GIS Odyssey Journal

2024 • Volume 4 • Number 2

https://doi.org/10.57599/gisoj.2024.4.2.147

Jerzy Dorobisz[1]

ANALYSIS OF TRENDS AND RISKS IN THE FIELD OF NETWORK SECURITY BASED ON STATISTICAL DATA

Abstract: The study analyses contemporary trends in cybersecurity, focusing on evolving threats, methods, and their implications in the European Union, particularly Poland. Data from NIST reveals a rise in vulnerabilities, surpassing 28,000 in 2023. ENISA's 2022/2023 report identifies key threats, including ransomware, DDoS, social engineering, and malware, highlighting trends like extortion-only attacks, geopolitical influences, and the professionalization of cybercrime services. In Poland, CERT recorded nearly 40,000 cybersecurity incidents in 2022, predominantly phishing (64%), malware (8.5%), and system hacking. Ransomware remains a critical issue, with groups like LockBit and BlackCat leading attacks. Phishing evolves with advanced techniques such as "Browser in the Browser" attacks, often targeting individuals through email and social platforms. Despite advancements in malware protection and internal network security, vulnerabilities persist in areas like supply chain security and mobile device management. The use of AI in cybercrime is expected to grow, enabling sophisticated phishing, deepfakes, and large-scale personalized attacks. Future threats also include state-sponsored cyber espionage and attacks on multi-cloud environments. The study underscores the need for proactive security measures, technological advancements, and public awareness to mitigate growing cyber risks.

Keywords: analysis of risks, statistics, risks

Received: 15 November 2024; accepted: 21 December 2024

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0009-0008-2509-6615, email: jerzy.dorobisz@wat.edu.pl

Introduction

The ever-evolving landscape of cybersecurity presents significant challenges, particularly in identifying and mitigating cyber threats. This study provides an overview of current trends in cybersecurity, with a focus on the nature and evolution of threats, the techniques employed by cybercriminals, and their implications within the European Union, with a particular emphasis on Poland. Statistical data has been sourced from official reports by leading institutions in cybersecurity.

This study is intended to provide an overview of current trends in the world of cyber security, with particular emphasis on the description of existing threats, their nature, techniques and modifications compared to previous years used by cyber criminals in the countries of the European Union and especially in Poland. Statistical data is taken from official reports of institutions dealing with network security.

As an introduction, it is worth looking at a statistic published by the US NIST (National Institute of Standards and Technology). According to it, the number of new vulnerabilities in the field of cyber security has an increasing trend, as shown by data from the National Vulnerability Database. In 2023, the number exceeded 28,000 (Fig. 1.).

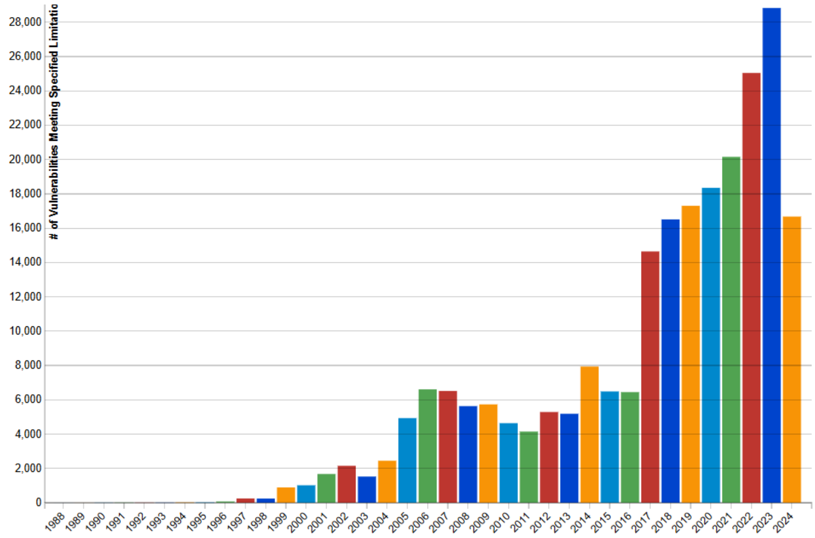


Fig. 1. Total Matches By Year 2023
Source: National Vulnerability Database

Materials and methods

European Union. ENISA (The European Union Agency for Cybersecurity), the European Union's agency for cyber security in Europe, for 2022/2023, the most threats in the field of cybersecurity it classified as ransomware, DDoS (distributed denial-of-service), data, malware, social engineering and information manipulation (Fig. 2, Fig. 3 a, 3 b, 3 c, 3 d, 3 e).

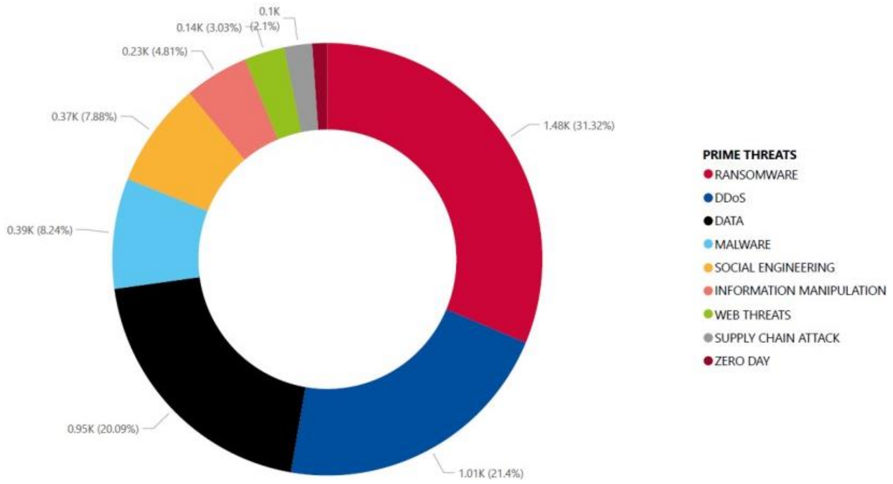


Fig. 2. Breakdown of analysed incidents by threat type (July 2022 – July 2023)
Source: ENISA Threat Landscape 2023

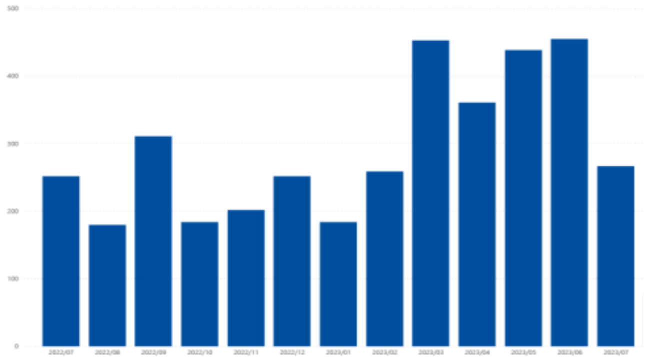


Fig. 3 a. Incidence of Ransomware 2023
Source: ENISA Threat Landscape 2023

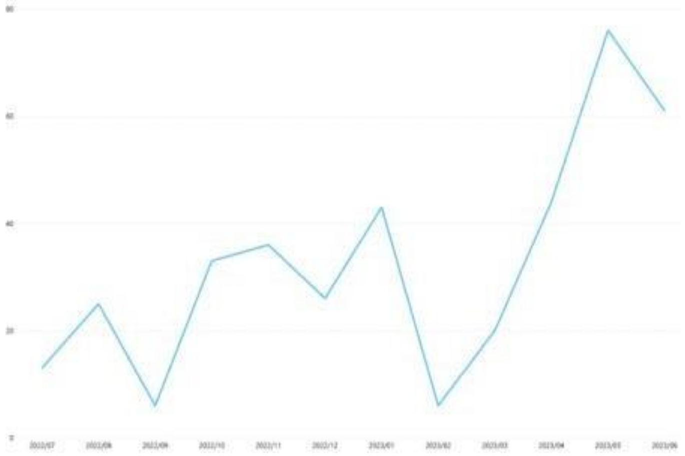


Fig. 3 b. Incidence of Malware 2023
Source: ENISA Threat Landscape 2023

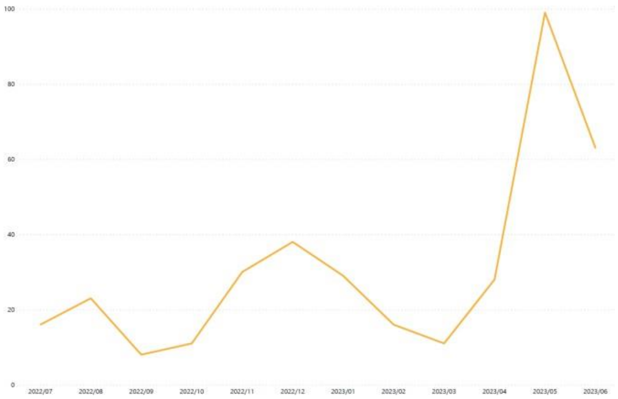


Fig. 3 c. Incidence of Social engineering 2023
Source: ENISA Threat Landscape 2023

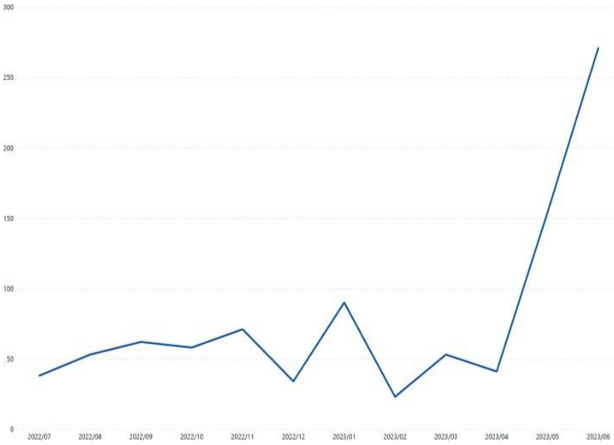


Fig. 3 d. Incidence of Data 2023
Source: ENISA Threat Landscape 2023

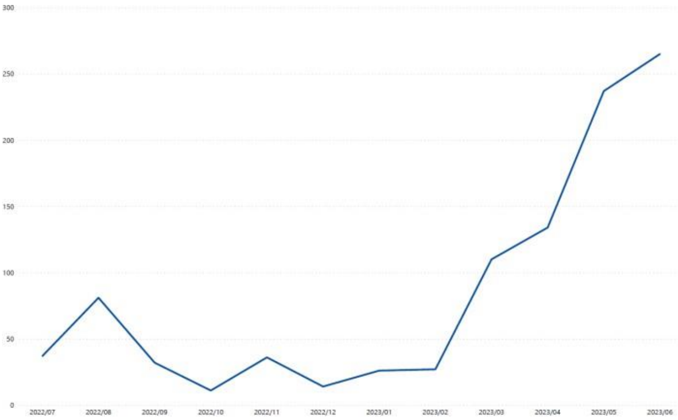


Fig. 3 e. Incidence of DDOS 2023
Source: ENISA Threat Landscape 2023

Among the leading trends in the field of cyber threats within the European Union between 2022 and 2023 were:

- the largest number of threats belong to those in the ransomware and anti-access cateories,
- use and abuse of legal tools to attack, make it more difficult to identify and more easily exploit the victim's confidence,
- strong influence of geopolitics on illegal cyber activities,
- professionalisation of software as a service (aaS),
- increasing use of Extorsion-only attacks, which differ from traditional ransomware in that they do not use encryption on the victim's data, but instead obtain sensitive data and threaten to make it public unless a ransom is paid,
- increased number of actions taken against cybercrimes by Member States' law enforcement authorities,
- activities of the Russian cybercrime group Cl0p, involved in malware distribution, extortion techniques, large-scale phishing and zero-day attacks,
- as in previous years, data theft continues to be one of the biggest threats (e.g. Agent Tesla, Readline Stealer and FormoBook) (ENISA Threat Landscape 2023),
- there is a steady decline in classic malware targeting mobile devices; the most common type of attack on mobile devices is spyware,
- there is an increase in statements by hacktivists about alleged attacks on the OT's IT infrastructure, but this is often not supported by the facts,
- phishing is still the most common means of access initiation, with it increasingly being initiated in the physical world,
- attackers still make heavy use of BEC (business email compromise: this technique involves sending personalised emails to specific individuals within an organisation and getting them to send money to the criminal, for example) and VEC attacks in order to obtain financial gain,
- criminals continue to shift from using Microsoft macros to ISO, OneNote and LNK files,
- there has been an increase in data leakage (data compromise),
- cyber security is increasingly influenced by artificial intelligence chatbots,
- DDoS attacks are becoming increasingly complex and sophisticated and are targeting mobile and IoT networks,
- the highest ever number of threats of Internet access loss has been observed,
- numerous manipulations of information related to the Russian military action against Ukraine,
- the rise of so-called "cheap fakes" and data manipulation created by artificial intelligence,
- the growing interest of cybercrime groups in attacking the supply chain (National Vulnerability Database).

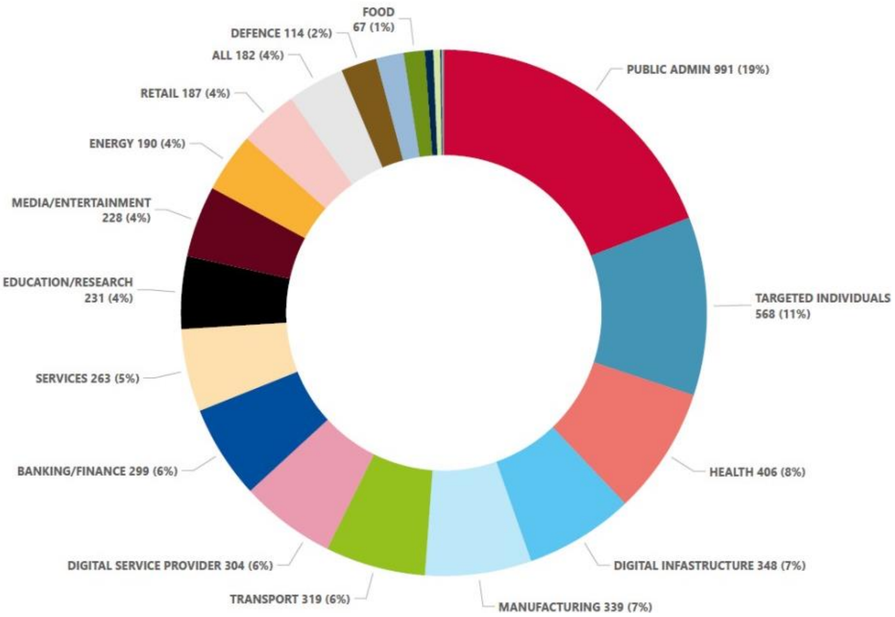


Fig. 4. Targeted sectors per numer of incidents (July 2022 – June 2023)
Source: ENISA Threat Landscape 2023

ENISA has distinguished four categories of cyber threat actors (threat actors):

- advanced Persistent Threats (APTs) – heavily paid groups by the armed forces, Intelligence Agencies or state control authorities whose main purpose is espionage and profit generation,
- cybercriminals,
- hackers for hire,
- hacktivists.

Most of the units causing risk in the EU were unidentified (55%). The remaining entities were mainly: NoName, LockBit3.0, Cl0P, KillNet, BlackCat, PLAY and Anonymous Sudan (National Vulnerability Database) (Fig. 4).

Poland. In 2022, 39683 cyber security incidents were recorded by CERT, with a total of 322479 reports. The most frequent incidents included: phishing scams (64% of incidents, mainly using the image of InPost, Facebook and Vinted), malware (approximately 8.5% of incidents, especially Flubot software) and hacking of IT systems and email accounts (1%). A significant number of ICT incident reports were also recorded by the ARAKIS GOV system (as many as 1234040 reports of potential incidents in total). The trend in the number of cyber security incidents is shown in the chart (Fig. 5).

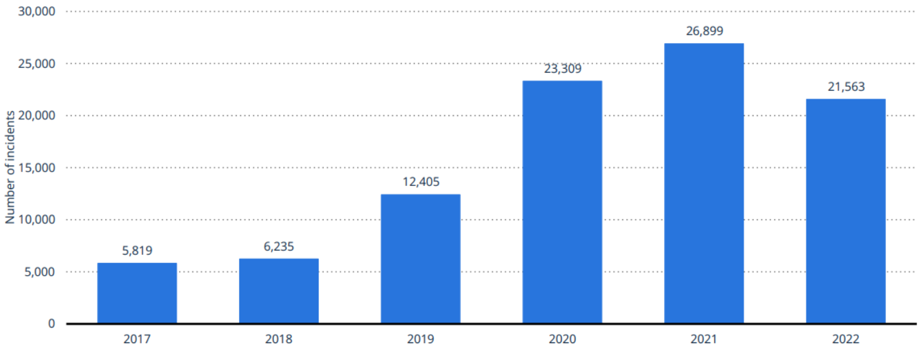


Fig. 5. Number of cybercrime incidents in Poland from 2017 to 2022
Source: Cybercrime and cybersecurity in Poland, 2023

The good news is that the number of unauthorised access to data (data breaches) in Poland has decreased significantly over the last three years (Fig. 6).

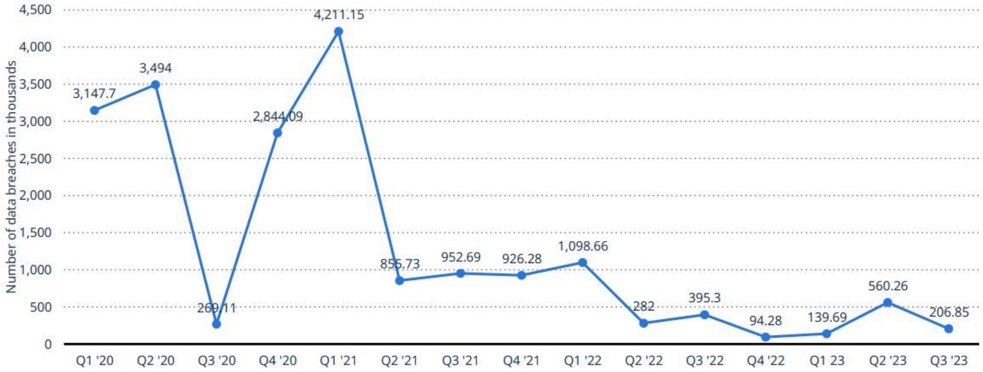


Fig. 6. Number of incidents of data breaches in Poland from 1st quarter 2020 to 3rd quarter 2023 (in 1,000s)
Source: Cybercrime and cybersecurity in Poland, 2023

The vulnerability categories of the incidents recorded by CSRIT GOV are shown in the chart (Fig. 7).

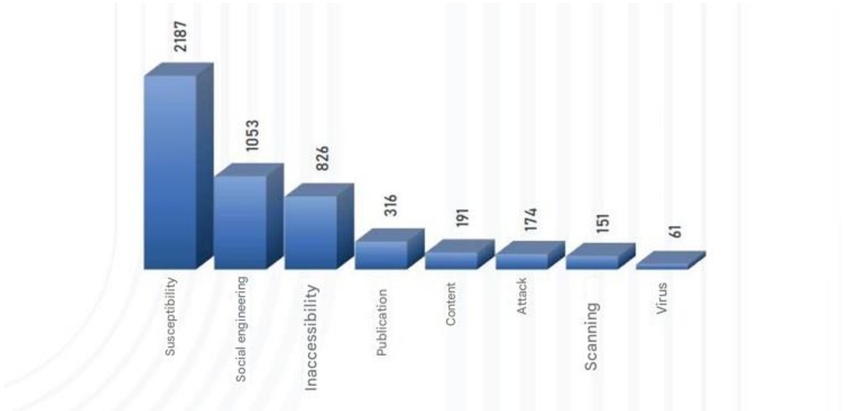


Fig. 7. Statistics of incidents in 2022 reported by entities of the national system cyberscurity
Source: Cybercrime and cybersecurity in Poland, 2023

By economic sector, CERT recorded the highest number of incidents in media, postal services, trade, energy and among individuals (Fig. 8).

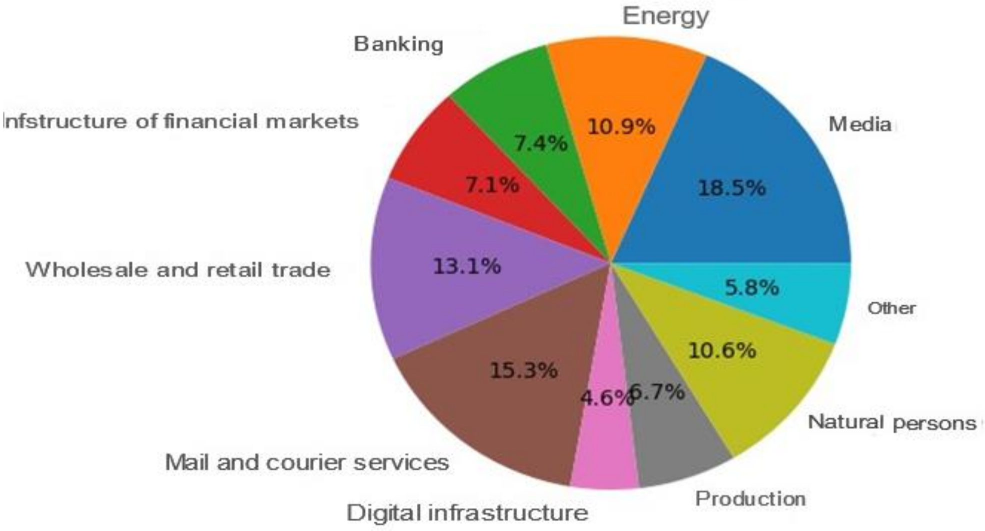


Fig. 8. Share of incidents by econimic sector
Source: Cybercrime and cybersecurity in Poland, 2023

The CSRIT, on the other hand, recorded the most incidents concerning threats to telecommunications networks used by critical network operators; a lot of reports concerned attacks on government offices and authorities (National Vulnerability Database) (Fig. 9).

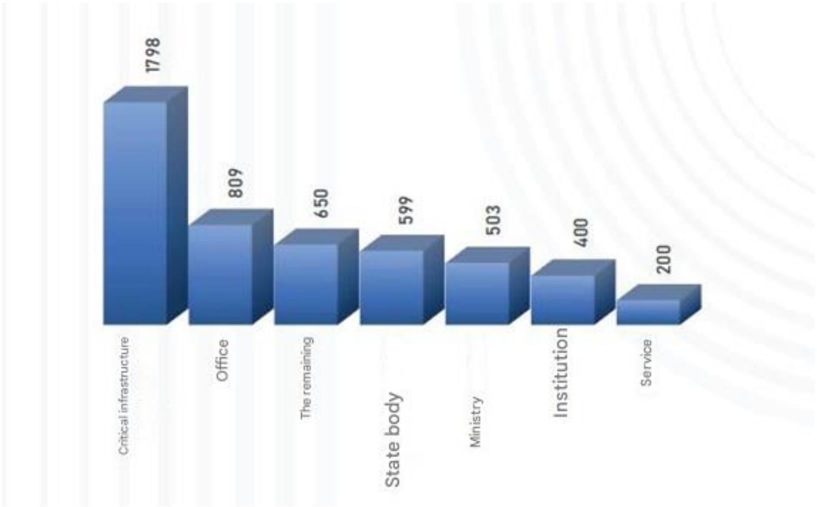


Fig. 9. Number of incidents by sector reported by entites
of the national system cybersecurity
Source: Report on the state of Poland's cybersecurity in 2022

Ransomware. As in 2021, repelling ransomware attacks was a major challenge. CERT recorded 85 of these in 2022, 20% fewer than in 2021, but these incidents involved larger private companies, state institutions and health sector institutions. The most common ransomware families observed were:

- LockBit v2 and v3: Ransomware as a Servive (RaaS); the targets of the attacks are mainly small and medium-sized enterprises, although attacks on international companies have also been reported,
- Deadbolt,
- Medusa,
- Phobos,
- Macop.

Attention should also be paid to other types of ransomare, as described by foreign network security players (MSTC, Sophos, etc.):

- Prestige: the attacks, believed to have been carried out by Russian groups IRIDIUM and Sandworm targeted institutions related to transport and logistics in Poland and Ukraine. The AES algorithm is used to encrypt the data.
- BlackCat: according to Sophos, this type of ransomware was the second most used in the world in 2022. The software encrypts and steals local and cloud-based data. The attack uses the CobaltStrike tool and a Microsoft tool, after gaining access to administrative and Active Directory user accounts.

UK-based Sophos has noted a new trend of providing various types of services as a Service. They included among these services: access to credentials to ICT systems, malware distribution, phishing, OPSEC techniques, encryption, fraud, phishing and scanning. Sophos cites the increase in funding for cybercrime groups as a reason for the rise in attacks via Services as a Service.

Another trend has been noted by CERT: increasingly, criminals are also sending data to their servers while attacking and encrypting the data, in order to increase the likelihood of the victim paying the ransom. Hackers make information about the theft of the data and the date it was made public available on a site hosted on the TOR network.

Phishing. The phishing scams recorded by CERT in 2022 primarily include the following types, which are already familiar from previous years:

- false alerts on bank accounts – fraudsters used communication by e-mail or SMS,
- fake payment gateways – SMS messages with links to fake payment panels usually went to random phone numbers,
- Netflix user accounts stolen,
- phishing for money from sellers on advertising portals (OLX, Vinted, as well as Booking, BlaBlaCar) – fraudsters mainly use communication via WhatsApp,
- interception of Facebook accounts.

These methods make extensive use of inducing time pressure on the victim of the attack, and are often designed to create fear of potential consequences if the victim fails to pay and/or log in to the fake login panel.

In addition to the above phishing campaigns, new variants of this type of scam have been observed:

- Campaigns using the image of government websites and institutions (portal "gov.pl", Ministry of Finance, Twój e-PIT website).
- Use of the innovative Browser In The Browser technique – displaying an apparently

new browser window with a fake login panel inside the visited website. This method is characterised by the fact that the fake address bar contains the correct domain address, moreover, the 'window' is graphically well crafted and blends in with the page being viewed.

- Distribution of information stealer software via e-mail. Infostealer is a type of malware that involves stealing user data by infecting the device with malware. Attackers use fake advertisements, emails, links and websites to do this. Some of these attacks use spoofing – impersonating the email address, phone number or IP address of a selected institution/person when SPF and DMARC mechanisms have been misconfigured by the domain owner. A common variant of this type of threat was the Agent Tesla remote access trojan (a type of Remote Access Trojan), which involves impersonation of business correspondence (it was not uncommon for criminals to impersonate Polish companies) in emails, where fake .img or .xlsx files are attached, which are in fact archive files containing malicious executable scripts. In some cases, instead of an attachment, the email contained a link to the OneDrive platform. The malware families installed on infected computers are mainly Redline and Xloader/Formbook. Among other things, the Tesla agent is able to obtain saved passwords and logins from browsers and typed data using FTP, SMTP and HTTP protocols and a malicious .NET file downloader.
- "ad hijacking" via the Google Ads system. Sites pretending to be software distributors but actually promoting malware were ranked highly in search results. This method allowed criminals to gain full access to a user's system. When the victim downloaded the file (.exe or .zip), a malicious BatLoader installer was installed on the device, which in turn infected the victim's computer with a Royal-type ransomware or the computer was infected by IcedID, which triggered the delivery of further programmes and scripts.
- Fraud using QR codes on the Discord platform. The targets of the attack were mainly children and teenagers. The criminals impersonated a friend of the portal user.
- Personalised blackmail on website owners. In an email, the criminals informed website owners that the site had allegedly been hacked and databases stolen, demanding a ransom in BitCoin.
- Hydra banking trojan. Victims of the attack received a message pretending to be from ING Bank informing them that they had allegedly failed to install a security app on their mobile device, resulting in their account being temporarily locked. The victim was then prompted to enter their banking details on the fake bank's website, scan the QR code with the 'app' (which was in fact a Trojan) and give it special privileges, allowing criminals to steal their credentials.

- Hydra banking trojan. Victims of the attack received a message pretending to be from ING Bank informing them that they had allegedly failed to install a security app on their mobile device, resulting in their account being temporarily locked. The victim was then prompted to enter their banking details on the fake bank's website, scan the QR code with the 'app' (which was in fact a Trojan) and give it special privileges, allowing criminals to steal their credentials.

- UNC1151/Ghostwriter group activities: phishing targeting individuals involved directly or indirectly in policies towards Russia and Belarus. The method of attack uses links sent by e-mail or the Browser in the Browser technique (Cybersecurity Barometer).

The characteristics of the phishing problem encountered by Polish consumers are illustrated by the statistics (Fig. 10).

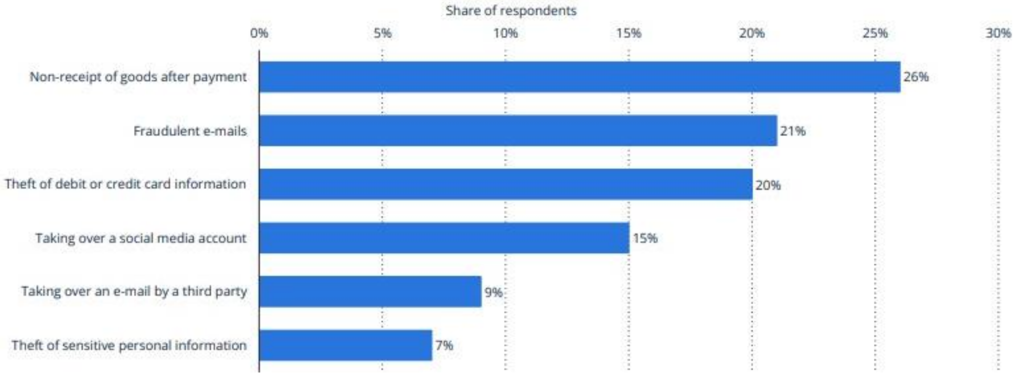


Fig. 10. Most common online scams and cyber attacks encountered
by consumers in Poland in 2022
Source: Report on the state of Poland's cybersecurity in 2022

Malware. Compared to 2021, CSRIT GOV identified 46% more malware cases in 2022, 743 malicious files, some of which could be classified as on (Fig. 11).

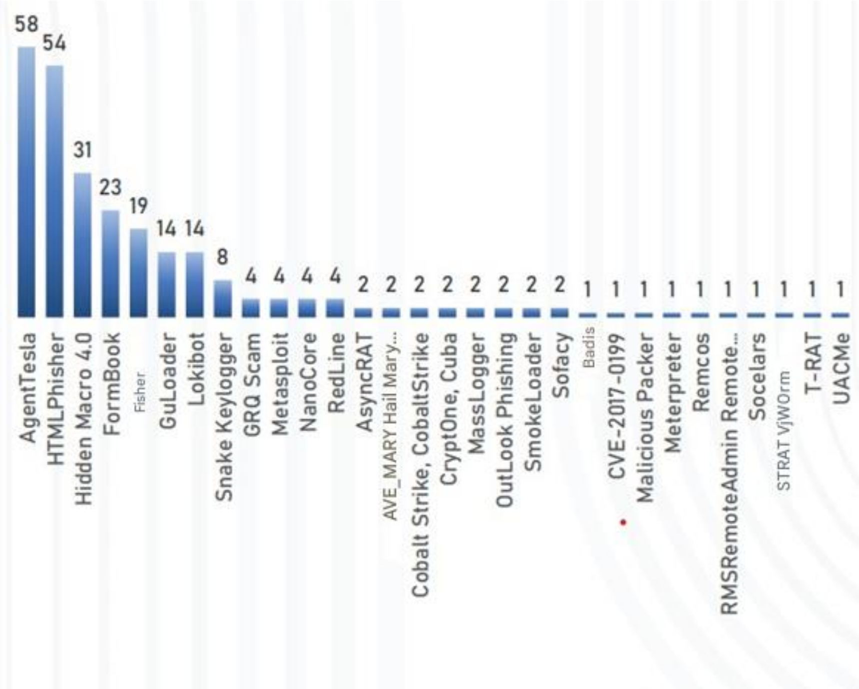
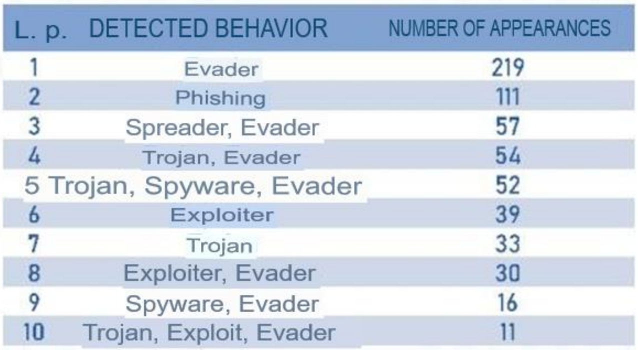


Fig. 11. Malware classification
Source: Report on the State of Poland's Cybersecurity in 2022

- CSRIT, like CERT, identified a large amount of Agent Tesla software as described above.
- HTML Phisher: uses HTML or HTM attachments to email messages. The attachment has JavaScript code that generates a link to a website with a form, aiming to phish the victim's data. It is also not uncommon for this method to use HTML Smuggling, which is able to infiltrate unidentified by traditional security mechanisms by placing infectious data in permitted file formats.
- Hidden Macro 4.0: this technique affects files with extensions .xls and .xlsx containing hidden sheets with VBA macros, the running of which caused malicious scripts to be downloaded externally.
- Formbook: this software allows criminals to access the sequence of keys typed on the keyboard, retrieve screenshots and passwords stored in browsers, and download and run external files.

CSRIT GOV classified the analysed files according to their behaviour (Table 1).

Table 1. Behavior of analyzed files/web resources



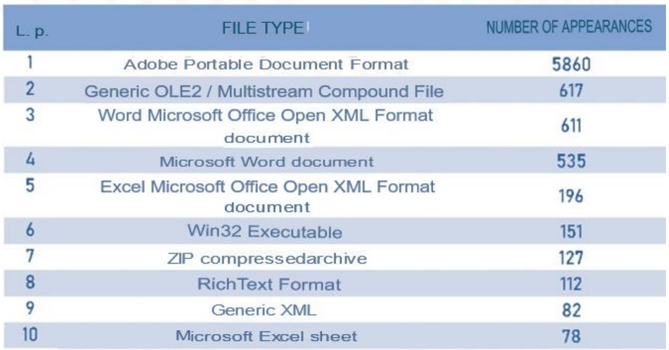
L. p.	DETECTED BEHAVIOR	NUMBER OF APPEARANCES
1	Evader	219
2	Phishing	111
3	Spreader, Evader	57
4	Trojan, Evader	54
5	Trojan, Spyware, Evader	52
6	Exploiter	39
7	Trojan	33
8	Exploiter, Evader	30
9	Spyware, Evader	16
10	Trojan, Exploit, Evader	11

Source: Report on the State of Poland's Cybersecurity in 2022

The most common type of malicious file behaviour is Evader, which is a type of malware that can bypass antivirus software detection systems, network prevention and detection systems (IPS, IDS) and even breach firewalls. A real threat is also posed by i.e. Spreader (an initially small viral file grows in size when injected), Trojan, Exploiter (a code or programme that exploits a security weakness in an application or system) and Spyware (used to steal data from a device and share it without the owner's permission).

It is worth noting the types of malicious files used by criminals to carry out the attack (Table 2).

Table 2. Most common file types



L. p.	FILE TYPE	NUMBER OF APPEARANCES
1	Adobe Portable Document Format	5860
2	Generic OLE2 / Multistream Compound File	617
3	Word Microsoft Office Open XML Format document	611
4	Microsoft Word document	535
5	Excel Microsoft Office Open XML Format document	196
6	Win32 Executable	151
7	ZIP compressedarchive	127
8	RichText Format	112
9	Generic XML	82
10	Microsoft Excel sheet	78

Source: Source: Report on the State of Poland's Cybersecurity in 2022

Among the sources of attacks by country of origin, those from the United States, Russia and China account for the largest proportion (Fig. 12).

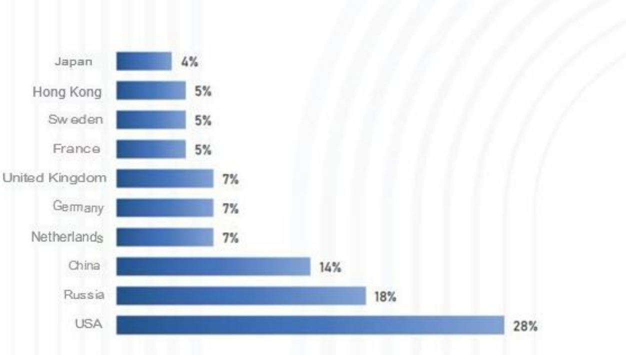


Fig. 12. Distribution of souces of attacks on networks monitored by the ARAKS GOV system for number of generated flows
Source: Report on the State of Poland's Cybersecurity in 2022

Results and discussion

Analysis of risks for Polish enterprises. In 2022 in Poland, the war in Ukraine and the associated heightened alert level of CHARLIE-CRP brought the greatest cyber security concerns. Hostile Russian actions in cyberspace have increased significantly. According to KPMG statistics, as many as one in three Polish companies have experienced an increase in the intensity of cyberattacks, with one in five companies linking these attacks to the ongoing war across the eastern border.

As in previous years, organised cybercrime groups remain the biggest threat, although solo hackers are also a real concern. Concern is particularly high against criminal groups from outside the country's borders. Concern over advanced targeted attacks (APTs) has increased significantly.

Despite the increase in real threats in cyberspace, Polish companies still do not put enough emphasis on monitoring the security of their own systems (as many as 57% of Polish companies). Only one in five companies has an in-house cyber attack response team, usually these services are outsourced – 81% of Polish companies use external services to protect their assets from cyber attacks. The cyber security market has almost tripled in value over the last 10 years (Fig. 13).

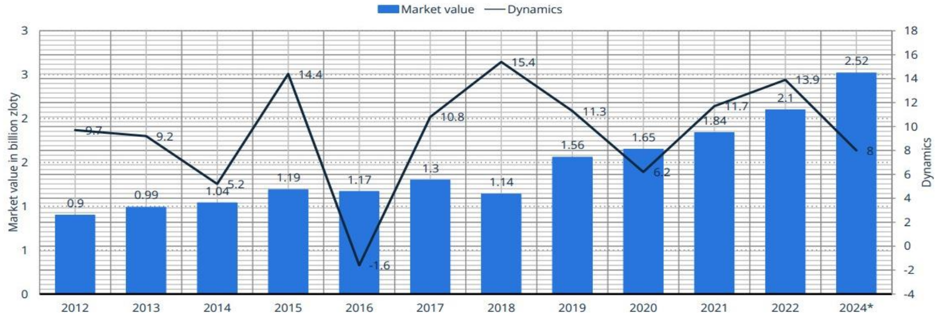


Fig. 13. Value and dynamics of the cyber security market in Poland from 2012 to 2024 (in bilion zloty)
Source: Cyber security barometer

Two-thirds of companies draw knowledge from external sources of threat information to improve threat detection internally. Among the companies surveyed, budget shortfalls (57%) and difficulties in retaining qualified staff were cited as the biggest obstacles to increasing the quality of companies' cyber security systems.

58% of Polish companies have recorded at least one incident involving a security breach, with a third of companies admitting that the intensity of attacks has increased. This statistic is the highest in 5 years. KPMG's research has never shown such a high percentage of companies - as high as 12% – that recorded more than 30 cyber incidents in a year, as was recorded in 2022. One in three Polish companies in 2022 came into contact with a ransomware attack, but all of them were repelled without paying a ransom and without disruption to business continuity (Fig. 14).

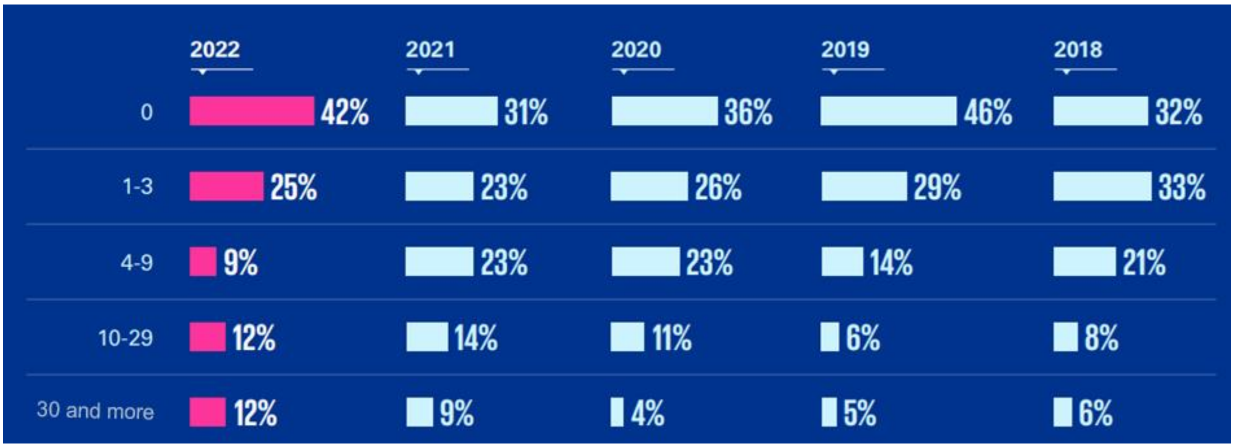


Fig 14. The number of incidents registered by companies that threaten the cyberseucirty of the company
Source: Cyber security barometer

Entities posing a threat to Polish companies in 2019–2023 [%] (Fig. 15–21).

It can be seen that there is a trend of an increase in recent years in the threat from organised groups such as criminal groups, cyber-terrorists and foreign-backed groups. At the same time, the threat from individual, non-professional individuals has decreased (individual hackers, 'internet kids', employees). This indicates an increase in the skills of cyber criminals and the growing use of cyberattacks by criminals and foreign states for warfare and terrorism.

Currently, the biggest risks among Polish entities in terms of risk are:

1. Phishing;
2. Malware;
3. Data theft by employees;
4. Ransomware.

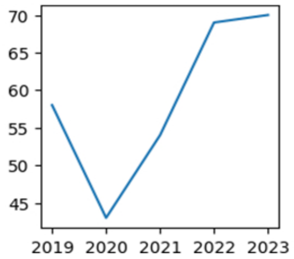


Fig. 15. Organized crime Groups
Source: Cybersecurity Barometer

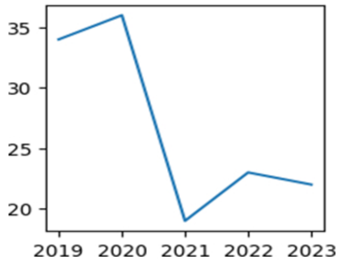


Fig. 16. Internet nursery
Source: Cybersecurity Barometer

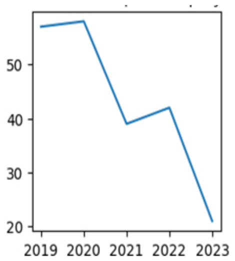


Fig. 17. Dissatisfied or underpaid employees
Source: Cybersecurity Barometer

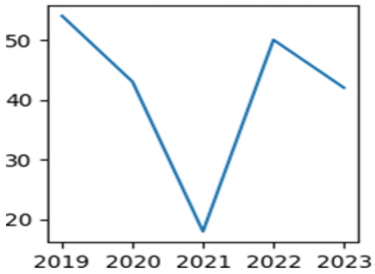


Fig. 18. Cyber-terrorits
Source: Cybersecurity Barometer

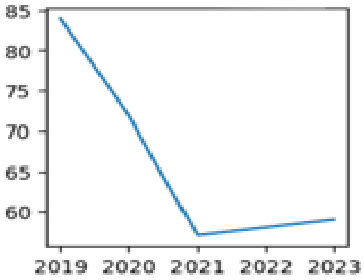


Fig. 19. Single hackers
Source: Cybersecurity Barometer

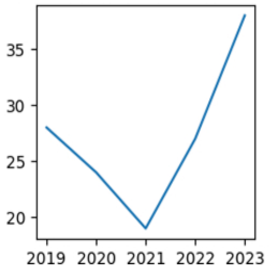


Fig. 20. Groups supported by foreign countries
Source: Cybersecurity Barometer

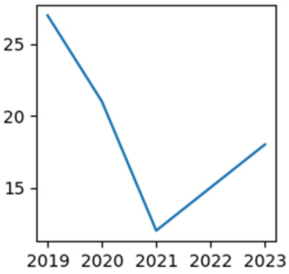


Fig. 21. Hacktivists
Source: Cybersecurity Barometer

Attacks exploiting flaws in applications. Polish companies have, to a fairly large extent, reached maturity in the areas of malware protection, internal network security, internet contact security, security incident response, identity and access management, development of business continuity plans, security monitoring and employee cyber security training. Unfortunately, there are areas where Polish companies often lack adequate security. These are primarily:

1. Safety in programming production processes.
2. Security management of business partners.
3. Mobile device security management.
4. Vulnerability management.
5. Classification and control of assets.
6. Protection against data leaks.

In addition, planned spending by companies to strengthen their cyber security areas often does not include items from the above list (Cybersecurity Predictions).

Conclusions

According to this year's predictions made by Google's cyber security, detection and counter-attack specialists, cybercriminals can be expected to specialise primarily in artificial intelligence in the near future. Generative AI and Large Language Models (LLMs) will be used in phishing, for sending fake text messages and in social engineering techniques to generate more credible content, including video and audio. Previously easy to detect typos, phrases and errors specific to phishing messages will become increasingly difficult to recognise. Artificial intelligence, moreover, will make it possible to carry out phishing campaigns on a much larger scale than before, while personalising their attacks using data on, for example, employees of an organisation. Fake news, deepfakes and phone calls generated by generative AI will also pose a significant threat. Generative AI and LLM will be offered as a service to criminals (as a Service) (Cybersecurity Threat).

On the other hand, Gen AI and Big Data analytics will be used by cyber security professionals to detect and protect against cyber attacks.

Google predicts that the main threat in the future will come from cybercrime groups from China, Russia, North Korea and Iran. Cybercriminals will continue to use zero-day vulnerabilities. An upward trend will be noted in the sphere of cybercriminals' influence on state politics, extortion attacks and hacktivism (especially from Russia, Hamas and Israel) involving DDoS attacks, data leaks and information distortion. States will want to arm themselves with wiper malware. Infrastructure in space may also prove vulnerable to cyber attacks. Cyber espionage and so-called 'sleeper botnets' are forecast to continue to grow.

The rise of attacks on hybrid and multi-cloud environments is almost certain, to which serverless cloud services will be more readily exploited by attackers. Furthermore, according to Google, criminals will reuse old attack techniques, make greater use of modern programming languages (e.g. Go, Rust and Swift), will attack supply chain IT systems and will increase activity in criminal activity involving mobile devices (Incident statistics in Poland).

With mankind's increasing integration with cyberspace in every area of life, the development of artificial intelligence, particularly generative AI, it is natural for cybercriminals to increase their exploitation of system weaknesses and knowledge gaps among humansand the use of an increasingly sophisticated and larger-scale variety of attack types. The upward trend of cyber threats to date is likely to continue, but the level of damage caused by attacks, malware and social engineering depends on the response of cyber security professionals, increased prevention efforts to protect security and privacy, as well as continuing to educate the public about the new threats that exist in cyberspace, with the aforementioned factors fortunately also improving continuously.

References

Cybercrime and cybersecurity in Poland. Statista: 2023. Report on the state of Poland's cybersecurity in 2022: CSRIT GOV (Computer Security Incident Response Team). https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [12.10.2024].

Cybersecurity Barometer. KPMG. https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/02/pl-raport-kpmg-w-polsce-barometr-cyberbezpieczenstwa-2023-secured.pdf [13.10.2024].

Cybersecurity Predictions. Google Threat Analysis Group 2024. https://cloud.google.com/security/resources/cybersecurity-forecast?hl=pl [14.10.2024].

Cybersecurity Threat Report. Sophos 2022. https://www.datapac.com/sophos-2022-threat-report/ [14.10.2024].

ENISA Threat Landscape 2023. ENISA (The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [10.10.2024].

Incident statistics in Poland. CERT Polska 2022. https://cert.pl/en/uploads/docs/Report_CP_2022.pdf [15.10.2024].

National Vulnerability Database (NVD). National Institute of Standards and Technology (NIST) https://nvd.nist.gov [11.10.2024].