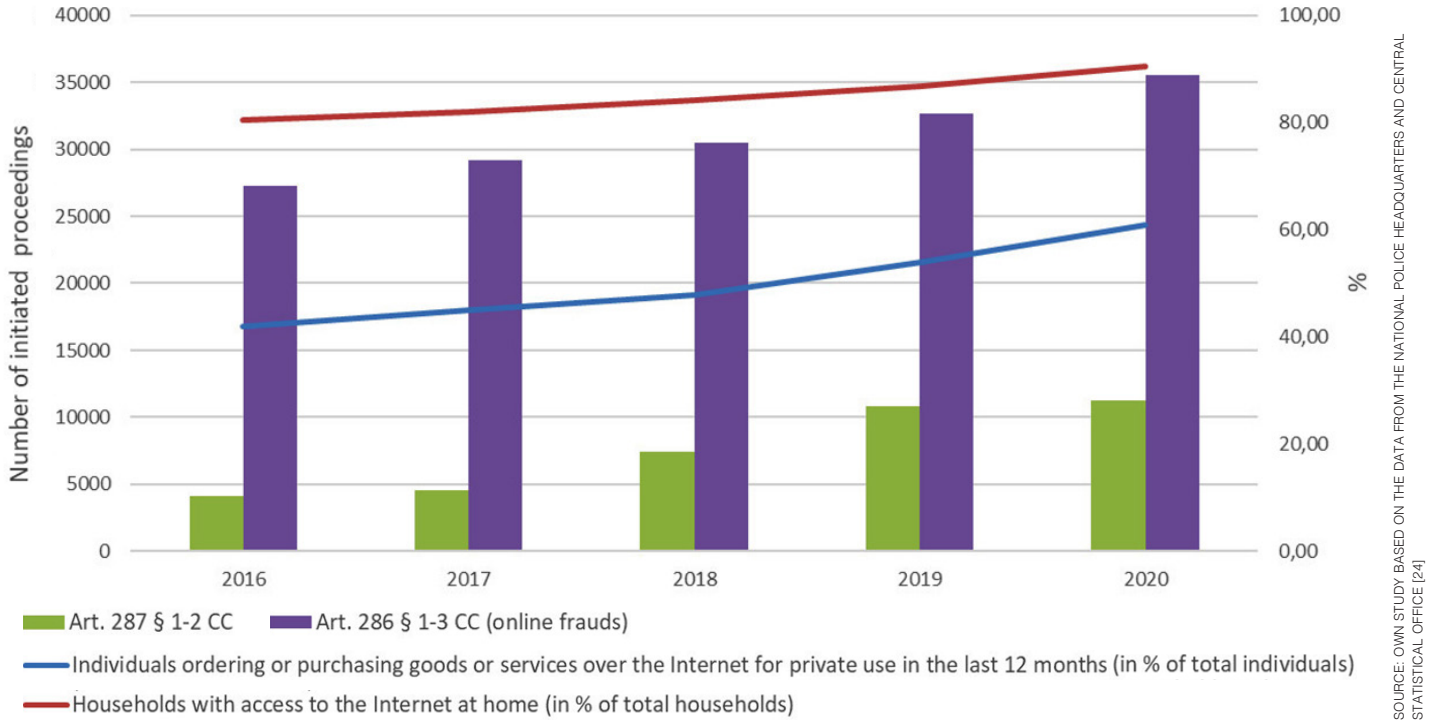


Fig. 2. Cybercrime and incidents classified by CSIRT NASK and CSIRT GOV in Poland



SOURCE: OWN STUDY BASED ON THE DATA FROM THE NATIONAL POLICE HEADQUARTERS AND CENTRAL STATISTICAL OFFICE [24]

Fig. 3. Cybercrime and the evolution of the information society in Poland

the number of people accessing government services online, reaching 41.9%. There was a greater increase in the number of people contacting online for educational purposes (8.1%) or online shopping (7%). However, it should be emphasised that the household survey conducted by the CSO takes place in April and May each year. Taking into account the methodology, the statistical research for 2020 should be confronted with the research for 2021. Only research conducted in 2021 will show the real impact of the pandemic on the basic indicators of the information society in Poland. At the same time, global studies show that the amount of time spent online by each category of Internet users is increasing more significantly [22, 23].

As Fig. 3 indicates, the increase in online shopping correlates with an increase in online fraud and computer fraud. Research on the relationship between the increase in the number of people using online services (new users), the time spent online by Internet users, and the increase in cybercrime should be continued and collated with at least the statistics of 2021.

3. CROSS-CUTTING CRIME FACILITATORS

Cross-cutting crime facilitators include the use of social engineering, the Cybercrime-as-a-Service (CaaS) model, cryptocurrencies to pay for electronic services and as a money laundering method, the anonymity of online services, the availability of many legal services providing encryption, and of bank accounts opened by money mules. Some of the factors that make it easier to commit crimes are also the ones that make it difficult to identify the criminals.

Targeting human weakness in the security chain, social engineering and phishing have a high impact on society and facilitate the majority of cybercrimes. The use of social engineering is widely recognised not only as the primary threat, but also as a factor facilitating cyber-enabled crimes as well as cyber-dependent crimes. Inadequate security measures or insufficient knowledge and skills of users make even poorly prepared attacks based on social engineering successful. At the same time, there is a growing number of well-prepared attacks organised by perpetrators using strategies that combine social engineering with the ability to use tools, systems, and security gaps, false identities, acting in close cooperation with other cybercriminals. Targeted attacks have become easier due to the CaaS model, whereas the increase in sophistication of the perpetrators is particularly evident in the area of cashless payments [25]. Cybercrime marketplaces are equipped with mechanisms that ensure anonymity, security of payments, and tools to facilitate high-risk transactions (escrow), and limit abuse (seller and buyer rating system, comments). On DarkWeb marketplaces, cybercriminals offer or purchase tools, services, and data necessary to commit crimes and recruit others for the business. They also provide technical support services and beginners' guides. This results in more serious and better-prepared attacks causing increasingly more damage. New tools and platforms are becoming more accessible to those who lack advanced technical skills, enabling newcomers to start criminal activities, whereas more experienced criminals to develop more specialised skills or find people who can complement their services and work with them to develop new or better criminal tools and techniques.

Payments for services, mutual settlements between people who cooperate in committing crimes, or transfers of funds from crime are possible with the use of cryptocurrencies. Bitcoin

remains a key facilitator for cybercrime; other cryptocurrencies such as Monero or Ethereum are also gaining popularity within the digital underground. Undoubtedly, settlements and laundering money from criminal activities are also made easier thanks to the availability of bank accounts set up by the so-called money mules. The lack of data exchange between banks, combined with the protection of bank secrets and the time-consuming process of obtaining data for criminal proceedings all make it extremely difficult to recognise such accounts and block the funds available there. Criminals also make use of the possibility offered by some banks to open online accounts for which they use data from identity theft.

4. FACTORS HINDERING IDENTIFICATION OF CRIMINALS

Perpetrators of cybercrimes respect operational security rules, in particular anonymity. People who work together do not know each other's personal data, image, or location, and they do not exchange information about their private lives. Communication between them occurs with the use of encrypted communicators (mainly jabber and Telegram). To maintain anonymity, criminals use technical tools hindering or preventing the analysis of the network traffic (TOR), determination of the IP address assigned to them by a telecommunications network operator (VPN, PROXY), or interception of communication content (encryption). Cybercriminals hide their identity also by illegally using created fake identities and identities of others. Thanks to such fake or intercepted identities, perpetrators register domains and SIM cards, use electronic services, set up e-mail accounts, profiles on social networking sites, accounts on cryptocurrency exchange platforms or online currency exchange sites, or communicate with people they work with or that they attack. To ensure the anonymity of banking transactions, for money laundering purposes they use both bank accounts set up using other people's data and bank accounts to which they have managed to gain unauthorised access.

Since without structures ensuring the secure transfer of funds, it would not be possible for criminal activity to take place, various chains used for money laundering must be eliminated. Following money transfers is also the most effective method of establishing the identity of those who are at the top of the schemes and who are in charge. To reduce the availability of accounts used for money laundering and transfers of funds from victims' accounts, it is necessary to take actions aiming at improving data exchange between banks and financial institutions. Detaining and prosecuting perpetrators also requires that data on money laundering accounts and suspicious transactions be immediately transferred to law enforcement authorities. The excessive waiting time for data usually prevents securing ATM recordings or urban monitoring from the time and place of withdrawal.

Law enforcement authorities also take actions to eliminate perpetrators' access to tools used to commit or facilitate the commission of crimes, as well as to DarkWeb marketplace or criminal forums [26]. Only in December 2020, Europol reported the interception of the virtual private network SafeInet infrastructure [27], whereas the National Crime Agency from the UK reported the detention of 21 people – customers of WeLeakInfo, an online criminal marketplace that advertised stolen personal credentials [28]. Identifying perpetrators and the distributed infrastructure that they use, in particular servers, VPSs, email accounts, cryptocurrency exchange platforms, and bank accounts, is extremely difficult due to anonymous payments and the methods used by cybercriminals to conceal their identity. These actions require coordinated international cooperation given that the perpetrators, electronic data, and evidence necessary for criminal proceedings, and the victims are usually situated in different jurisdictions. Currently, more than half of all criminal investigations require access to cross-border electronic evidence. Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations, there is a need to obtain evidence from online service providers based in another jurisdiction [29]. Insufficiently effective mechanisms of international cooperation, securing of electronic evidence and data exchange in cybercrime cases are important factors hindering criminal proceedings. In view of the identified problems, there are initiatives taken within the EU aiming at increasing the efficiency and speed of the process to secure and obtain electronic evidence stored or held by service providers having establishments in another jurisdiction, in the form of European Production and Preservation Orders for electronic evidence in criminal matters [30]. Work on a directive establishing harmonised rules on the appointment of legal representatives to gather evidence in criminal proceedings is also underway [31]. Further work on the aforementioned legislation intensified in December 2020 after an almost one-year break. These regulations will complement or partly replace existing instruments, such as the European Investigation Order or regulations resulting from conventions or bilateral agreements related to international legal assistance [32].

5. PROTECTION OF USERS FROM CYBERATTACKS

In 2020 in Poland among Internet users aged 16–74, individuals with a low level of overall digital skills accounted for 31.5%, with basic skills 24.1%, and with above basic skills – 26.1% [33], therefore protection of Internet users from cyberthreats should be implemented as part of a system-wide approach at different levels and by different actors. First of all, extensive education and dissemination of the principles of cyber hygiene are essential at all levels of education and among diverse audiences. Cyberthreats affect the youngest children who start using mobile phones, the Internet, or smart toys even before they commence their formal education. Elements of cybersecurity, by analogy to traffic safety rules, should be widely introduced into the curricula as early as in pre-schools, and then developed at further stages of education. The concurrent education of adults is equally important as they are the ones who are very often unaware of the risks. Education for cybersecurity, including current attack scenarios, responding to cyber threats or disinformation should become permanent components of the curricula at all levels of education and as part of the training for the workforce.

Regardless of educational activities or information campaigns, proactive measures should be considered to protect users. One of the possible mechanisms is blocking access to specific Internet websites. Many countries have extensive or point regulations connected with blocking access to specific websites and removing specific content [34]. In Poland, blocking access to websites has been regulated on a point basis as regards: 1. specific IT data related to a terrorist event or specific IT services used or exploited to cause a terrorist event [35], 2. domains used to offer gambling services against the law [36]. The analysis of methods of perpetrators who use the COVID-19 pandemic shows that none of the models of blocking provided for in the Polish law could be applied. Furthermore, as analyses of victims' speed of response show, none of the aforementioned models would be effective for the most frequent attacks in which criminals intercept login credentials to social networking sites, banks, or e-mail accounts. Users immediately respond to text messages containing hyperlinks to websites with fake login panels, without giving themselves time to think. About 80% of attempts to access the fake site occurs within 15 minutes of receiving a message containing the link. Only 10% of people try to open the phishing site the next day [37]. Authors of text messages usually send them in the evening, counting on reduced vigilance of potential victims. Moreover, the domain names used by cybercriminals are registered within a few hours before the attack takes place. This makes it extremely difficult to formally block access to the content by a court, prosecutor's order, or administrative decision.

In Poland during the pandemic, to protect Internet users from phishing attacks, the so-called "Warning List" was created, containing domain names used to fraudulently obtain data and financial resources. The list is maintained by the Scientific and Academic Computer Network, which is the national CSIRT. Domain names on the list may be blocked by telecommunications operators. On 31 December 2020, there were already 7396 items on the list [38]. Currently, this mechanism is only temporary: its functions are based on an agreement, not generally applicable legal provisions, and only during states of emergency, epidemics, or public health emergencies. The analysis of the warning list makes it possible to select domain names used by criminals responsible for the "fake payment gateway" (typical strings of characters: "pay," "mail," "courier," "inpost," "parcel," "dhl," "dpd") and the perpetrators creating pages with hair-raising news and intercepting login credentials to social networking sites (typical strings of characters: "fact," "kidnapping," "rape," "news"). As a result, an attempt can be made to select domain names that can be used in an attack during a certstream analysis, which is an intelligence feed that gives real-time updates from the Certificate Transparency Log network.

6. CONCLUSIONS

Cybercrime is one of the most dynamic forms of crime. Those committing cybercrimes are highly adaptable. To achieve their goals, they quickly adjust their methods, the tools that they use, and the social engineering techniques involved in their attacks.

The conducted research indicates an increasing number of proceedings initiated in cybercrime cases in Poland between 2016 and 2020. Although research has not shown a notable rise in cybercrimes committed in Poland during the pandemic, changes in the attack scenarios deployed by the perpetrators have been observed. What is more, most of the analyses conducted so far have not covered the modus operandi of the perpetrators of frauds, considered typical crimes against property. As the conducted research demonstrates, in 2020, 42% of proceedings initiated under Article 286 CC were marked as "online" in police databases. The omission of fraud in determining the scale of the cybercrime phenomenon leads to erroneous conclusions as regards the threats and to poor prioritization of law enforcement actions.

The new threats inspire discussions on anonymity in the use of electronic services and methods to verify the identity of those who want to use them. In most cases, cybercriminals cannot be caught due to various methods of concealing their identity, in particular exploiting fake or intercepted identities when registering domains or SIM cards or when using electronic services or payments. Problems of de-anonymisation of criminals' data are inextricably linked to the growing phenomenon of identity theft, the anonymity ensured by the TOR network, and the use of cryptocurrencies.

New threats should also lead to discussions on the protection of users of electronic services. On the one hand, widespread education is necessary to raise awareness of threats and develop the ability to recognise attacks. The increasing number of incidents and high effectiveness of the attacks lead to the introduction of solutions that proactively protect end-users. Blocking domain names that are used to fraudulently obtain data and funds is not only a technical problem, but – above all – a legal issue concerning legal guarantees of freedom of information, information autonomy, or freedom to carry on business. The effectiveness of protection provided in Poland by the so-called "List of Warnings" inspires work focusing on anchoring this solution in the generally applicable law, while introducing an appeal procedure for subscribers of domains deemed as involved in phishing. For this solution to be practical, it is also necessary to ensure rapid detection of domain names with a specific structure or those registered using fake or intercepted data, by analysing data from registries, registrars, or certstream networks.

REFERENCES

[1] "Agari H2 2020 Email Fraud Report". [Online]. Available: https://www.agari.com/cyber-intelligence-research/e-books/agari-h2-2020-email-fraud-report.pdf [Accessed: 15-Jun-2021].

[2] "IC3 Internet Crime Report 2019", p. 9. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf [Accessed: 15-Jun-2021].

[3] "Internet Organised Crime Threat Assessment (IOCTA) 2020" [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 [Accessed: 15-Jun-2021], hereinafter as: IOCTA 2020.

[4] "How COVID-19-related crime infected Europe during 2020" [Online]. Available: https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020 [Accessed: 15-Jun-2021].

[5] Rise of fake 'corona cures' revealed in global counterfeit medicine operation. [Online]. Available: https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation [Accessed: 15-Jun-2021].

[6] Warnings about fake online shops are published on consumer or cybersecurity websites. Sample fake online shop search engine: "Suspicious online shops!" [Online]. Available: https://www.legalniewsieci.pl/aktualnosci/podejrzane-sklepy-internetowe [Accessed: 15-Jun-2021], [in Polish].

[7] Criminal Code of June 6, 1997 (Journal of Laws of 2020, item 1444, as amended), hereinafter CC.

[8] Already on 16 March 2020, criminals created a fraudulent fundraiser in Poland at https://pomoc.siepomaga.net/koronawirus?SS52.

[9] "Annual Report on the Activities of CERT Poland. Security Landscape of the Polish Internet", 2018, pp. 59–67. [Online]. Available: https://www.cert.pl/uploads/docs/Raport_CP_2018.pdf [Accessed: 15-Jun-2021], [in Polish].

[10] In connection with the discovered insufficient implementation of technical and organisational measures to secure customer data, by a decision of 10 September 2019, Morele.net Sp. z o.o. was charged with an administrative fine of PLN 2.8 million (Decision of President of the Personal Data Protection Office of 10 September 2019, no. ZSPR.421.2.2019, subsequently upheld by a judgement of the Provincial Administrative Court in Warsaw of 3 September 2020, no. II SA/Wa 2559/19, [in Polish].

[11] Regulation of the Minister of National Education of 11 March 2020 on the temporary restriction of the functioning of educational facilities in relation to preventing, counteracting and combating COVID-19 (Journal of Laws item 410 as amended), [in Polish].

[12] Government's bill to amend the Law on special solutions to prevent, counteract and combat COVID-19, other communicable diseases and the resultant crises, and to amend certain other laws, form no. 299 of 26 March 2020. [Online]. Available: http://sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=299 [in Polish].

[13] A. Gryszczyńska, "The use of COVID-19 in scenarios of social engineering attacks", *Maritime Security Yearbook,* 2021, pp. 137–161, [Online]. Available: https://wdiom.amw.gdynia.pl/wp-content/uploads/2021/06/PT2020v0.13.pdf [in Polish].

[14] M.S. Islam et al., "COVID-19-Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis", *Am. J. Trop. Med. Hyg.* 103(4), 1621–1629, (2020), doi: 10.4269/ajtmh.20-0812.

[15] J. Tidy, "Dr Reddy's: Covid vaccine-maker suffers cyber-attack", BBC, Oct. 22, 2020 [Online]. Available: https://www.bbc.com/news/technology-54642870 [Accessed: 15-Jun-2021].

[16] "Advisory: APT29 targets COVID-19 vaccine development". [Online]. Available: https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf [Accessed: 15-Jun-2021].

[17] BBC News, "Pfizer/BioNTech vaccine docs hacked from European Medicines Agency", BBC, Dec. 09, 2020 [Online]. Available: https://www.bbc.com/news/technology-55249353 [Accessed: 15-Jun-2021].

[18] "Pandemic profiteering: how criminals exploit the COVID-19 crisis". [Online]. Available: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis [Accessed: 15-Jun-2021].

[19] Wired, Sep. 19, 2020 [Online]. Available: https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital [Accessed: 15-Jun-2021].

[20] "Annual Report on the Activities of CERT Poland. Security Landscape of the Polish Internet", 2019. [Online]. Available: https://www.cert.pl/uploads/docs/Raport_CP_2019.pdf [Accessed: 15-Jun-2021], [in Polish].

[21] "Report on the state of Poland's cybersecurity in 2019". [Online]. Available: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html [Accessed: 15-Jun-2021], [in Polish].

[22] A. Pérez-Escoda, C. Jiménez-Narros, M. Perlado-Lamo-de-Espinosa, and L. Miguel Pedrero-Esteban, "Social Networks Engagement During the COVID-19 Pandemic in Spain: Health Media vs. Healthcare Professionals", *Int. J. Environ. Res. Public Health* 17(14), (2020), doi: 10.3390/ijerph17145261.

[23] GWI Coronavirus Research, March 2020 Series 2: Travel & Commuting, GWI Connecting the dots 2021; The biggest COVID-19 trends that are here to stay. [Online]. Available: https://www.globalwebindex.com [Accessed: 15-Jun-2021].

[24] "Information society in Poland in 2020", Central Statistical Office, [Online]. Available: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2020-roku,1,14.html [Accessed: 15-Jun-2021], [in Polish].

[25] "IOCTA 2020", pp. 6–7, 13–17 (2020). [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[26] For example in 2013 the Silk Road has been seized: "Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts — FBI". [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts [Accessed: 15-Jun-2021].

[27] "Cybercriminals' favourite VPN taken down in global action". [Online]. Available: https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action [Accessed: 15-Jun-2021].

[28] "21 arrests in nationwide cyber crackdown". [Online]. Available: https://www.yorkpress.co.uk/news/18970445.21-arrests-nationwide-crackdown-website-selling-stolen-personal-data/ [Accessed: 15-Jun-2021].

[29] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM/2019/70 final.

[30] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD).

[31] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final – 2018/0107 (COD).

[32] A. Gryszczyńska, "Acquisition and analysis of data on cybersecurity incidents", *Internet. Data analyst*, G. Szpor, Ed., *C.H. Beck*, Warsaw, 2019, pp. 296–313, [in Polish].

[33] "Information society in Poland in 2020", p. 156, [in Polish].

[34] "Comparative study on filtering, blocking and take-down of illegal content on the Internet", Swiss Institute of Comparative Law, 2015, [Online]. Available: https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html [Accessed: 15-Jun-2021].

[35] Law of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws of 2020 item 27 as amended), [in Polish].

[36] Law of 19 November 2009 on Gambling (Journal of Laws of 2020 item 2094), [in Polish].

[37] P. Dęba, "Multi-vector protection of Internet users as illustrated by the Orange Cyber Shield", presented at the 12th Scientific Conference Security in the Internet – Cyber Pandemic, UKSW, Warsaw, Oct. 22–23, 2020, [in Polish].

[38] Index of domains. [Online]. Available: https://hole.cert.pl/domains/ [Accessed: 15-Jun-2021].