

Phishing, oszustwa w sieci i ransomware.

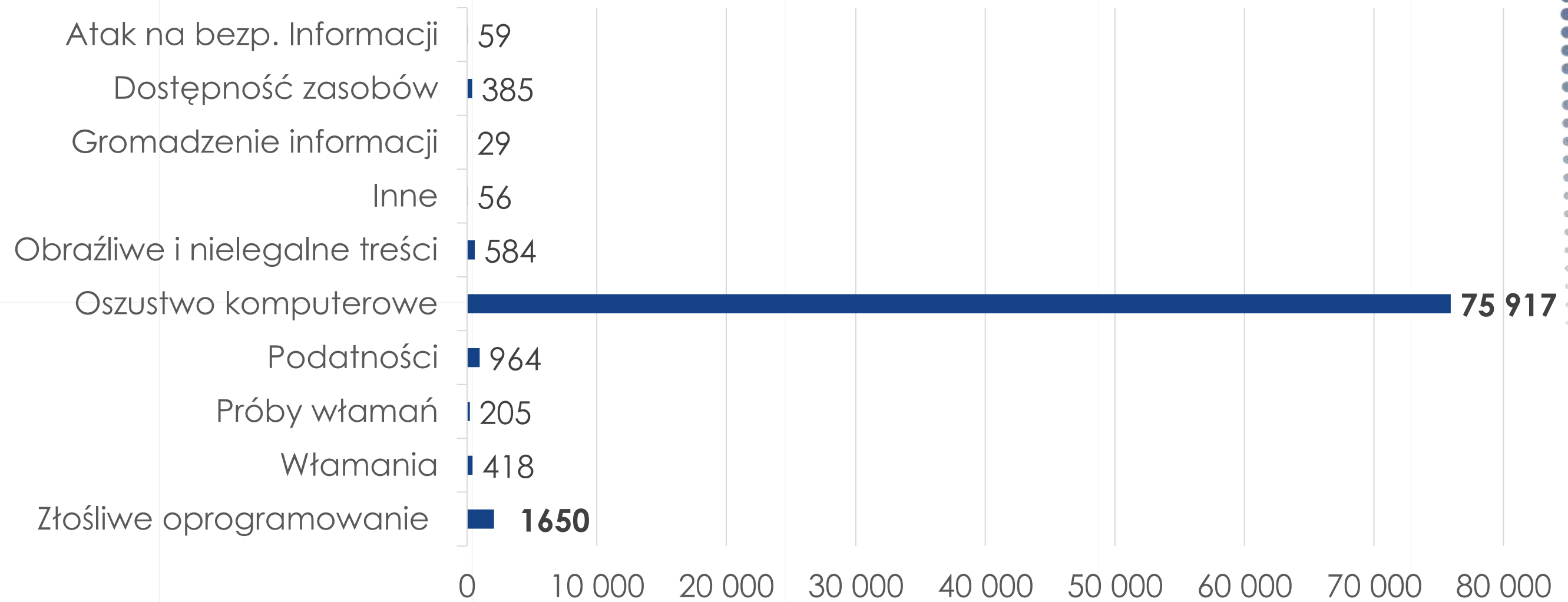
Najpowszechniejsze cyberzagrożenia
– jak rozpoznać, jak zapobiegać

Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa
NASK – PIB

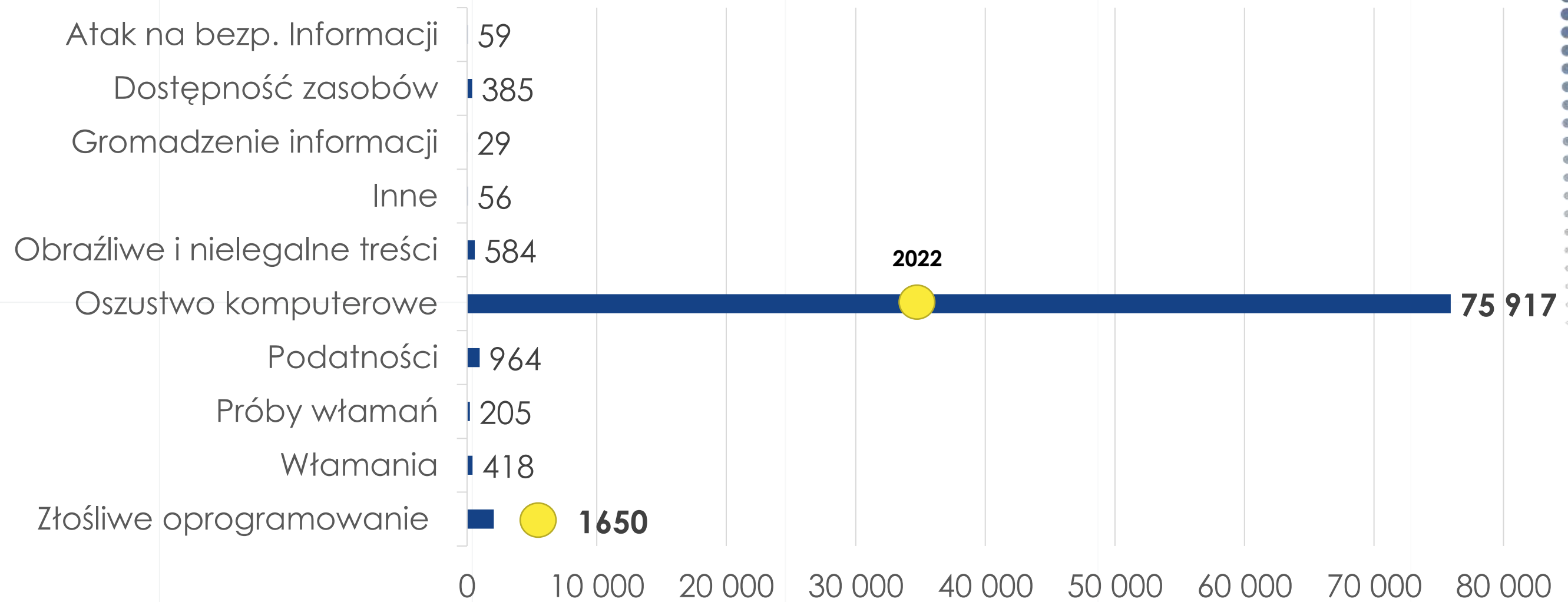
Cyberzagrożenia w liczbach

– statystyki incydentów zgłaszanych do CERT POLSKA

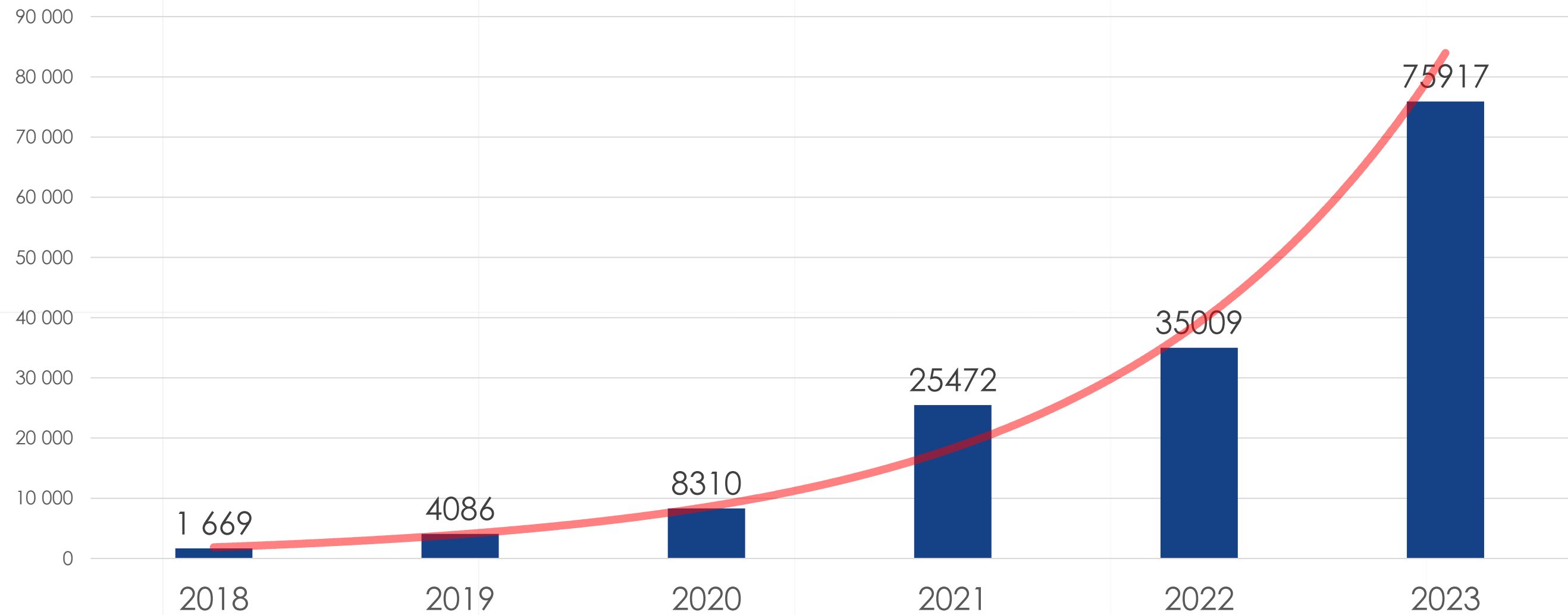
Incydenty zarejestrowane przez CERT Polska w 2023 roku



Incydenty zarejestrowane przez CERT Polska w 2023 roku



Oszustwa zarejestrowane przez CERT Polska w latach 2018-2023





Phishing

– Metody ataku i socjotechnika

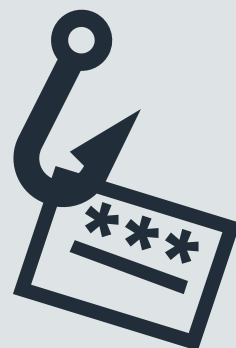
Phishing

Popularny atak socjotechniczny.

Wprowadzenie ofiary w błąd poprzez **podszycanie się pod zaufany podmiot lub osobę**.

Wykorzystanie **falszywych** wiadomości, **podrobionych** stron internetowych, nieprawdziwych informacji itp.

Cele ataku:



Przejęcie poufnych danych



Kradzież pieniędzy



Instalacja złośliwego oprogramowania

W jaki sposób jesteśmy atakowani?



W mailach



SMSami



Przez telefon



W reklamach,
mediach
społecznościowych,
przez kod QR itp.

Granie na **emocjach** odbiorców



– Należy dokonać pilnej płatności!

– Potrzebna jest twoja pomoc!



– Stało się coś strasznego!

– Ktoś Cię okrada!



– Wygrywasz na loterii!

Jak to wygląda w praktyce?




Phishing masowy


- Wysyłka fałszywych wiadomości do **setek/tysięcy odbiorców**;
- Pretekst kontaktu i historia wykorzystana do ataku jest **uniwersalna**;
- Liczy się **skala ataku**, bo tylko odsetek odbiorców uda się w ten sposób oszukać.



Podszywanie się pod instytucje publiczne

 **Powiadomienie o zwrocie środków**

From **Ministerstwo Finansów - Portal Gov.pl** <support@widok.justsport.it>
To [Redacted]
Date **Today 11:19**

 | Serwis Rzeczypospolitej Polskiej

Portal podatkowy


Drodzy Klienci,

Masz prawo do zwrotu podatku w wysokości **634.79 PLN**
Prześlij poniższy formularz, abyśmy mogli go przetworzyć
Prosimy o jak najszybszy zwrot pieniędzy.

[Uzyskaj dostęp do formularza](#)

Kontynuacja procesu zwrotu kosztów może zająć do 24 godzin.
Ten proces może zostać opóźniony, jeśli formularz zwrotu nie zostanie prawidłowo przesłany

20:04
◀ Messenger


+48 [Redacted]

Wiadomość
Dzisiaj, 12:05

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

Szanowni Pasazerowie,

Jesteśmy zespołem PKP Intercity i chcemy poznać Wasze opinie na temat doświadczeń związanych z podróżowaniem naszymi pociągami. Wasza opinia jest dla nas niezwykle ważna, dlatego serdecznie zapraszamy do wzięcia udziału w naszej krótkiej ankiecie.

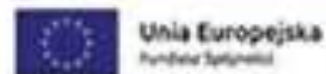
Aby wyrazić naszą wdzięczność za poświęcenie czasu na wypełnienie ankiety, każdy uczestnik ma szansę wygrać nagrodę w wysokości 244,21 PLN. Po zakończeniu ankiety

[Kliknij tutaj](#) : [Weź udział teraz](#)

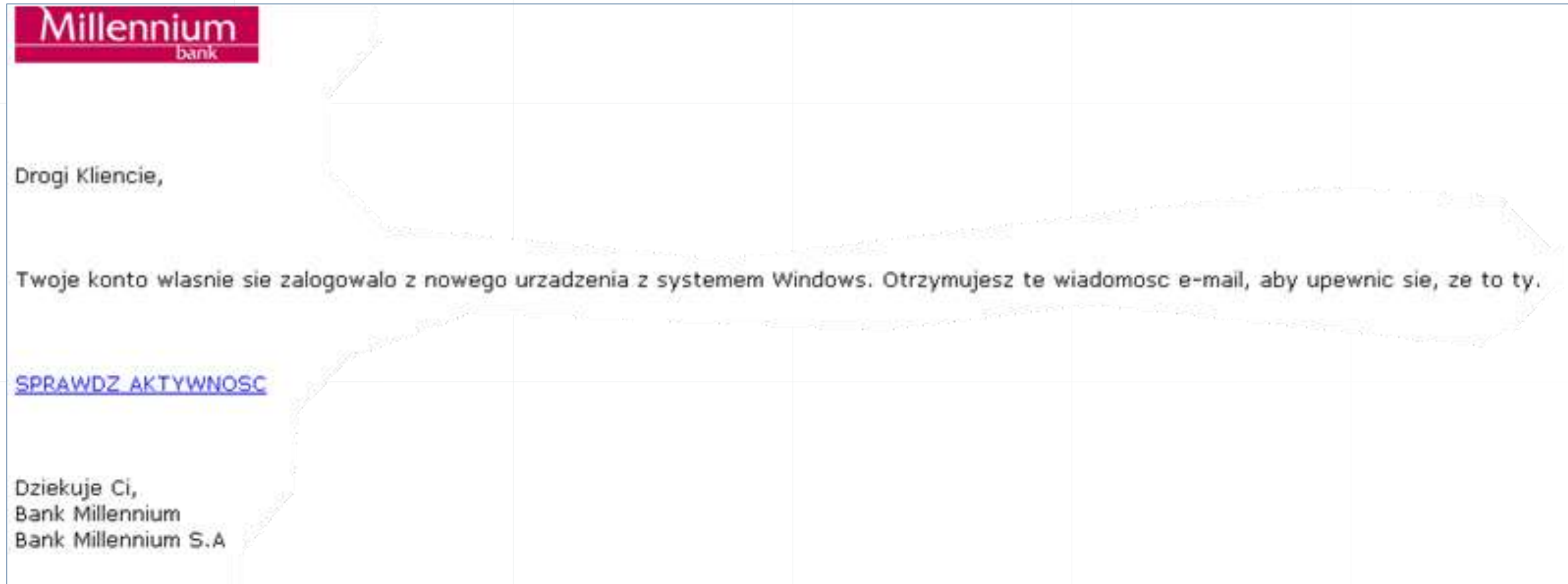
Wasze odpowiedzi będą traktowane w pełnej poufności i posłużą nam do dalszego doskonalenia naszych usług.

Dziękujemy za wsparcie i uczestnictwo w tej ankiecie. Czekamy na Wasze cenne opinie!

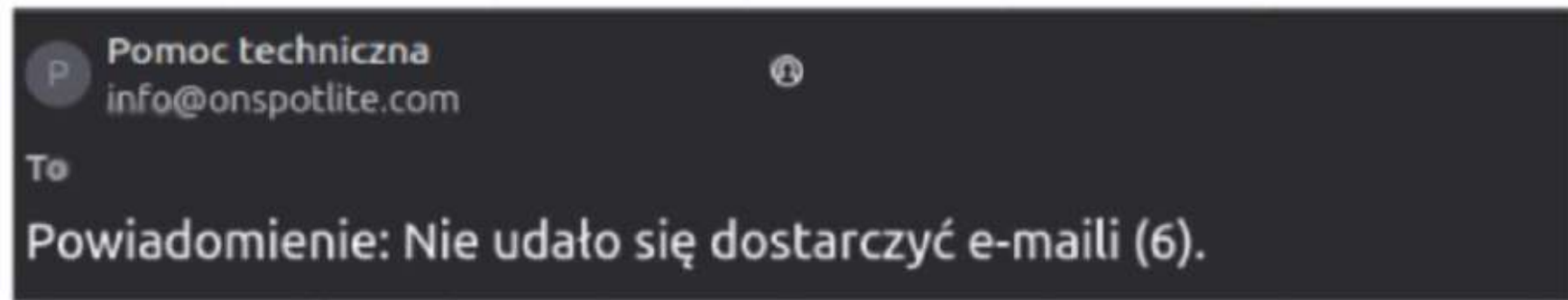
Z wyrazami szacunku,
Zespół PKP Intercity



Podszywanie się pod banki



Podszywanie się pod pomoc techniczną



Informacja o
niepowodzeniu

Konieczne są działania

biuro
Odbiorca

Powiadomienie o niepowodzeniu odbioru wiadomości.

UWAGA

Masz zawieszoną wiadomość przychodzącą
Popraw poniżej

Zezwalaj na wiadomości

Przejrzyj Wiadomości

powiadomienie

Wiadomości techniczne



szoi@nfz-centrala.pl

Wczoraj

Do: [Redacted]

Aktualizacja systemu SZOI

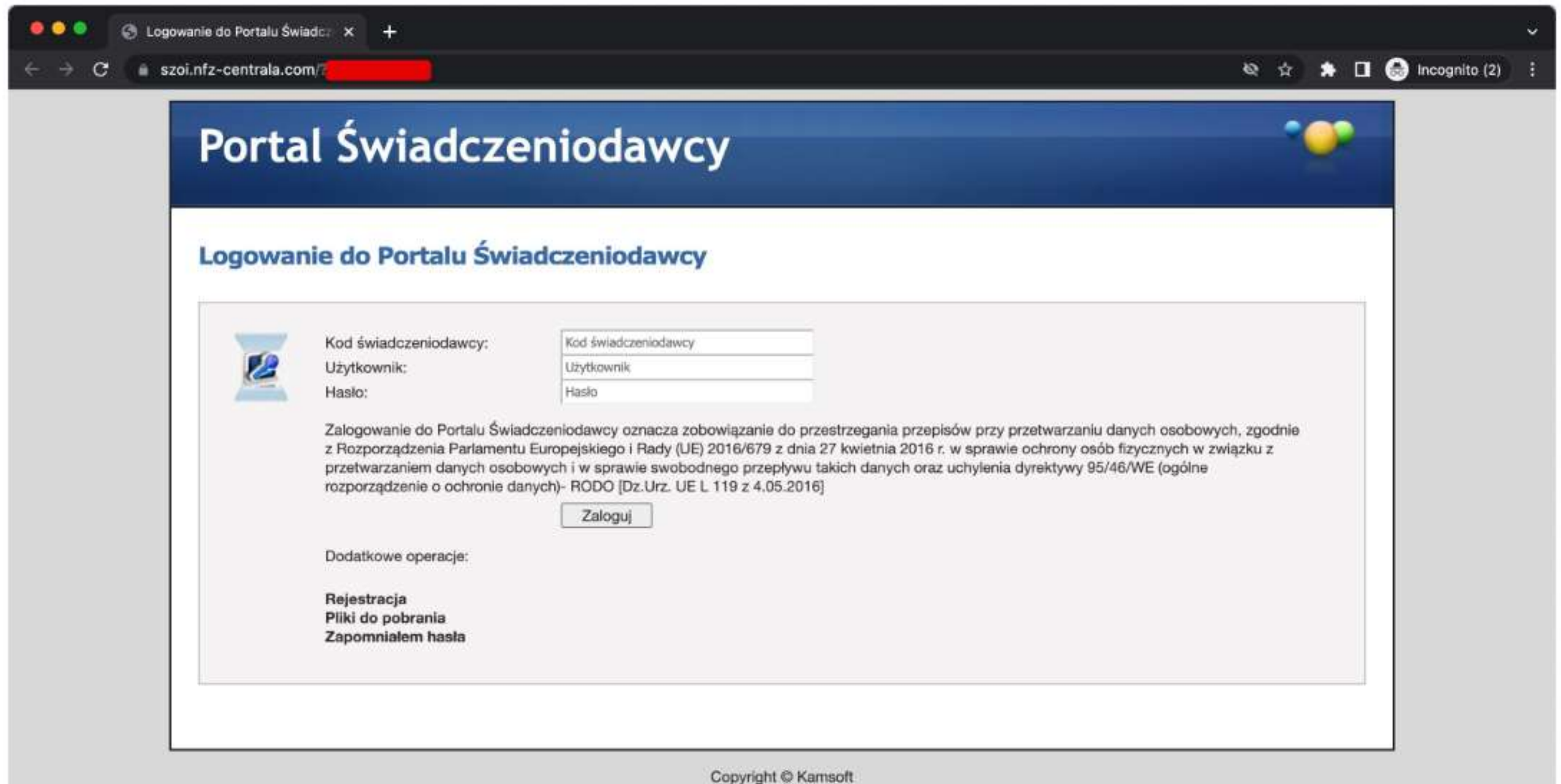
Informujemy, że w dniu dzisiejszym nastąpiła aktualizacja systemu SZOI dostarczanego przez Kamsoft. Prosimy o zalogowanie do systemu, aby zsynchronizować dane z poprzedniej wersji.

[Logowanie do systemu](#)

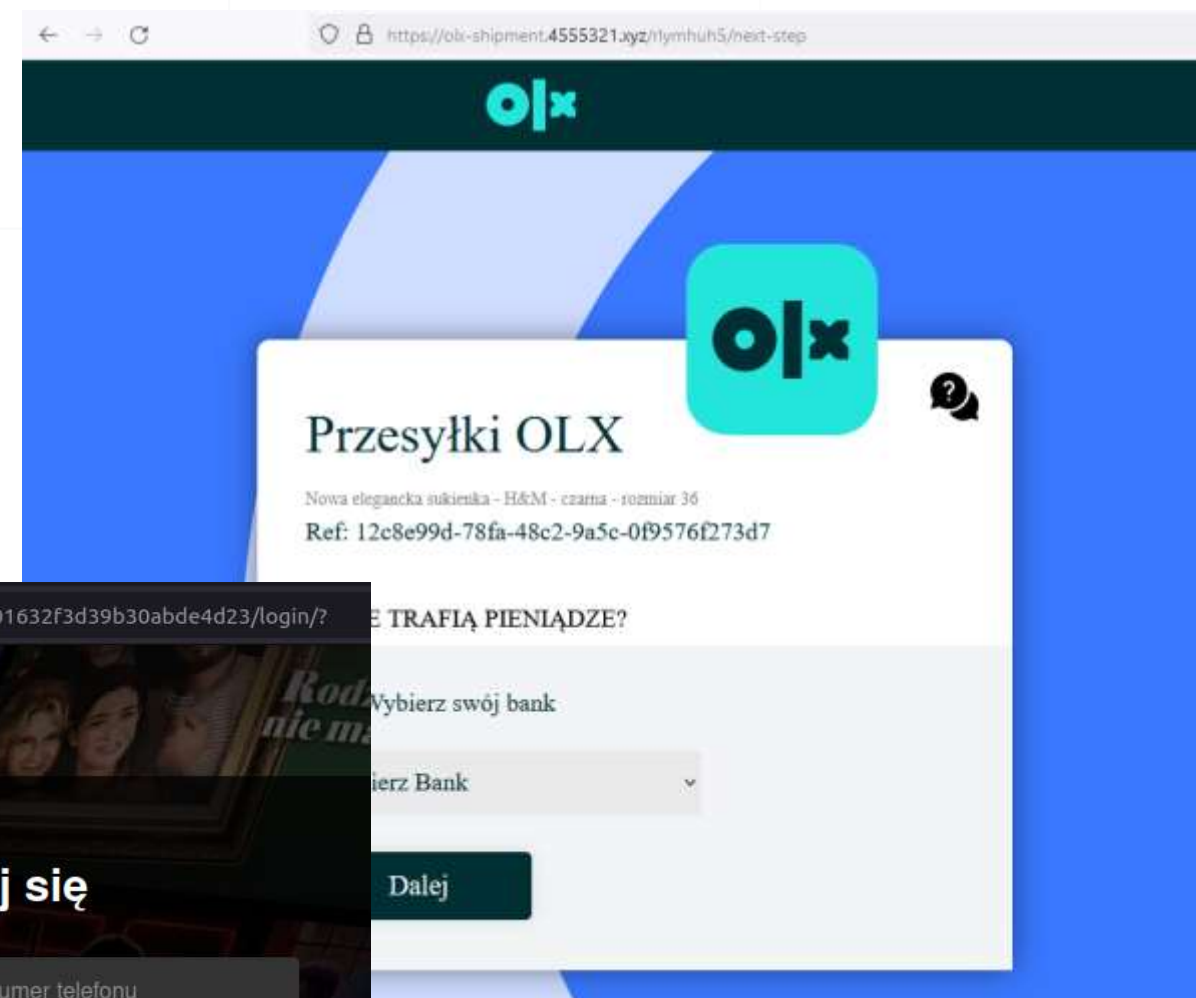
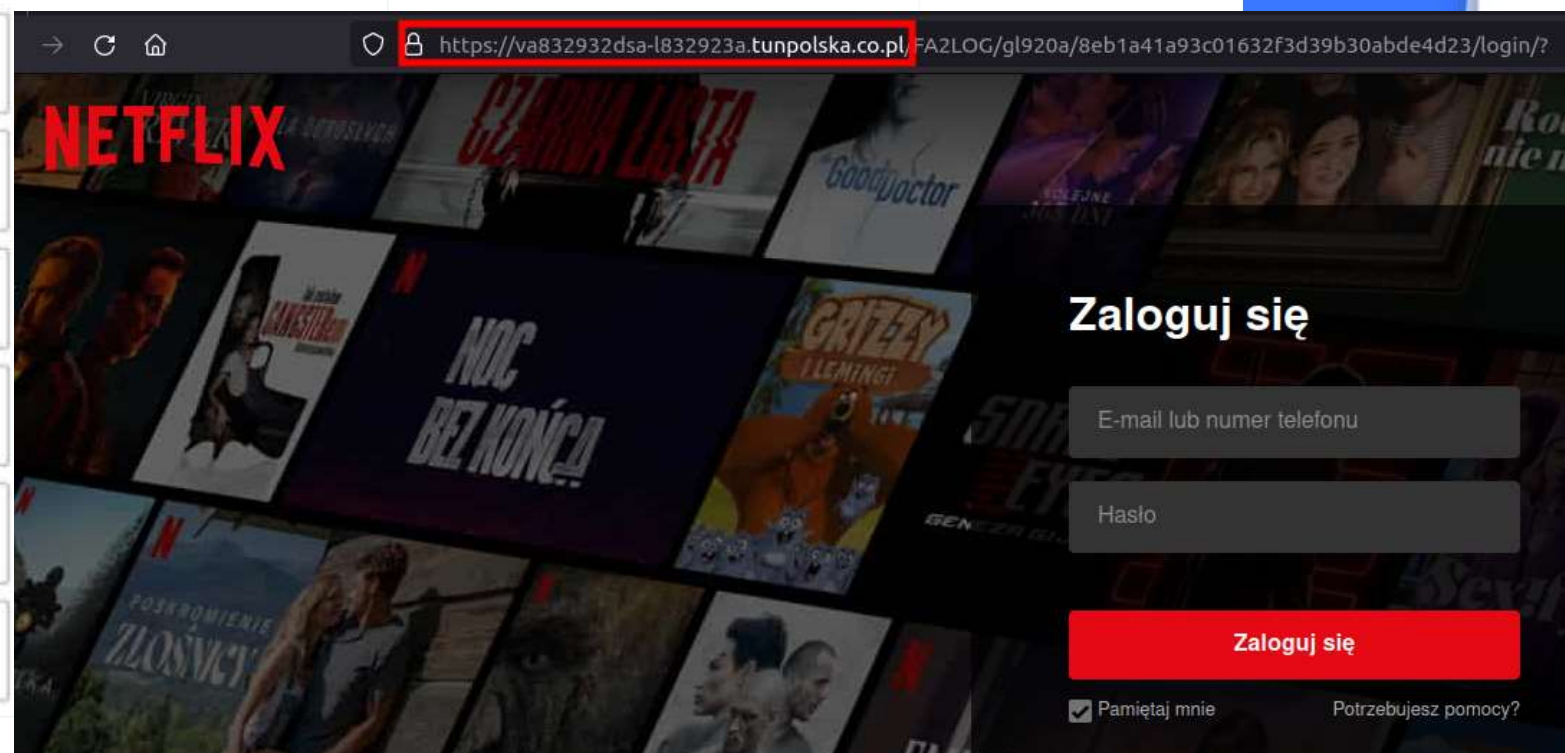
Ta wiadomość została wysłana automatycznie. Informacja dotycząca przetwarzania danych osobowych przez Narodowy Fundusz Zdrowia (NFZ) w zakresie realizacji zadań statutowych i obowiązków ustawowych

■ Administratorem Pani/Pana danych osobowych jest Narodowy Fundusz Zdrowia z siedzibą w Warszawie, ul. Rakowiecka 26/30, 00-500 Warszawa

Fałszywy panel do logowania do systemu



Inne przykłady – podszywanie się pod popularne serwisy



Sign in to manage your property

Username

Also known as 'Login name' and 'Email address'

Next

[Having trouble signing in?](#)

Do you have questions about your property or the extranet? Visit [Partner Help](#) or ask another question on the [Partner Community](#).

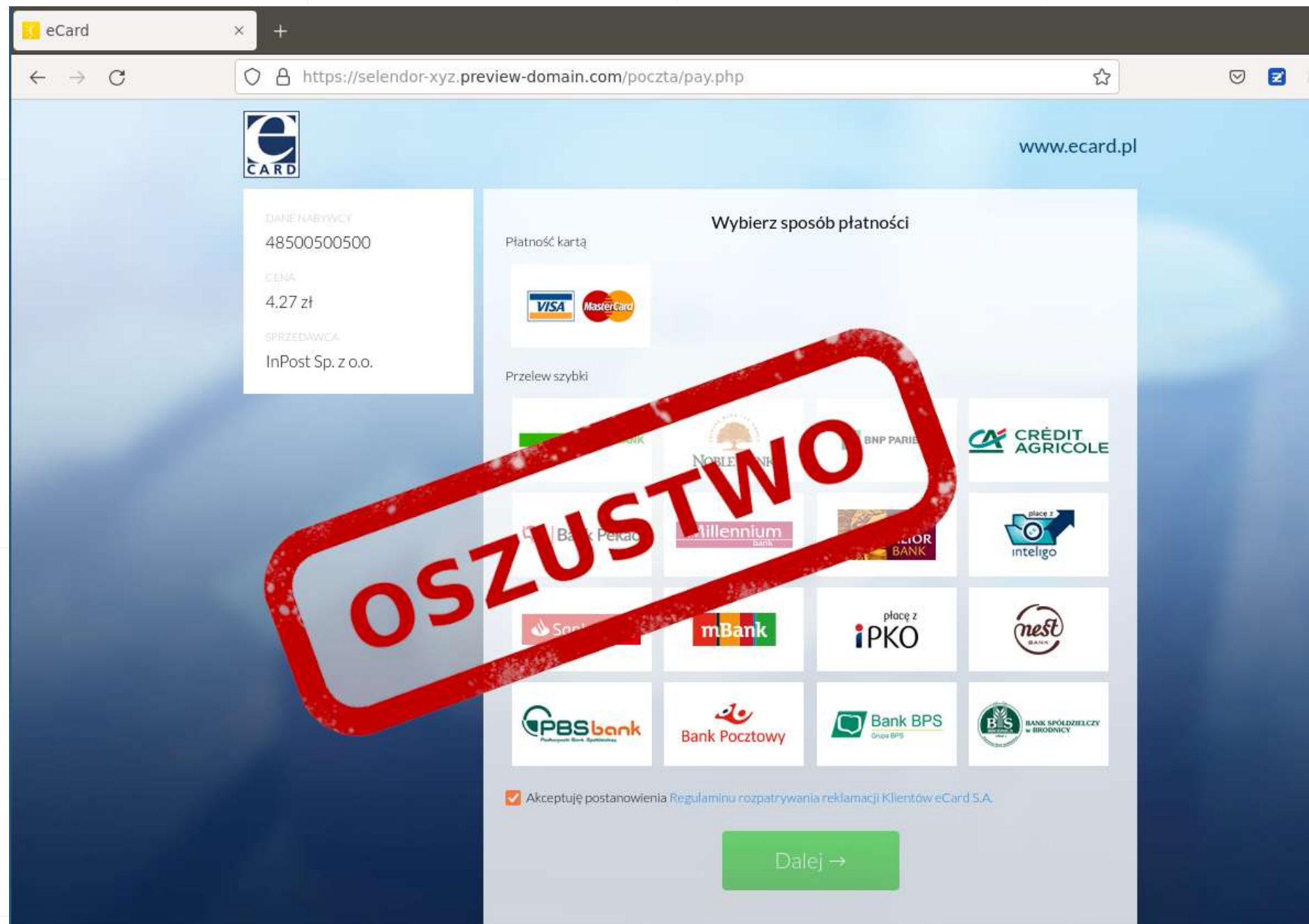
[Create your partner account](#)

By signing in or creating an account, you agree with our [Terms & conditions](#) and [Privacy statement](#).

All rights reserved.

Copyright (2006 - 2024) - Booking.com™

Fałszywe bramki płatności



Opłaty, nadpłaty, ankiety w SMSach



PGE: Na dzień 23.04 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności 10.50 zł Zapłac teraz na <https://luminnotik.store/>

10:33

20:04

◀ Messenger



+48 [redacted]

Wiadomość
Dzisiaj, 12:05

Akcja Ministerstwa Finansów!
Wypełnij krótka ankietę i zyskaj 250 zł na swoje konto
<https://min-fin.live/ystd>

Wyłudzenie danych i środków pieniężnych

10:24

Niezabezpieczona — paczkomat24.xyz

InPost

Płatności online

Zamierzasz uregulować należność za paczkę oczekującą w Paczkomacie.
Poniżej znajdziesz szczegóły płatności.

Paczka numer: **604086896000449218079098**

Wartość pobrania: **0,50 zł**

Imię

Nazwisko

Akceptuję regulamin

Dalej →

REZYGNUJĘ

10:25

Niezabezpieczona — paczkomat24.xyz

eCARD www.ecard.pl

DATA NAGYWCY
Test Test

CENA
0.50 PLN

SPRODUWCA
InPost Sp. z o.o.

Wybierz sposób płatności
Przelew szybki

10:25

Niezabezpieczona — paczkomat24.xyz

Santander Przelew24

Płacisz za:
32893730;176699000; DLA InPost nr zam 32893730 paczkomaty.pl

Płacisz w:
PayPro SA
PayPro SA

Kwota: **0.50 PLN**

Zaloguj się i potwierdź transakcję smsKodem, tokenem lub Mobilnym podpisem.

Przelew24

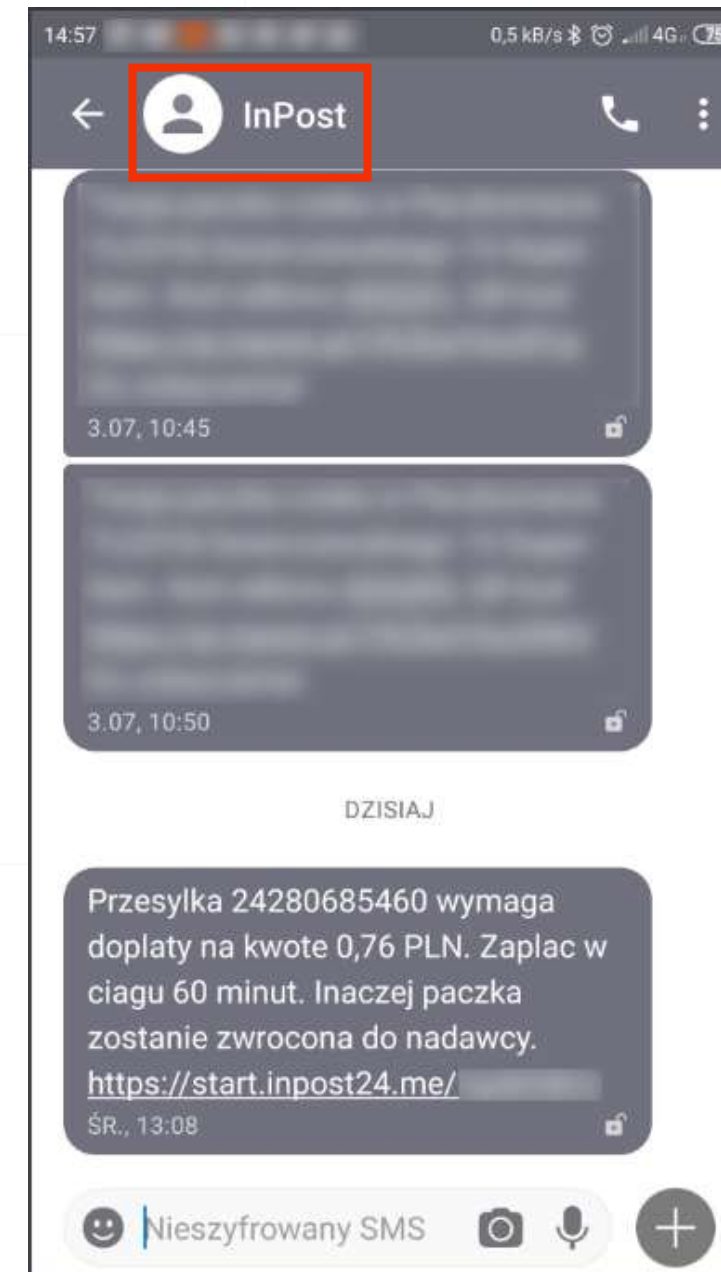
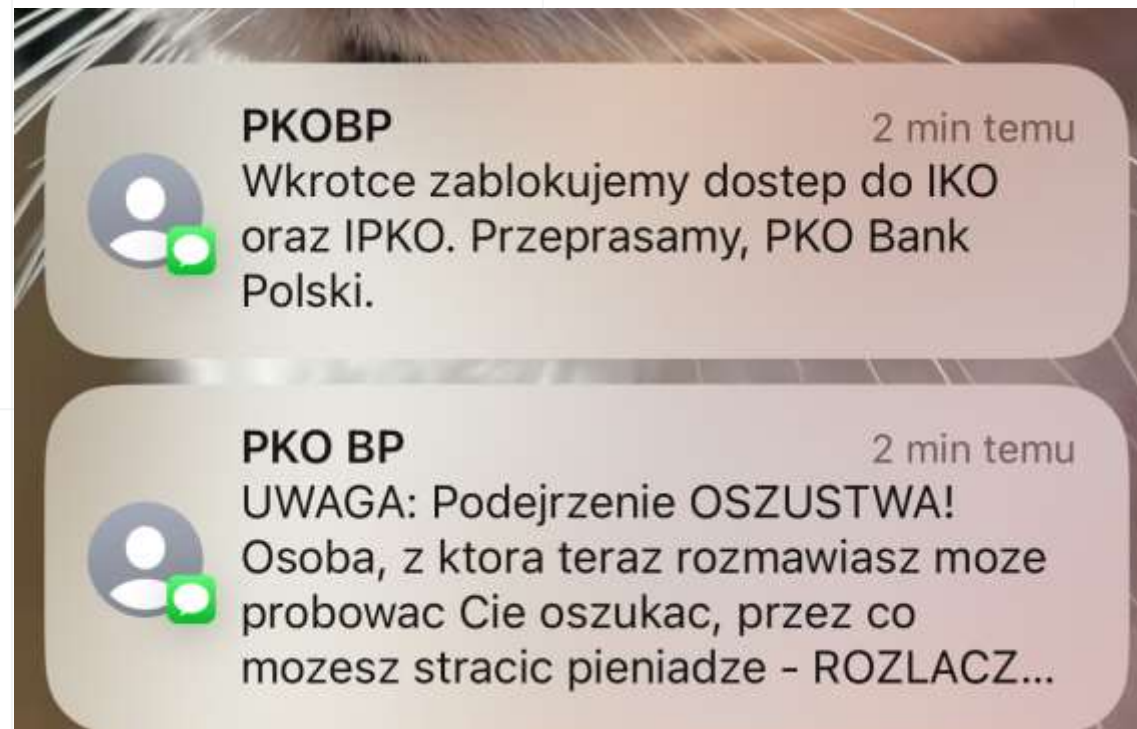
Przelew24 KROK 1

Wpisz login

Dalej

Problem z logowaniem? Zresetuj swoje hasło

Uwaga na **spoofing**,
czyli **podszycanie się pod zaufany numer telefonu!**





Inne oszustwa

- Metody ataku i socjotechnika

Fałszywe reklamy, fałszywe strony

millennium

Wszystko Mapy Wiadomości Grafika

Około 376 000 000 wyników (0,47 s)

Wyniki dla lokalizacji **os.Łomianki Baczyńskiego...**

Reklama · <https://www.millenniumpl.com/>

Zaloguj się - Millennium

Zaloguj się z dowolnego miejsca na świecie, bądź na bieżąco z nowymi
Pomożemy Ci z każdym problemem, nasi eksperci są zawsze pod ręką.

<https://www.bankmillennium.pl>

Bank Millennium: Klienci Indywidualni - Konta, pożyczki

Najlepsza oferta dla klientów indywidualnych, firm, przedsiębiorstw. Bank
kredyty hipoteczne, konta, karty, inwestycje - złóż wniosek ...

Oszuści podszywają się pod Bank Millennium i informują o nowych "zabezpieczeniach" - nie klikaj w link i nie podawaj danych

KLIENTY INDYWIDUALNI PRESTIGE BANKOWOŚĆ PRYWATNA FIRMY PRZEDSIĘBIORSTWA

Millennium bank

Wpisz, czego szukasz

POŻYCZ GOTÓWKĘ ZAŁÓŻ KONTO LOGOWANIE

Konta Karty Kredyty Oszczędności Inwestycje Ubezpieczenia Bankowość elektroniczna Wsparcie Kontakt

Otwórz się na **nowe możliwości**

Wybierz konto Millennium 360° z innowacyjną aplikacją

ZALÓŻ TERAZ DOWIEDZ SIĘ WIĘCEJ

Nota prawna

MILLENNIUM 360°
Prowadzone zawsze za 0 zł

KARTA IMPRESJA (RRSO 25,68%)
Loteria do 5.01.2023

POŻYCZKA GOTÓWKOWA (RRSO 12,83%)
Promocja do 20 stycznia 2023

ZWROTY ZA ZAKUPY
Przemysłowy sposób na zakupy

Oszustwa w mediach społecznościowych

MEBLE UŻYWANE I GRATY WARSZAWA

17h

Hania została zgwałcona... Musicie nam pomóc, szukamy sprawcy, w artykule jest nagranie z tego zdarzenia :(Jeśli możesz, udostępnij ten post gdzie się da, w innych grupach, u siebie na profilu... Razem uda się na pewno



WIADOMOSCI.WP.PL

Szukają podejrzanego o gwałt na nieletniej. Policja prosi o pomoc

Policjanci z Łodzi prowadzą poszukiwania mężczyzny podejrzanego o gwałt na nieletniej dziewczynce...

10 Comments 216 Shares

Like Comment Share

Grupa Stary dawny Szczecin

7m

w 14 sekundzie widać, że panu komornikowi się chyba podoba, tak jęczy i się wypina hahah, albo to ból. W sumie gościu z marszu ściągnął spodnie, i mu włożył hahahah



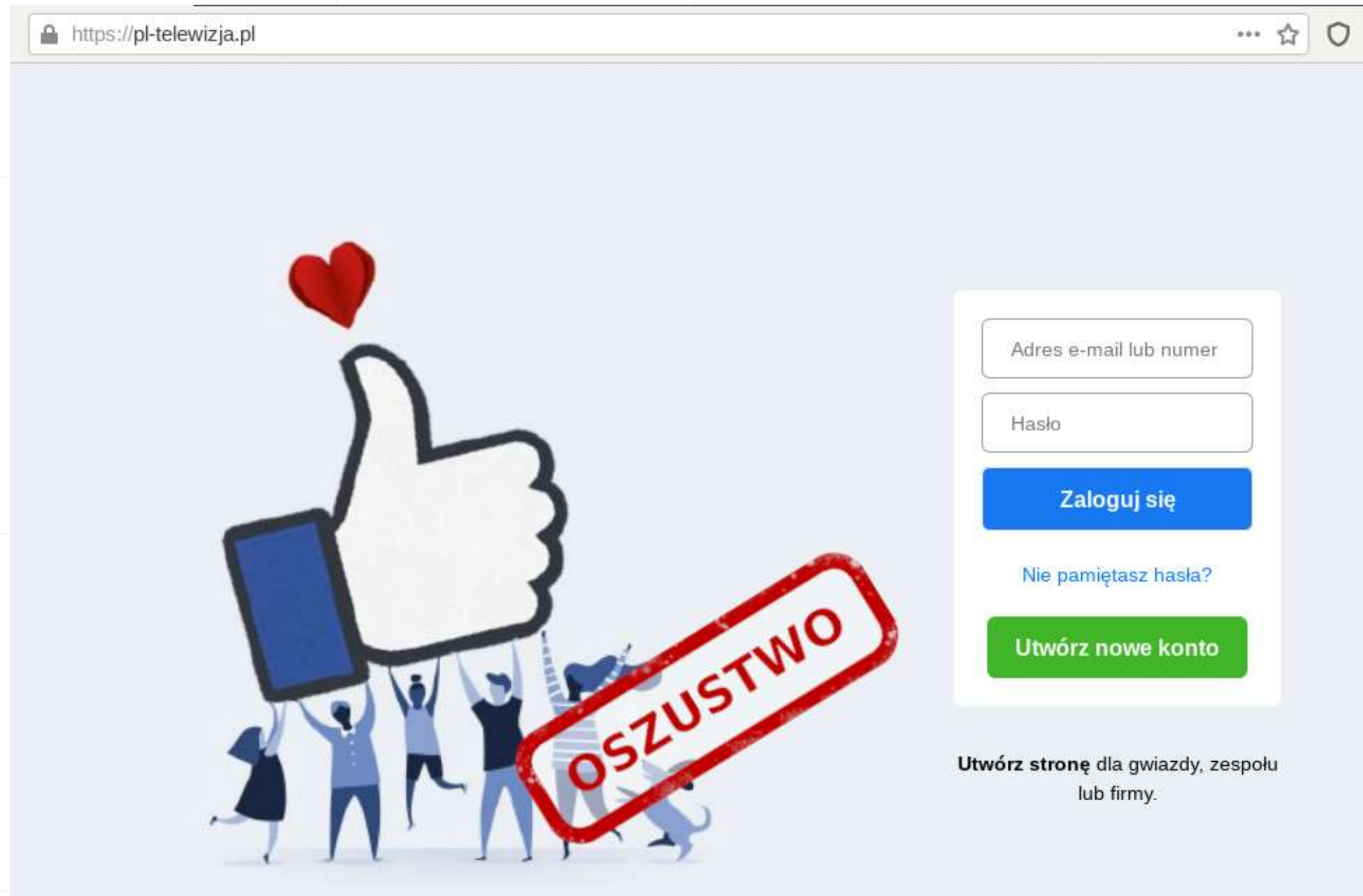
PUDELEK-ONET-43856872713.AZUREEDGE.NET

Szczecin: 42 latek zgwałcił Komornika , całą sytuację nagrał i udostępnił w sieci. [WIDEO]

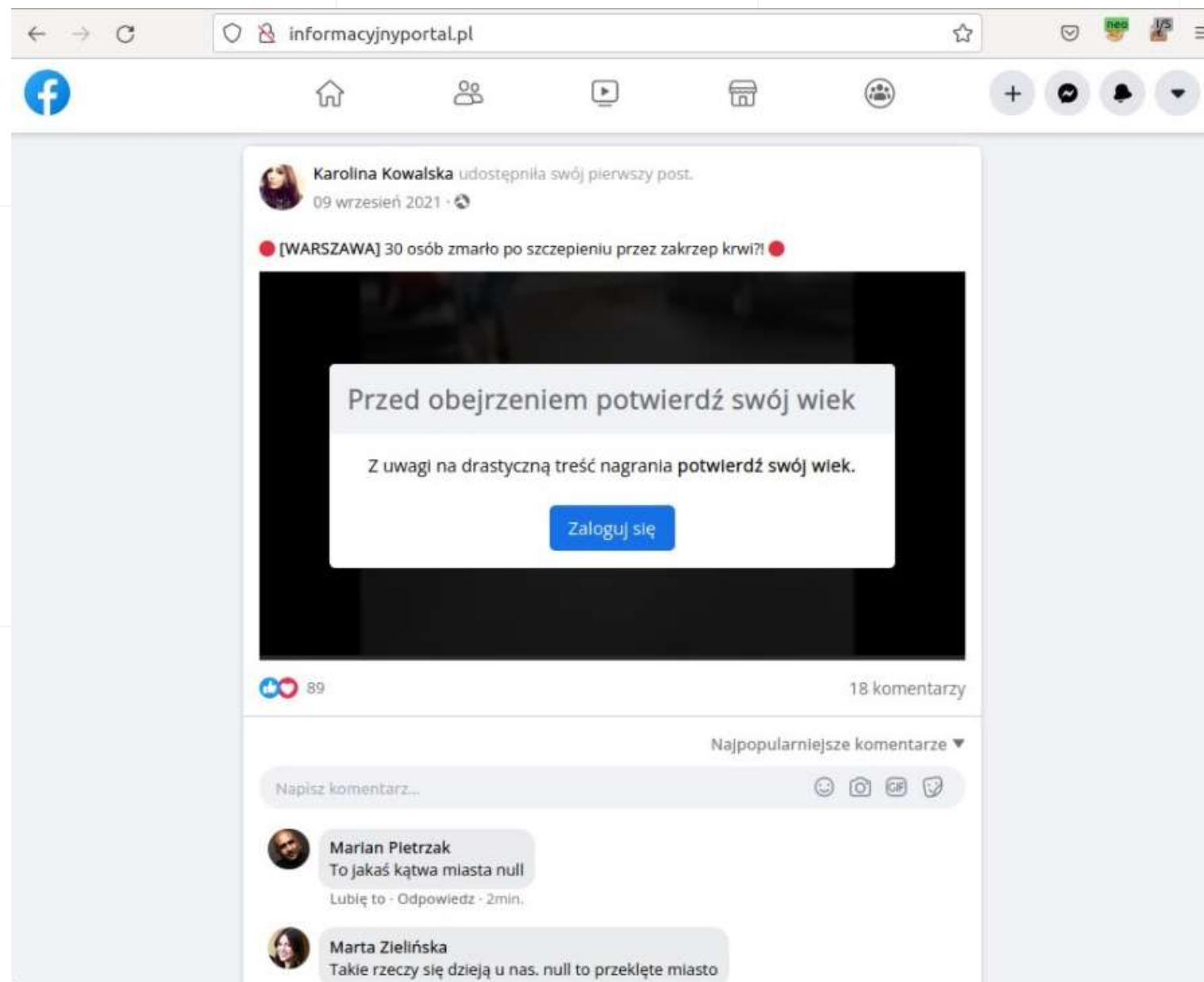
1

Like Comment Share

Ataki na użytkowników mediów społecznościowych



Konieczność „potwierdzenia wieku”

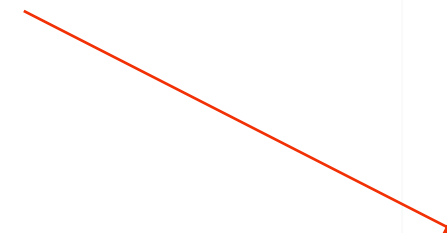
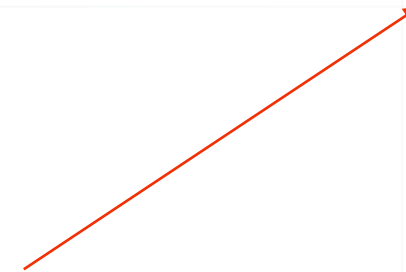


...lub inny dowolny pretekst:

- Zakupy przez facebooka
- Prośba o udział w głosowaniu itp.

Podsumowując...

Dostajemy:

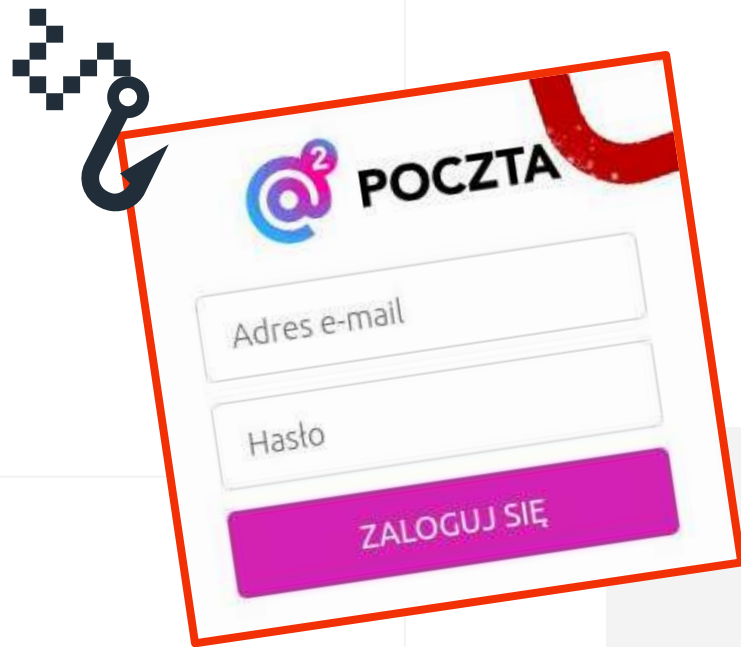


Tracimy:

Login i hasło,
czasem kod
jednorazowy

Dane **karty płatniczej/**
numer blik → pieniądze

Dane osobowe



adamek*****@o2.pl	no*****
adam*****@o2.pl	12*****
adame*****@o2.pl	me*****
adame*****@o2.pl	ad*****
adamekwitk*****@o2.pl	fb*****
adame*****@o2.pl	la*****
adamia*****@o2.pl	ku*****
adamia*****@o2.pl	ly*****



Ochrona przed phishingiem

Jak postępować po otrzymaniu **KAŻDEJ** wiadomości?

Zatrzymaj się.

Daj sobie czas na ocenę sytuacji...

Ocena sytuacji – Jak patrzeć na wiadomość?

1. Sprawdź czy **kontekst wiadomości** jest ukierunkowany na podjęcie przez ciebie szybkich działań.
2. Weryfikuj **adres domeny**, z której przyszedł e-mail (nazwa domenowa to część adresu po znaku „@”).
3. Nie daj się zwieść **pozorom** (logo, stopki, formatu i kolorystyki maili).
4. Zwracaj uwagę na **błędy językowe** (ale: wykorzystanie modeli językowych, coraz lepsza treść).

✓ Powiadomienie o zwrocie środków



From Ministerstwo Finansów - Portal Gov.pl <support@widok.justsport.it>

To

Date Today 11:19



gov.pl

Serwis Rzeczypospolitej Polskiej

Portal podatkowy

Drodzy Klienci,

Masz prawo do zwrotu podatku w wysokości **634.79 PLN**
Prześlij poniższy formularz, abyśmy mogli go przetworzyć
Prosimy o jak najszybszy zwrot pieniędzy.

[Uzyskaj dostęp do formularza](#)

Kontynuacja procesu zwrotu kosztów może zająć do 24 godzin.
Ten proces może zostać opóźniony, jeśli formularz zwrotu nie zostanie prawidłowo przesłany

Jeżeli masz wątpliwości, nie ryzykuj.

Jeżeli zauważysz któryś z wcześniej wymienionych symptomów:



nie klikaj w linki.




nie pobieraj (i nie otwieraj!) załączników.




nie odpowiadaj na wiadomość.


Zgłoś otrzymaną wiadomość do CERT Polska, a następnie usuń ją.

← → ↻ <https://epgv01.fr/httpswww.govpl/4810f/>

 Serwis Rzeczypospolitej Polskiej

Szukaj usług, informacji, wiadomości 🔍 [Mój Gov](#) 

Koronawirus: szczepienia i ważne informacje [DOWIEDZ SIĘ WIĘCEJ](#)

Ministerstwo Finansów 

O ministerstwie Co robimy Aktualności Załatw sprawę Kontakt PL ▼

[Koronawirus - WYJĄTKOWE ŚRODKI DLA FIRM I PRACOWNIKÓW](#)

Formularz zwrotu

Nazwa <input type="text"/>	Adres <input type="text"/>
Nazwisko <input type="text"/>	Miasto <input type="text"/>
Data urodzenia -- / -- / --	Kod pocztowy <input type="text"/>
Telefon <input type="text"/>	

[Naprzód](#)

Zwrot środków - dane bankowe beneficjenta

Karta kredytowa <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>	OGÓLNE INFORMACJE DOTYCZĄCE ZWROTU PIENIĘDZY
Termin ważności -- / --	
CVV (3 Dane na odwrocie) <input type="text"/>	
Naprzód	

Odbiorca zwrotu	Smiki Nowak
Jak otrzymać	Karta kredytowa
Liczba plików	21926AXD197
Kwota Refundacji	634.86 PLN
Data	26/03/2021
Warunki płatności	24 godziny



Oszustwo w rozmowie telefonicznej

– czyli **vishing** (voice phishing)

Vishing – atak telefoniczny

ang. Voice + phishing

Uniwersalny pretekst kontaktu.

Stosowanie technik manipulacji w rozmowie.



Uwaga na **spoofing**,
czyli **podszycanie się pod zaufany numer telefonu!**



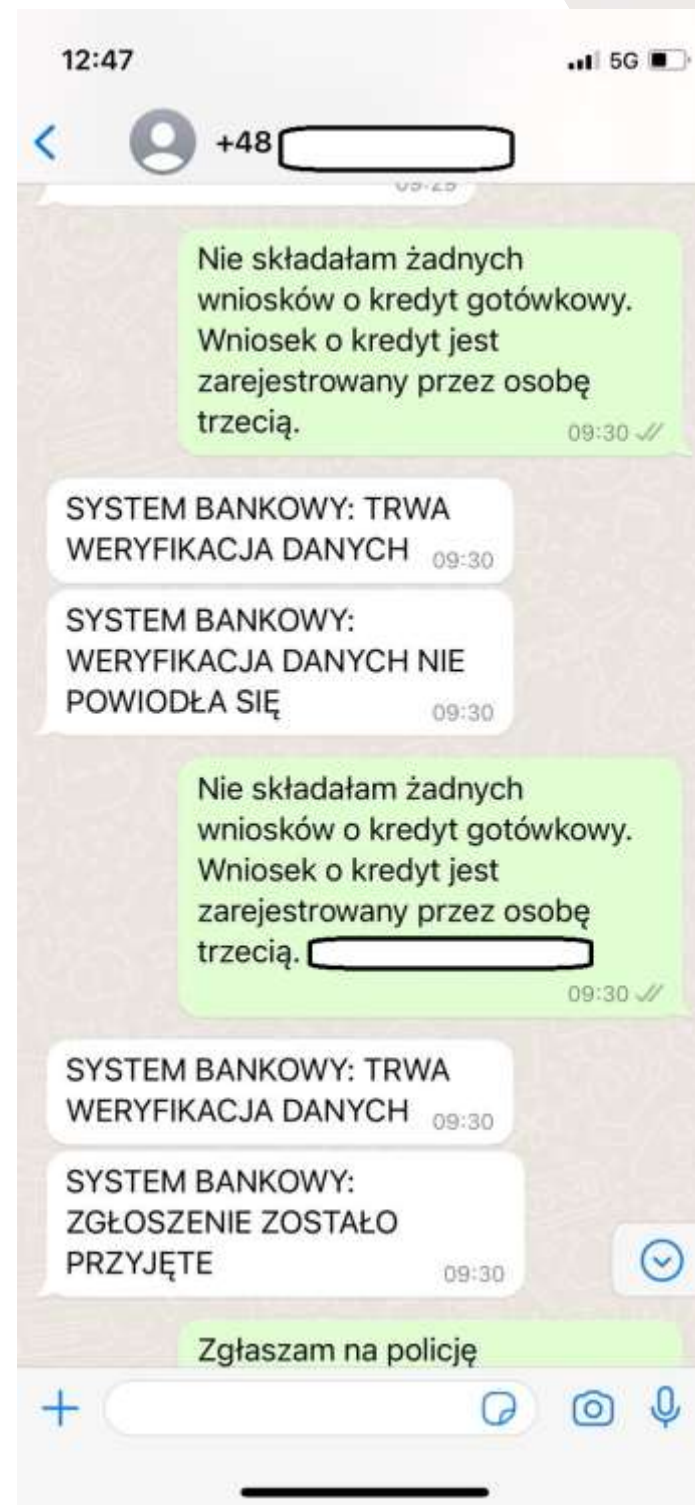
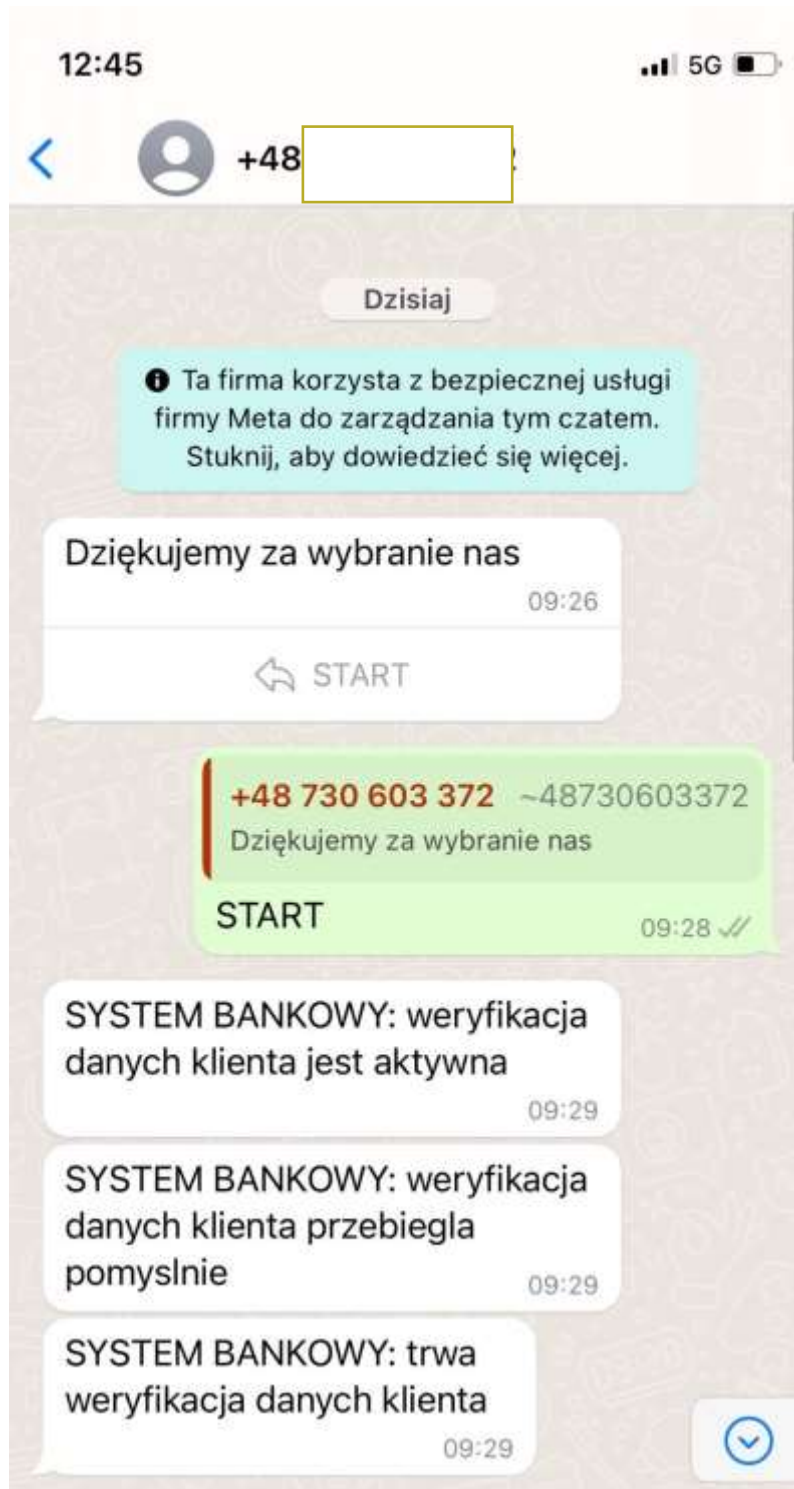
Cele ataku

– Wyłudzenie informacji 

– Instalacja oprogramowania 

– Wykonanie przelewu 





Atak telefoniczny „na zdalny pulpit”



Atak odwrócony, „na pomoc techniczną”

Twoja karta płatnicza
VISA została
zablokowana ze
względów
bezpieczeństwa.
Prosimy o pilny kontakt
mBankiem +48 42 6 300
800



Microsoft account

Your account has been temporarily blocked

Someone may have used your account to send out a lot of junk messages or done something else that violates the [Microsoft Services Agreement](#).

What do you need to do?

We'll send a verification code to your phone. After you enter the code, you can sign in.

[Continue](#)

[Skip this for now](#) (some Microsoft sites and services might be disabled)

 (1) System Virus Warning:

 **Your Computer May Have A VIRUS!**

Your Location:
United States

Your IP Address:
199.231.208.116

Date:
Wednesday, March 11,
2015

What to do:

Call **844-373-0540** immediately (toll-free) for assistance on how to remove malicious pop-ups and **VIRUSES**. This call is prioritized and 100% free

Possible network damages from potential threats: **UNKNOWN**

Data exposed to risk:



Vishing – jak reagować



Jeśli rozmówca wzbudzi Twoje podejrzania – rozłącz się.



Jeśli chcesz się upewnić, skontaktuj się samodzielnie **wyszukując w zaufanym źródle** numer obsługi klienta danej instytucji/banku itp.

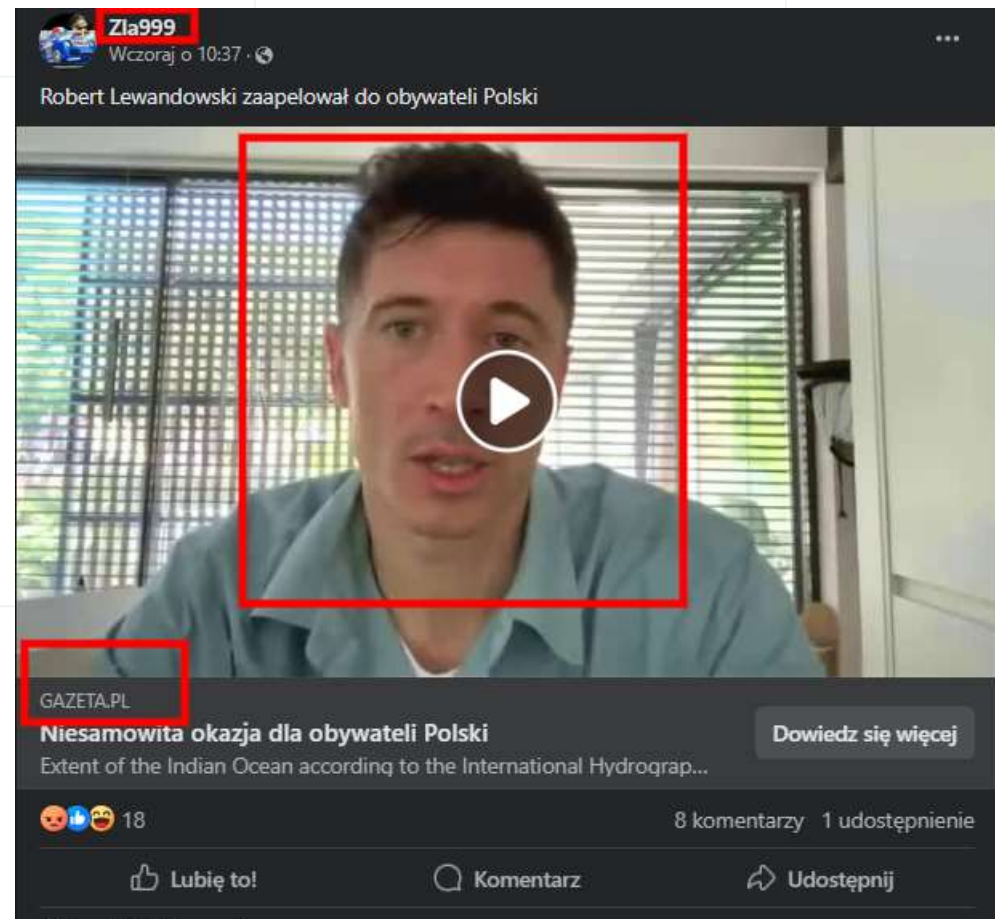




Deep fake

– czyli jak oszuści wykorzystują AI

Wykorzystanie wizerunku znanych postaci



Oszuści wykorzystują nagranie z Lewandowskim. Jest ostrzeżenie



Twitter / CSIRT KNF / Na zdjęciu: Rzekomo Robert Lewandowski

Robert Lewandowski reklamuje ryzykowne inwestycje finansowe? Uważaj! To tzw. deepfake. "Nie wierz w oferty ogromnych zysków w krótkim czasie i nie daj się okraść" - ostrzega CSIRT KNF.

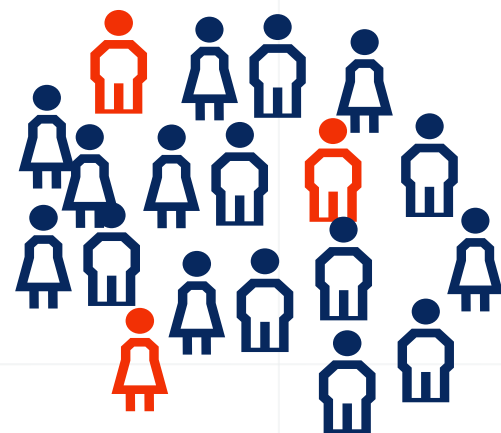
Materiał o Deep fake'ach, Adrian Kilar:

<https://www.youtube.com/watch?v=-nys7TAzSBg>

Źródło:

<https://sportowefakty.wp.pl/pilka-nozna/1118746/oszuci-wykorzystuja-nagranie-z-lewandowskim-jest-ostrezenie>

Rodzaje ataków w zależności od grupy docelowej



masowy

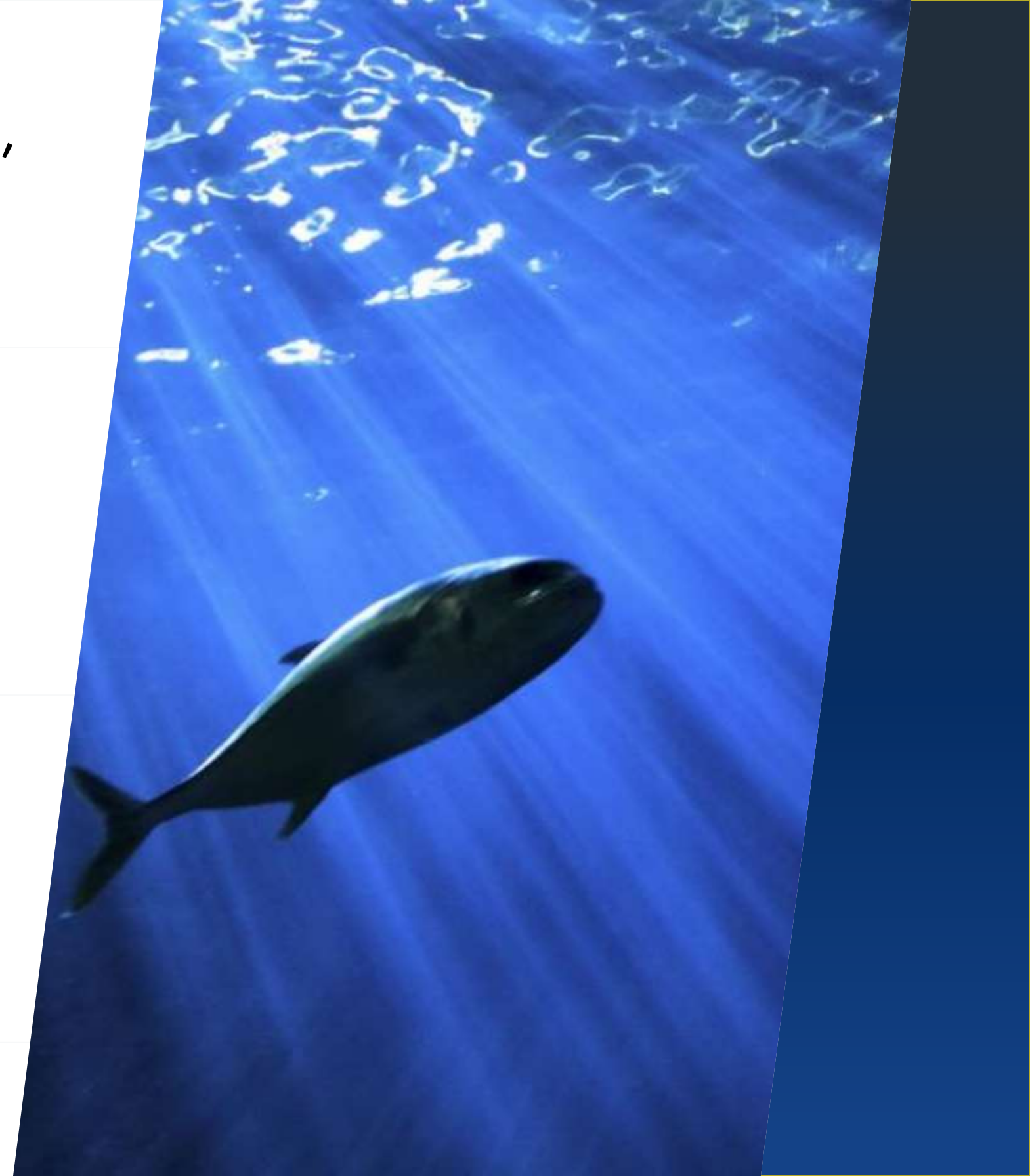


spersonalizowany

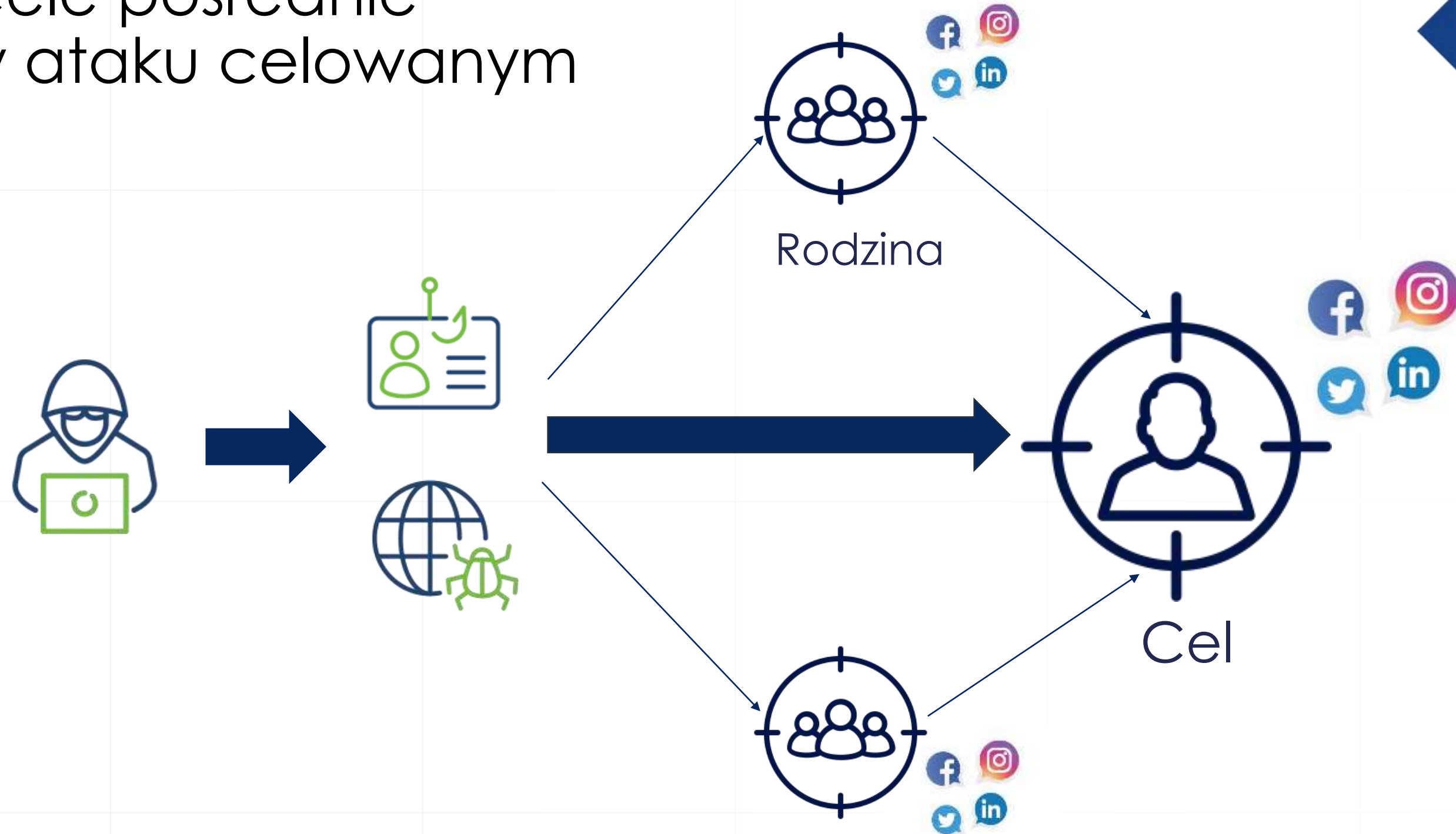
Phishing spersonalizowany, celowany

ang. Spear phishing, whaling

- **Precyzyjnie wybrany cel** – osoba lub grupa;
- **Rozpoznanie** celu i jego otoczenia;
- Pretekst i historia ataku **precyzyjnie dopasowane**.



Cele pośrednie w ataku celowanym



„Oszustwo na dyrektora” – atak na JST

Zapłata - Mozilla Thunderbird

Plik Edycja Widok Przejdź Wiadomość Narzędzia Pomoc

Pobierz Napisz Etykieta

Odpowiedz Odpowiedz wszystkim Przekaż Archiwizuj Niechciana Usuń DKIM Więcej

Od **Robert Serkis <director@vorsitze.info>**

Do [redacted]

31.01.2023, 07:39

Temat **Zapłata**

Dzień dobry

Jakie jest saldo konta, czy możemy dziś zapłacić 33 300,10 euro?

Pozdrowienia
Robert Serkis

Urząd Gminy Horyniec-Zdrój
Biuletyn Informacji Publicznej

Szukaj KONTAKT

zaawansowane wyszukiwanie

bip biuletyn informacji publicznej

Menu podmiotowe

- Dane teleadresowe
- Wójt**
- Rada Gminy
- Komisje
- Stanowiska
- Instytucje kultury
- Oświata
- Pomoc społeczna
- Spółki prawa handlowego z udziałem gminy
- Sołectwa

Menu przedmiotowe

- Oświadczenia majątkowe
- Wykaz spraw
- Prawo lokalne

Rozmiar tekstu **AAa** Kontrast Wydrukuj Dane XML Strona **WWW**

Strona główna > Organy > Wójt

WÓJT | KADENCJA 2018 - 2023

Wybierz kadencję

- Kadencja 2018 - 2023**
- Kadencja 2014 - 2018
- Kadencja 2010 - 2014
- Kadencja 2006 - 2010

ROBERT SERKIS - WÓJT GMINY HORYNIEC-ZDRÓJ

Telefon (16) 631 34 55	Fax (16) 631 34 55	E-mail wojt@horyniec-zdroj.pl
---------------------------	-----------------------	----------------------------------

„Oszustwo na dyrektora” ze spoofingiem

Pilna prośba

○ Paweł [redacted] <p.[redacted]@hospicjum[redacted]>
Do biuro@hospicjum[redacted]

09:13 

PG

[Odpowiedz](#) [Odpowiedz wszystkim](#) [Prześlij dalej](#) [Usuń](#) 

Mamy dziś pilną płatność, jaki jest stan naszych kont?

Z poważaniem,

Paweł [redacted]

Przykład oszustwa skierowanego do gminy

Pobierz | Napisz | Etykieta

Odpowiedz | Odpowiedz wszystkim | Przekaż | Archiwizuj | Niechciana | Usuń | DKIM | Więcej

Od j.r. [redacted] pl <j.[redacted]@[redacted].com>

Do [redacted] <skarbnik@[redacted].pl>

14.09.2023, 11:26

Temat **Re: RE: Faktura**

W załączniku faktura do opłaty.

Faktura

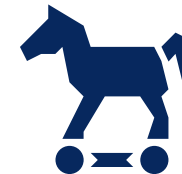
8/09/2023

SPRZEDAWCA [redacted]

NABYWCA [redacted]

DATA WYSTAWIENIA	2023-09-08	SPOSÓB PŁATNOŚCI	Przelew na rachunek bankowy
DATA DOSTAWY/WYKONANIA USŁUGI	2023-09-08	NAZWA BANKU	Nest Bank
TERMIN PŁATNOŚCI	2023-09-11 (3 dni)	BIC/SWIFT	NESBPLPW
		NR RACHUNKU	[redacted]
		WALUTA	[redacted]

LP.	NAZWA	PKWIU	ILOŚĆ	J.M.	CENA NETTO	WARTOŚĆ NETTO	STAWKA VAT	KWOTA VAT (PLN)	WARTOŚĆ BRUTTO
1	Skoda Fabia 1.0TSI 2020r. VIN-WR01XRTRG2UJ552331 Rej- WF6251R		1	szk.	38 700,00	38 700,00	zw	0,00	38 700,00
						38 700,00	zw	0,00	38 700,00
					RAZEM	38 700,00	x	0,00	38 700,00



Złośliwe oprogramowanie

– czyli o szkodliwych programach i socjotechnice raz jeszcze

Złośliwe oprogramowanie

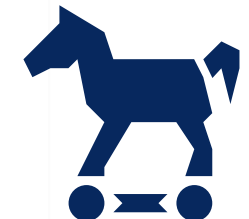
ang. **malware** (*malicious* - złośliwy i *software* - oprogramowanie)

– ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkowników.

Złośliwe oprogramowanie

Aktualnie stosuje się podział ze względu na **sposób działania**:

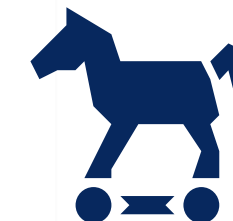
- ransomware
- trojany bankowe (bankery)
- spyware
- RAT (remote access trojan)
- kryptokoparki
- ...



W jaki sposób przestępcy infekują urządzenia?

Źródła infekcji

- Luki bezpieczeństwa w publicznie dostępnych usługach;
- Niewystarczające zabezpieczenia dostępu do infrastruktury oraz publicznych usług (często zbyt słabe hasło);
- **Maile nakłaniające do pobrania i uruchomienia pliku załączonego lub umieszczonego w linku.**



Załączniki w spreparowanych mailach

From: Krzysztofa Mudraka <info@tradersinfoss.club> ☆

Subject: Re:żądać informacji

06:13

Szanowni Państwo,

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

Czekam na Twoją pilną odpowiedź.

Z góry dziękuję i życzę dobrej pracy.

Z poważaniem

Krzysztofa Mudraka

Dyrektor/Director


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

e-mail: krzysztof.mudrak@modustrebinje.com strona: www.modustrebinje.com. Skype: admin.modustrebinje

[REDACTED]

[REDACTED]

[REDACTED] Kapitał zakładowy: 5000


 Think before you print!

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

1 attachment: specyfikacja.xlsx 224 KB

specyfikacja.xlsx 224 KB

Save



Najczęściej stosowane załączniki

Obecnie najbardziej podejrzane:

– archiwa i obrazy dysków:

.zip **.rar** **.iso** **.img**

– pliki wykonywalne (najczęściej wewnątrz poprzednich)

.exe **.com** **.scr** **.vbs** **.js**

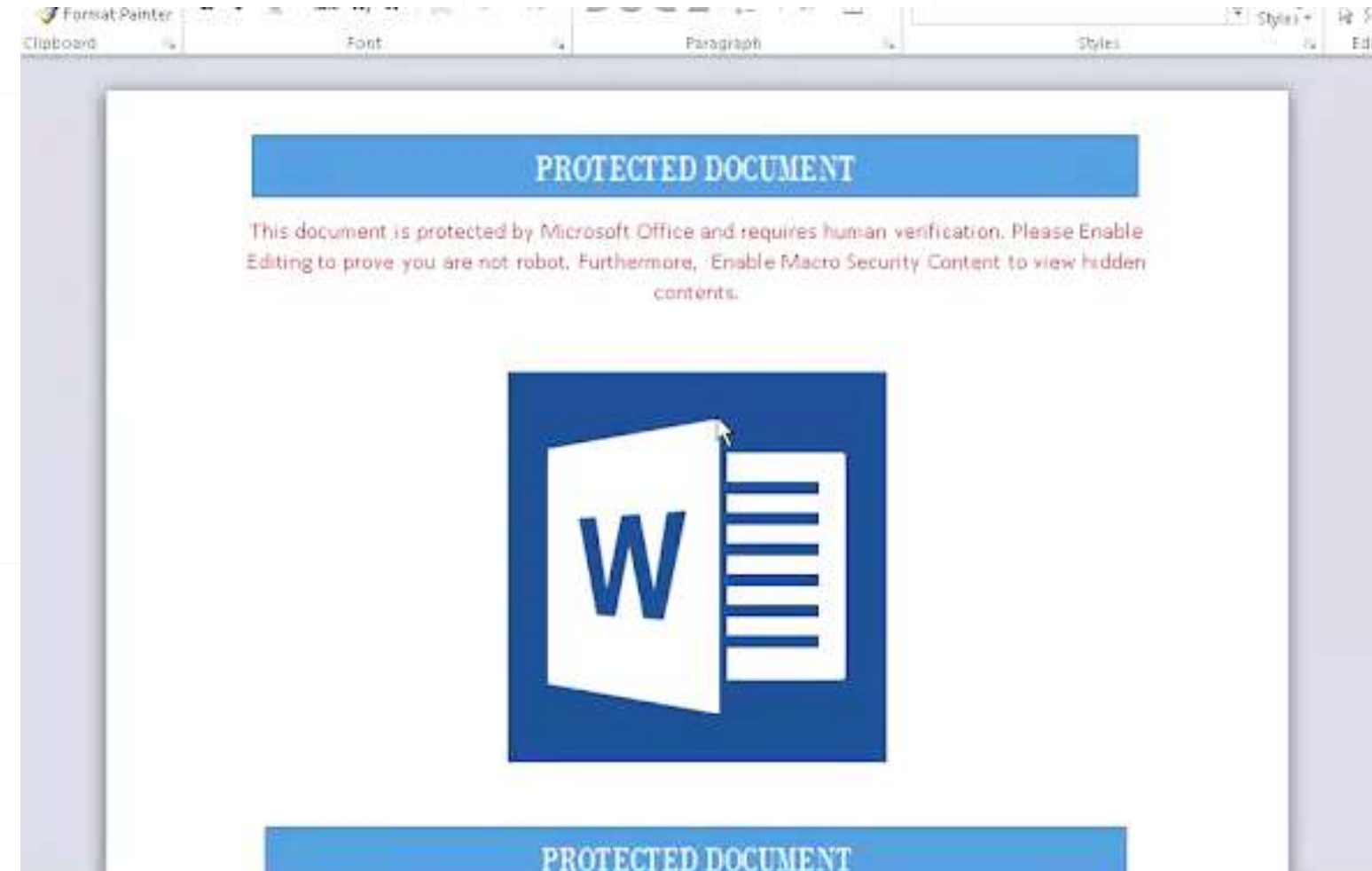
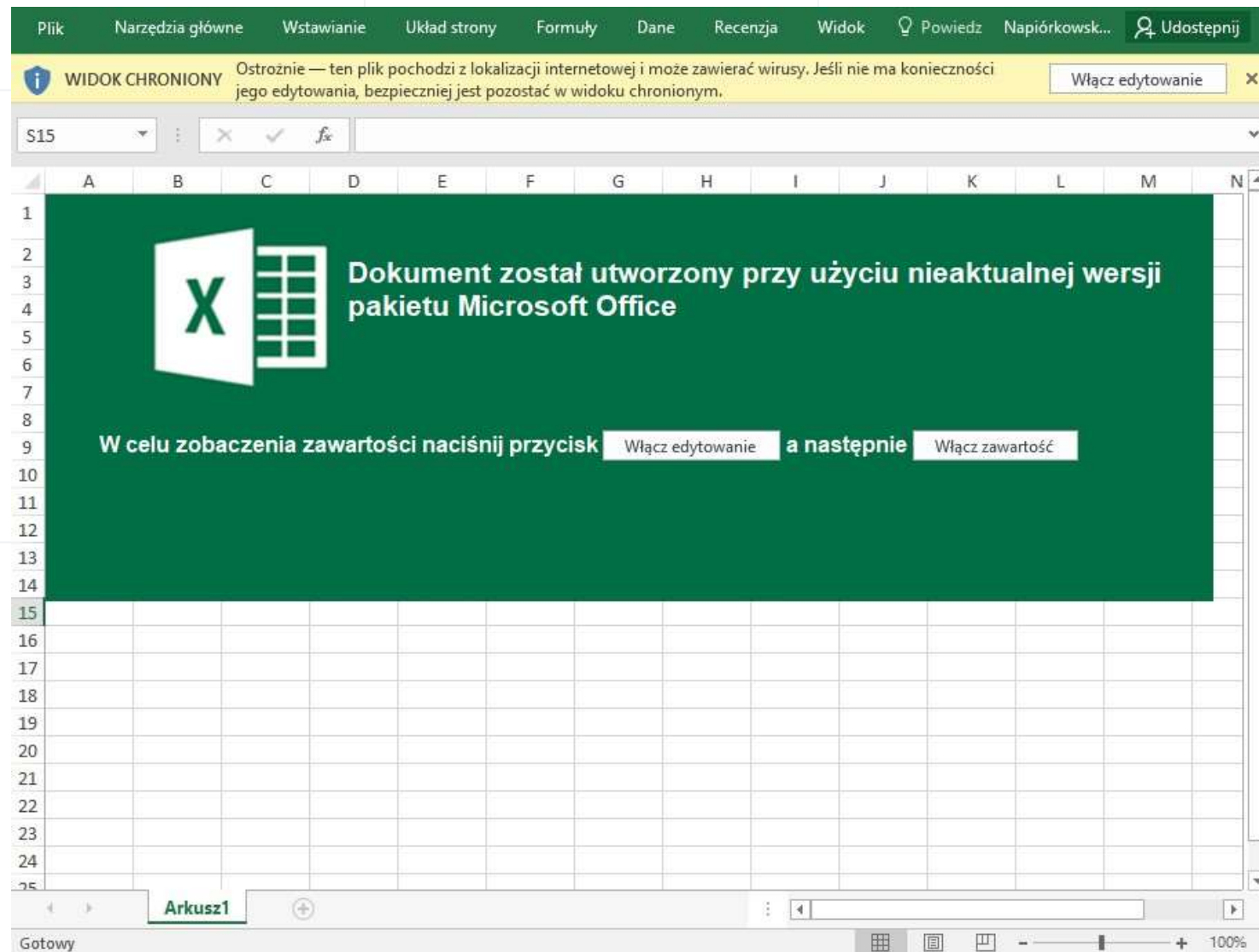
– linki i kopie stron (z dodatkową zawartością)

.lnk **.htm** **.html**

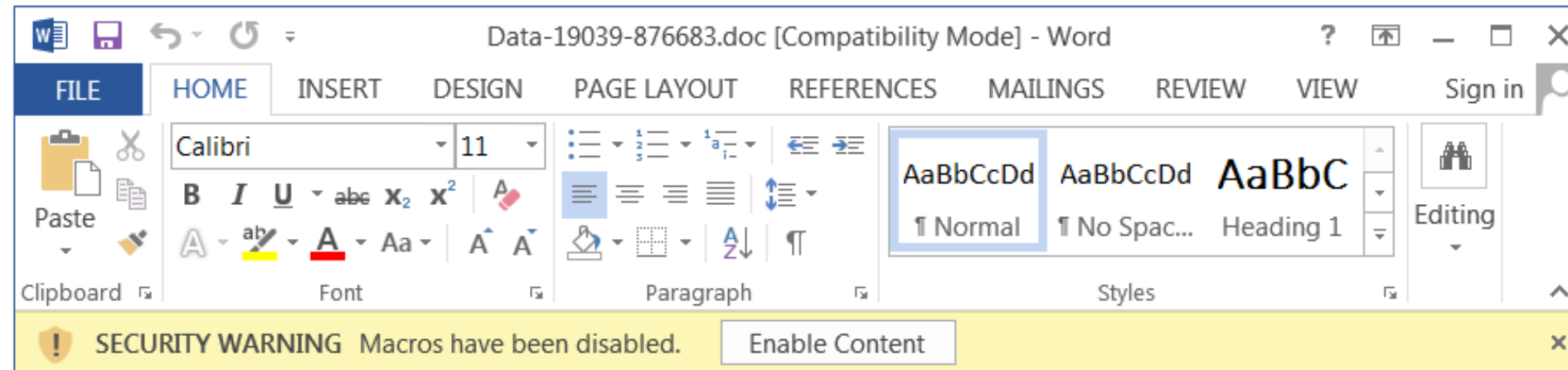
– pliki oprogramowania biurowego

.one **.xlsx** **.xlsm** **.xls** **.doc**

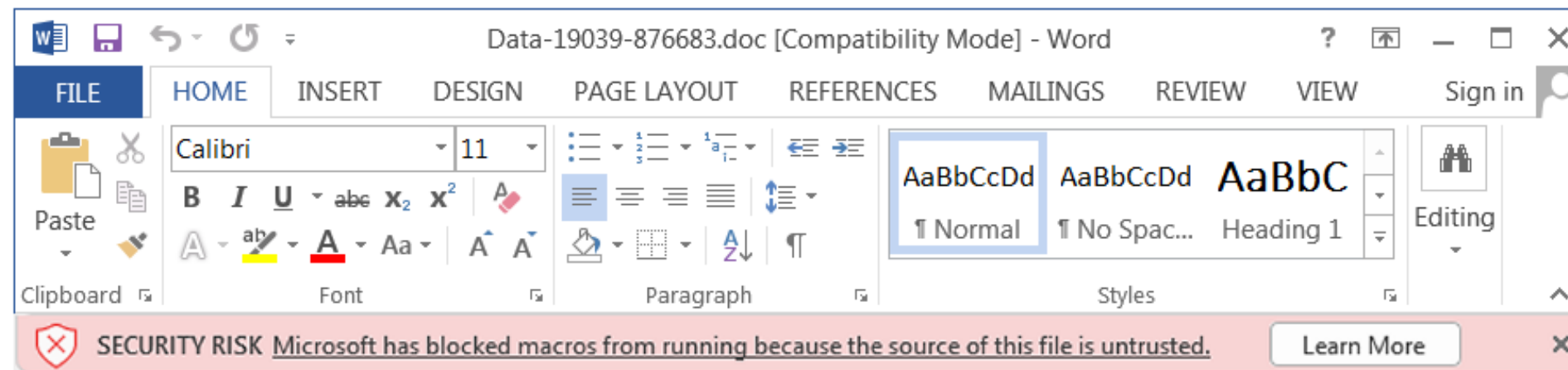
Złośliwy kod w plikach MS Office



Zabezpieczenie plików MS Office



OLD SECURITY ALERT



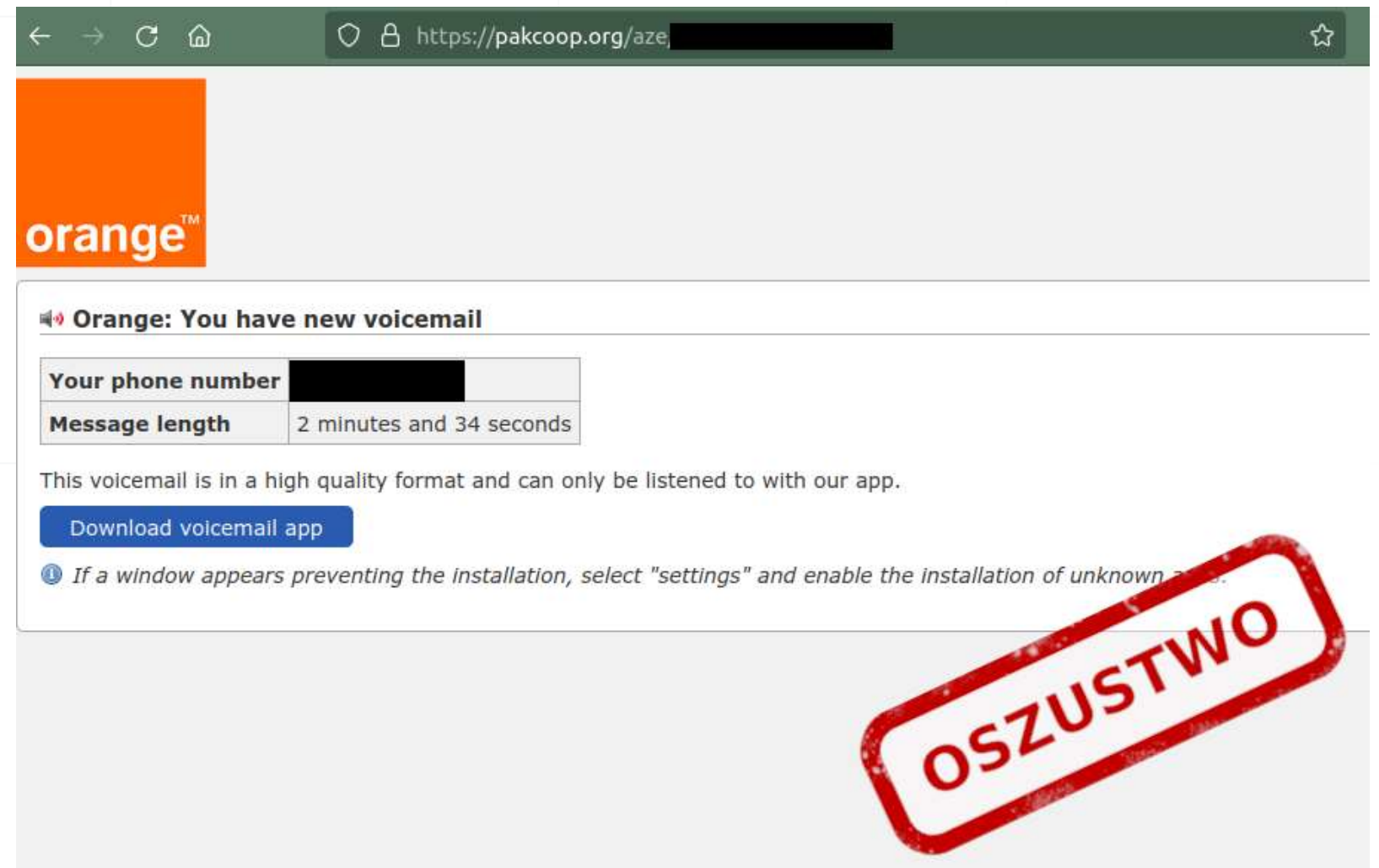
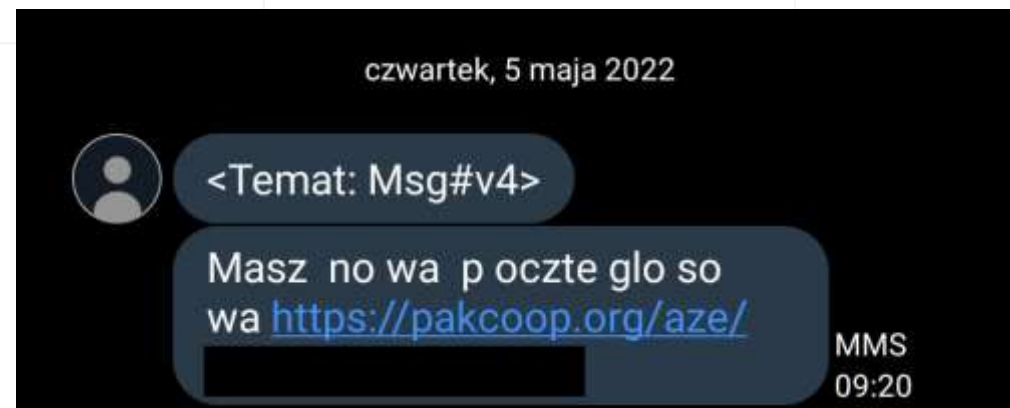
NEW SECURITY ALERT

- bleepingcomputer.com

Złośliwe oprogramowanie na telefon

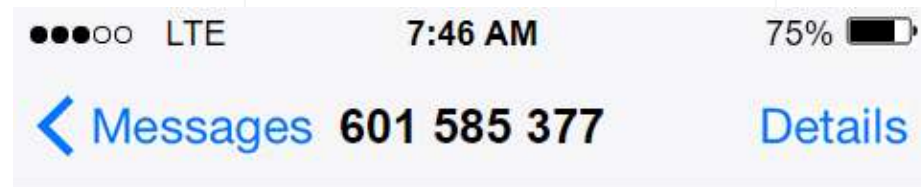
Sygnaty alarmowe:

- instalowanie „z nieznanych źródeł”
- aplikacja żąda uprawnień **ułatwienia dostępu**



Złośliwe oprogramowanie na telefon

- instalacja z nieznanych źródeł **jest domyślnie wyłączona**, stąd instrukcja instalacji dla odbiorców ataku.



Twoja paczka została zatrzymana przez służby celne:
<https://mounter.io/pkg/?uj0cz226uy4l>



Trojan bankowy, wykradanie danych



Złośliwe oprogramowanie w reklamach

The image shows a Google search interface with the query 'gimp'. The search results include an advertisement for 'Gimp.org - GIMP - Downloads - Feature Overview' and a search result for 'GIMP - GNU Image Manipulation Program'. A browser window is overlaid on the right, displaying the official GIMP website. The website features the GIMP logo (a cat-like character with a pencil) and the text 'GIMP GNU IMAGE MANIPULATION PROGRAM'. A prominent red button says 'DOWNLOAD 2.10.32' and a dark button says 'RELEASE NOTES'. Below the main banner, there are sections for 'The Free & Open Source Image Editor' and 'Recent News'. The 'Recent News' section lists 'Development version: GIMP 2.99.12 Released 2022-08-27' and 'GIMP 2.10.32 is on the Microsoft Store! 2022-06-18'.

Ransomware

- Oprogramowanie blokujące system komputerowy

Nota z żądaniem okupu

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

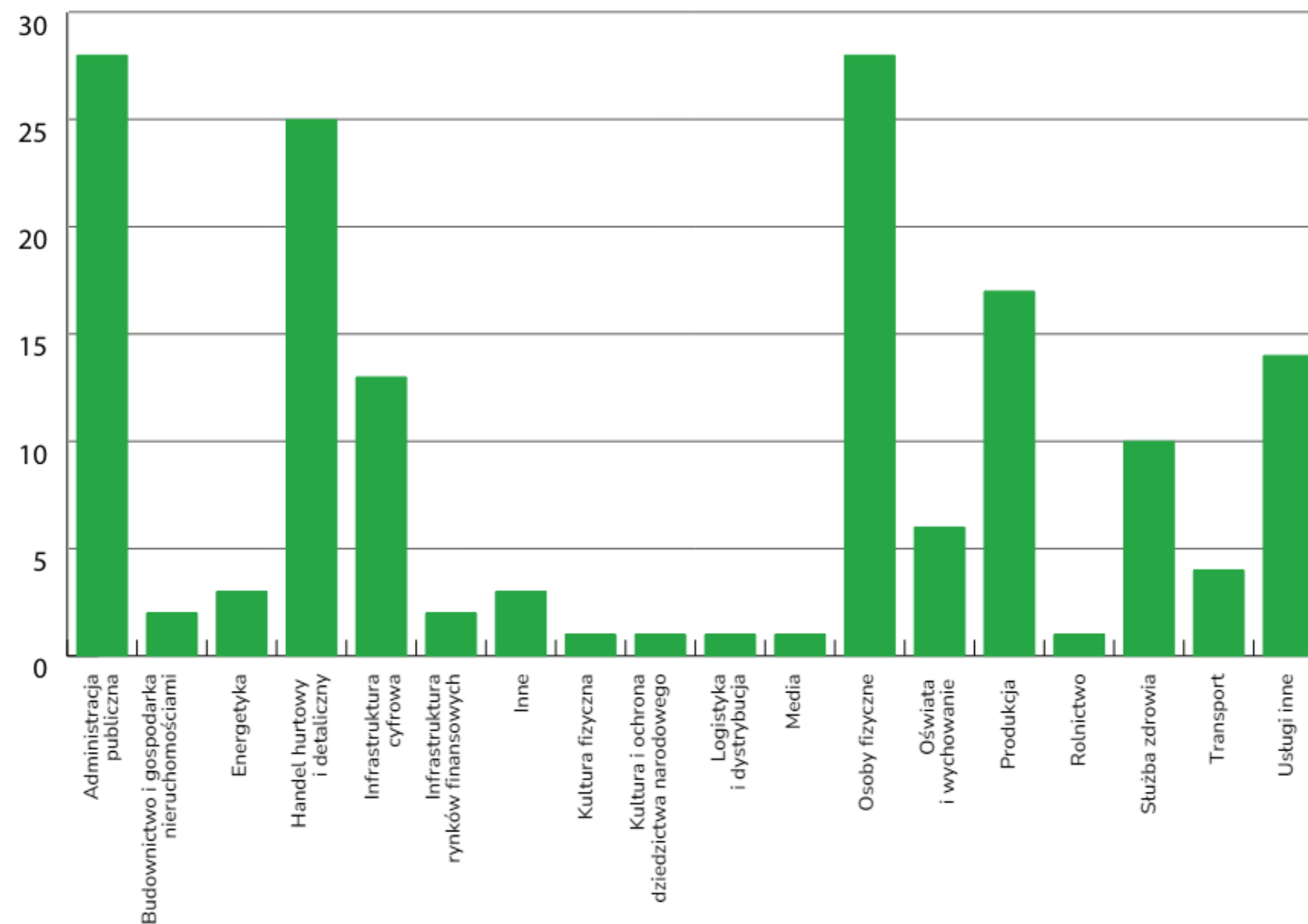
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

Raport CERT Polska 2023 – ataki ransomware



6.html

RA World Home Victim

ALAB laboratoria (Unpay)

Target Introduction

Name:
ALAB laboratoria

Official Website:
<https://www.alablaboratoria.pl>

SIZE:
246 GB

Content:
All Laboratory Reports
All Customer Information
Legal Documents
Financial Data
Business Contract
Others...

Schedule for Document Public Release:
2023-12-31 Part-1

Sample Files Download Address:
<https://g...>

Full Data Download Address:
<http://aworld...>

NIEBEZPIECZNIK.PL
RAW



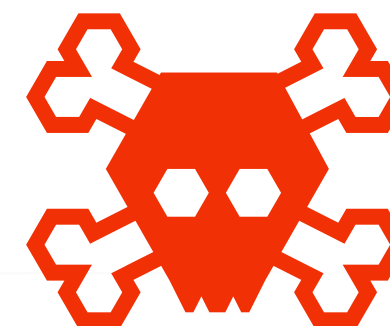
Copyright © RA World 2023

Ransomware – konsekwencje ataku

W przypadku ataku ransomware, **atakujący często nie tylko szyfrują dane, ale także wykradają je**, grożąc upublicznieniem w przypadku nie zapłacenia okupu.

Często dochodzi również do **zaszyfrowania kopii zapasowych**.

Zapłacenie okupu nie gwarantuje odzyskania danych i nie jest wskazane.





Ransomware – prewencja

Podstawowe środki ochrony:

- **dobra strategia tworzenia i weryfikowania kopii zapasowych**
zasada 3-2-1 (prywatnie warto mieć dysk zewnętrzny na który kopiujemy dane albo trzymamy kopię plików w chmurze);
- **regularna aktualizacja oprogramowania,**
- **edukacja własna i użytkowników.**



(CYBER)SZKOLENIA

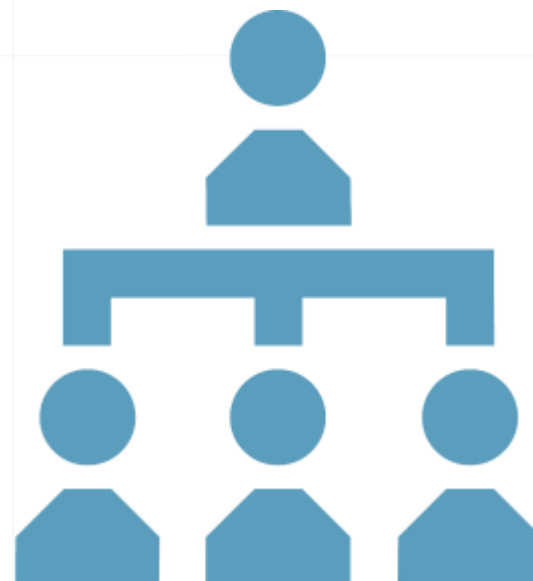
KRAJOWY SYSTEM
CYBERBEZPIECZEŃSTWA

Zgłaszanie incydentu



Kto zgłasza incydent w organizacji?

Incydent w środowisku służbowym może i powinna zgłaszać **każda osoba** w organizacji, ale:



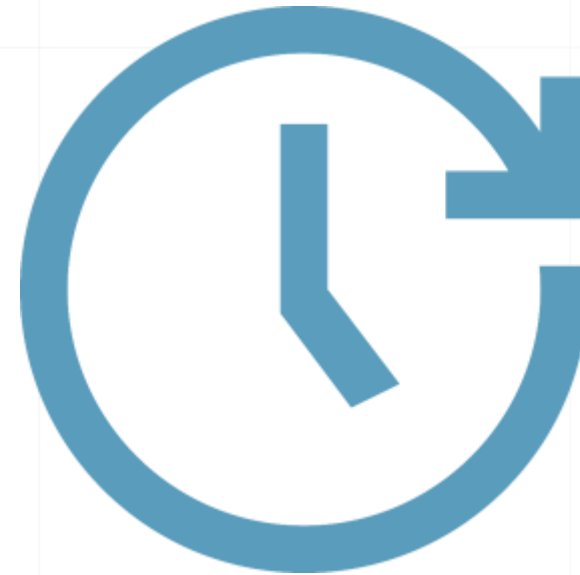
Pracownicy zgłaszają do **zespołu bezpieczeństwa/helpdesku**.



Do **CSIRT** incydent zgłasza **wyznaczona osoba** (lub komórka organizacyjna).

Zgłoszenie incydentu do CSIRT NASK

- Wyznaczona osoba/ zespół bezpieczeństwa
- Incydent należy **zgłosić niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia do właściwego CSIRT.
- Zgłoszenie przekazywane jest **w postaci elektronicznej**, poprzez uzupełnienie **formularza internetowego** znajdującego się na stronie: <https://incydent.cert.pl>.



24 godz.



<https://incydent.cert.pl>

lub

w systemie S46

Informacje prawnie chronione

- Poszczególne **zespoły CSIRT mają prawo przetwarzać dane osobowe**, w tym także **tajemnice prawnie chronione**, które są niezbędne do obsługi incydentów i zagrożeń cyberbezpieczeństwa.
- Zgłoszenie incydentu **powinno zawierać dane osobowe**, a także **tajemnice prawnie chronione**, jeżeli jest to konieczne do realizacji zadań CSIRT.



RODO (art. 23), inne tajemnice prawnie chronione.



bez informacji niejawnych!

Pamiętaj, aby wysyłając zgłoszenie **oznaczyć informacje prawnie chronione**, w tym stanowiące tajemnicę przedsiębiorstwa. Aby to zrobić, użyj nawiasów kwadratowych, na przykład: [Incydent w systemie bankowym miał wpływ na 10 tysięcy użytkowników końcowych.]

Uwaga: Nieuzasadnione użycie oznaczeń może wydłużyć czas odpowiedniej reakcji.

Obowiązek informacyjny

- Obsługa incydentu wiąże się również z **obowiązkiem przekazania informacji** osobom, na rzecz których realizuje się zadanie publiczne.
- **Osoby mają prawo dostępu do wiedzy pozwalającej na:**



zrozumienie zagrożeń cyberbezpieczeństwa.

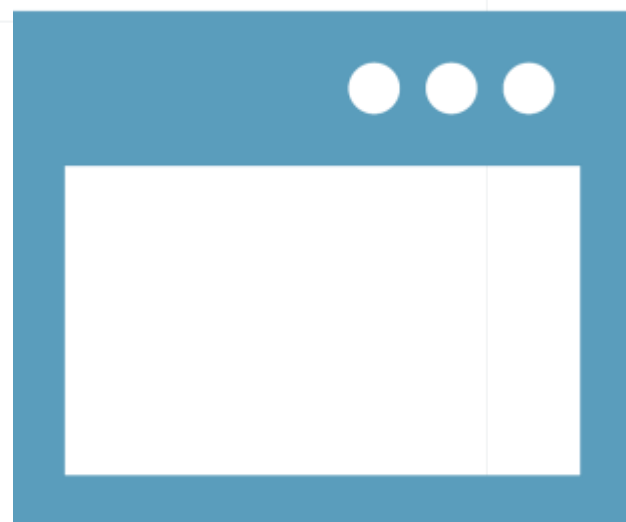


stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.



Obowiązek informacyjny może zostać spełniony poprzez publikację stosownego komunikatu na stronie internetowej.

Zgłoszenie incydentu **prywatnie**



przez formularz:
<https://incydent.cert.pl>



lub przez SMS
(SMShing)

Zgłoszenie przez SMS

Wiadomości z podejrzanyymi linkami najwygodniej zgłaszać za pomocą SMSa.

Wystarczy przekazać treść otrzymanej wiadomości na numer **CERT Polska**.

Trafi ona do analityków CERT Polska, którzy zdecydują o dopisaniu podejrzonej domeny do listy ostrzeżeń.



8080

Lista ostrzeżeń

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie (aktualizowana co 5 minut):

<https://cert.pl/lista-ostrzezen/>

<https://hole.cert.pl/domains/>



Budowana na podstawnie m.in. zgłoszonych podejrzanych domen
– **obrona przed phishingiem**





Wdrażają operatorzy telekomunikacyjni
– **automatyzacja**



Uwaga! Ta strona stanowi zagrożenie

Może ona wyludzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych. W trosce o Twoje bezpieczeństwo dostawca internetu powstrzymał próbę ataku poprzez tę stronę.

Przypominamy:

-  **Dokładnie sprawdzaj** adres i wygląd strony, na której podajesz dane logowania, dane osobowe czy karty płatniczej.
-  **Nie działaj pod presją czasu**, uważaj na wszelkie wiadomości, które skłaniają do działania natychmiast.
-  **Weryfikuj źródło** informacji zanim podejmiesz działania na jej podstawie lub ją powielisz.
-  Nie jesteś pewien czy dana wiadomość jest prawdziwa? **Skontaktuj się** z rzekomym nadawcą innym znanym kanałem i/lub poszukaj potwierdzenia informacji w innych źródłach.
-  **Zgłaszaj do CERT Polska** każdą podejrzaną stronę, a także wiadomości email i SMSy, które mogą wyludzać dane. Formularz znajdziesz na stronie <https://incydent.cert.pl>.

Oficjalne informacje i komunikaty na temat koronawirusa znajdziesz na stronie: <https://gov.pl/koronawirus>.

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie znajduje się na stronie https://cert.pl/ostrzezenia_phishing

Źródła obrazków/zdjęć

Jeżeli nie zaznaczono inaczej zrzuty ekranu pochodzą z materiałów CSIRT KNF i CERT Polska

<https://pixabay.com>

<https://www.pexels.com>

<https://unsplash.com/>

Dziękuję!

NASK – PIB,
Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa,
zbsc@nask.pl