NOWE METODY I TECHNIKI CYBERZAGROŻEŃ

kom. Michał Brykowski
Centralne Biuro Zwalczania
Cyberprzestępczości
Wydział w Łodzi

Łódź, 14.12.2022 r.

Wydział d[illegible]ępczością
KWP w Ło[illegible]

12.07.2022r

Centralne Biuro Zwalczania Cyberprzestępczości
Wydział w Łodzi

Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) jest jednostką organizacyjną Policji służby zwalczania cyberprzestępczości. CBZC odpowiedzialne jest za realizację na obszarze całego kraju zadań w zakresie:

1. Rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw;

2. Wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw.

Zwalczanie cyberprzestępczości powinno się opierać na ograniczaniu skutków jej wpływu na społeczeństwo oraz identyfikowaniu zagrożeń pochodzących z sieci. Głównym celem jest tworzenie bezpieczniejszej cyberprzestrzeni.

NAJCZĘŚCIEJ ZGŁASZANE SPRAWY Z ZAKRESU CYBERPRZESTĘPCZOŚCI

1. Ataki z wykorzystaniem oprogramowania typu Ransomware

2. Kradzież tajemnic przedsiębiorstwa

3. Oszustwa internetowe z wykorzystaniem narzędzi socjotechniki

SPOOFING NUMERU TELEFONU

Fałszowanie identyfikatora – praktyka polegająca na spowodowaniu, że sieć telefoniczna wskazuje osobie, którą jest odbiorcą, innego niż w rzeczywistości inicjatora. Powoduje to wyświetlenie u odbiorcy, numeru innego niż numer z którego wykonano Połączenie/wysłano wiadomość.

SPOOFING
"NADAWCY" SMS

SPOOFING
"NUMERU" DZWONIĄCEGO”

VISHING

RingCentral

Vishing (voice or VoIP phishing)

SMISHING

poniedziałek, 31 stycznia 2022

BLIK. Ktos wyslal ci przelew na telefon 450zl, skorzystaj z ponizszego linku do odbioru srodkow:
https://blik.auction/q91zvd4

22:0

PGE: Prosimy uregulowac naleznosc:
https://4.fo/pge-mlrGUu

Kliknij, aby wczytać podgląd

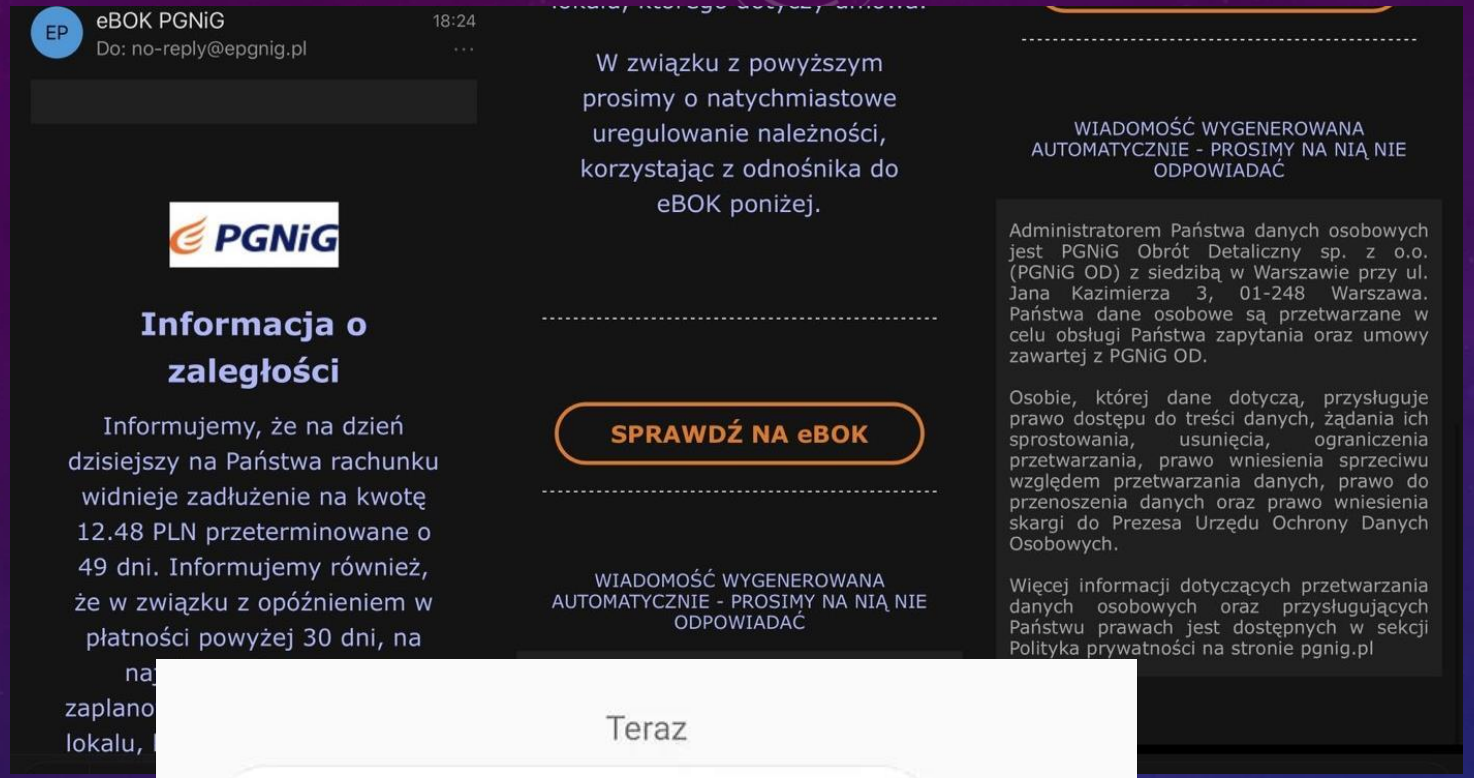
Teraz

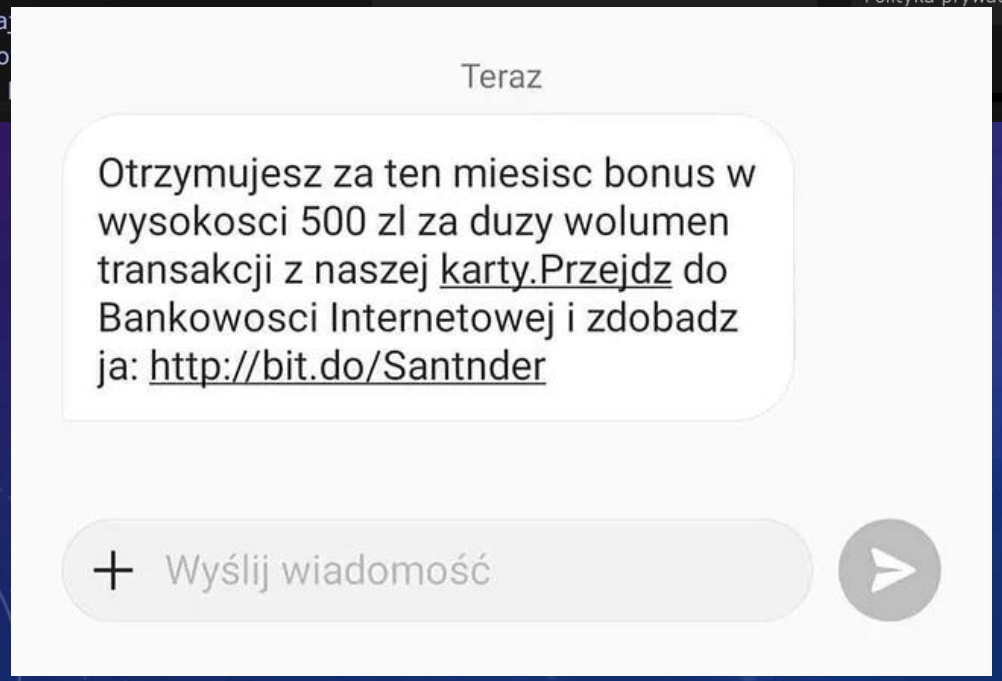
PHISHING

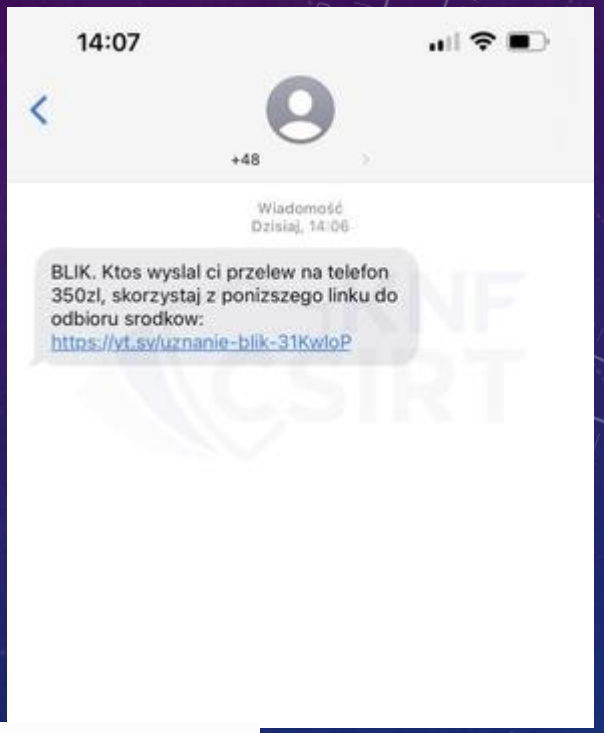

SOFTWARE
SOFTWARE LICENSE

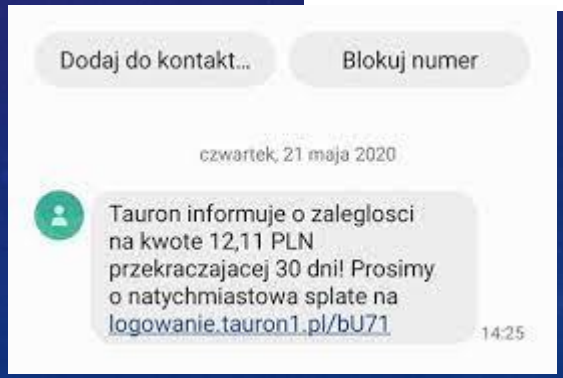

Wyższa Szkoła Gospodarki Narodowej w Kutnie
Sponsorowane
Wejście na rynek europejski wymaga dużych inwestycji, a Orlen otworzył dział inwestycyjny dla polskich mieszkańców. Zainwestuj w giganta naftowego i uzyskaj dochód ze stacji benzynowych
ORLEN daje możliwość zarabiania na stacjach benzynowych
WMMURRAY.COM
Damrob
Dlaczego jest to korzystne dla zwykłych obywateli Znaczne zyski przy ...
Więcej informacji


Papieska Akademia Teologiczna
Sponsorowany
"Zrobimy z niego skarb narodowy!" - władze wyraziły zgodę!
Oferta dla wszystkich Polaków! ... Wyświetl więcej
ORLEN
WILLIAMS RACING
"Po raz pierwszy w historii Polski! Inwestycje dostępne dla każdego Polaka!"
Śledź ten link! I wypełnij wniosek
toliman.pl
PAGE POLSKIE
Więcej informacji
3
Komentarze: 2
Lubię to!
Dodaj komentarz
Udostępnij


EP
eBOK PGNiG
18:24
Do: no-reply@epgnig.pl
PGNiG
Informacja o zaległości
Informujemy, że na dzień dzisiejszy na Państwa rachunku widnieje zadłużenie na kwotę 12.48 PLN przeterminowane o 49 dni. Informujemy również, że w związku z opóźnieniem w płatności powyżej 30 dni, na
W związku z powyższym prosimy o natychmiastowe uregulowanie należności, korzystając z odnośnika do eBOK poniżej.
SPRAWDŹ NA eBOK
WIADOMOŚĆ WYGENEROWANA AUTOMATYCZNIE - PROSIMY NA NIĄ NIE ODPOWIADAĆ
WIADOMOŚĆ WYGENEROWANA AUTOMATYCZNIE - PROSIMY NA NIĄ NIE ODPOWIADAĆ
Administratorem Państwa danych osobowych jest PGNiG Obrót Detaliczny sp. z o.o. (PGNiG OD) z siedzibą w Warszawie przy ul. Jana Kazimierza 3, 01-248 Warszawa. Państwa dane osobowe są przetwarzane w celu obsługi Państwa zapytania oraz umowy zawartej z PGNiG OD.
Osobie, której dane dotyczą, przysługuje prawo dostępu do treści danych, żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu względem przetwarzania danych, prawo do przenoszenia danych oraz prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
Więcej informacji dotyczących przetwarzania danych osobowych oraz przysługujących Państwu prawach jest dostępnych w sekcji Polityka prywatności na stronie pgnig.pl


Teraz
Otrzymujesz za ten miesisc bonus w wysokosci 500 zl za duzy wolumen transakcji z naszej karty.Przejdz do Bankowosci Internetowej i zdobadz ja: http://bit.do/Santnder
Wyślij wiadomość


14:07
+48
Wiadomość
Dzisiaj, 14:06
BLIK. Ktos wyslal ci przelew na telefon 350zl, skorzystaj z ponizszego linku do odbioru srodkow:
https://yt.sv/uznanie-blik-31KwloP


Dodaj do kontakt...
Blokuj numer
czwartek, 21 maja 2020
Tauron informuje o zaleglosci na kwote 12,11 PLN przekraczajacej 30 dni! Prosimy o natychmiastowa splate na logowanie.tauron1.pl/bU71
14:25

SCAREWARE & RANSOMWARE

scare - przestraszyć

ransom – okup

software-oprogramowanie

POLSKA POLICJA

CYBERPRZESTĘPCZOŚĆ DEPARTMENT

Wszystkie operacje wykonywane na tym komputerze, są rejestrowane.
Jeżeli używasz kamerę internetową, wideo i zdjęcia zachowywają się
identyfikacji.

Wideo nagrywania: ON

Można Cię łatwo utożsamić przez Twój adres IP i związaną z nim nazwą dom

Twój adres IP: 78.28.22.89
Nazwa domeny: Petrus Polska Sp. z o.o. spolka komandytowo-akc
Lokalizacja: Poland , Torun

Komputer został zablokowany!

Praca Twojego komputera została zawieszona z przyczyny niedozwolonej aktywno
cybernetycznej.

Niżej są wymienione przepisy, łamanie których miało miejsce z Twojej strony:

Artykuł 274 - Prawo autorskie
Grzywna lub pozbawienie wolności na okres do 4 lat
(Używanie i rozpowszechnianie plików zabezpieczonych prawem autorskim – filmy, oprogramowanie)

Artykuł 185 - Materiały pornograficzne
Grzywna lub pozbawienie wolności na okres do 2 lat
(Używanie i rozpowszechnianie plików pornograficznych)

Artykuł 184 - Materiały pornograficzne z udziałem dzieci (do 18 lat)
Pozbawienie wolności na okres do 15 lat
(Używanie i rozpowszechnianie plików pornograficznych)

Artykuł 106 – Popularyzacja terroryzmu
Pozbawienie wolności na okres do 25 lat
(Odwiedzałeś strony internetowe organizacji terrorystycznych)

Artykuł 287 – Lekceważące korzystanie z komputeru, które spowodowało poważ
konsekwencji
Grzywna lub pozbawienie wolności na okres do 2 lat
(Twój komputer został zarażony wirusem który z kolei zaraził inne komputery)

Artykuł 108 – Gry hazardowe
Grzywna lub pozbawienie wolności na okres do 2 lat
(Grałeś w gry hazardowe, ale według prawa twojego kraju biznes hazardowy jest zabroniony)

W związku z postanowieniem Rządu z dnia 22 sierpnia, wszystkie wymienione tam
przepisów mogą być traktowane jako umowne pod warunkiem zapłaty grzywny.

Kwota grzywny wynosi 1500. Płatność musi być dokonana w ciągu 48 godzin po
ujawnieniu naruszenia.
Jeśli grzywna nie zostanie zapłacona wobec Ciebie zostanie założona sprawa karna

Po dokonaniu płatności Twój komputer zostanie odblokowany

POLICJA.PL

wpisz szukaną frazę

DZIAŁANIA POLICJI | CBŚP | O POLICJI | STATYSTYKA | PRAWO | PRACA W POLICJI | ZAMÓWIENIA PUBLICZNE | KONTAKT

KOMPUTER JEST ZABLOKOWANY!

UWAGA! Pański komputer i IP 31 [redacted] 0 jest zablokowany ze co najmniej jednego z powodów podanych poniżej:

Pan/Pani oglądał/a lub rozpowszechniał zakazane treści pornograficzne (pornografia dziecięca/zoofilia itp.), w taki sposób naruszając artykuł 202 Kodeksu Karnego Rzeczypospolitej Polskiej. Artykuł 202 Kodeksu Karnego przewiduje karę grzywny do 500.000 zł i/lub pozbawienia wolności od 4 do 9 lat.
Nielegalny dostęp został zainicjowany z Pańskiego komputera bez Pańskiej wiedzy lub zgody; komputer może być zainfekowany przez złośliwe oprogramowanie, dlatego też Pan/Pani narusza Ustawę «O niedbałym wykorzystaniu komputera osobistego». Pańska osobowość i adres są obecnie identyfikowane, sprawa karna zostanie wszczęte przeciwko Pan/Pani w ramach jednego lub więcej artykułów określonych powyżej w ciągu najbliższych 72 godzin. Zgodnie z poprawką Kodeksu Karnego Rzeczypospolitej Polskiej z dnia 04 lutego 2013 roku, niniejsze naruszenie prawa (jeśli nie jest powtórzone – po raz pierwszy) można uznać jako warunkowe w przypadku, gdy Pan/Pani zapłaci grzywnę na rzecz państwa. Grzywny mogą być wypłacane tylko w ciągu 48 godzin po naruszeniu. Jak tylko 48 godziny upłynął, możliwość zapłaty grzywny wygasa, i sprawa karna zostanie wszczęta wobec Pana/Pani automatycznie w ciągu 72 godzin!

Wysokość grzywny wynosi 600 zł. Płatności dokonaj paysafecard

Kiedy Pan/Pani zapłaci grzywnę, komputer będzie odblokowany w ciągu od 1 do 24 godzin po wpływu pieniędzy na konto Państwa.

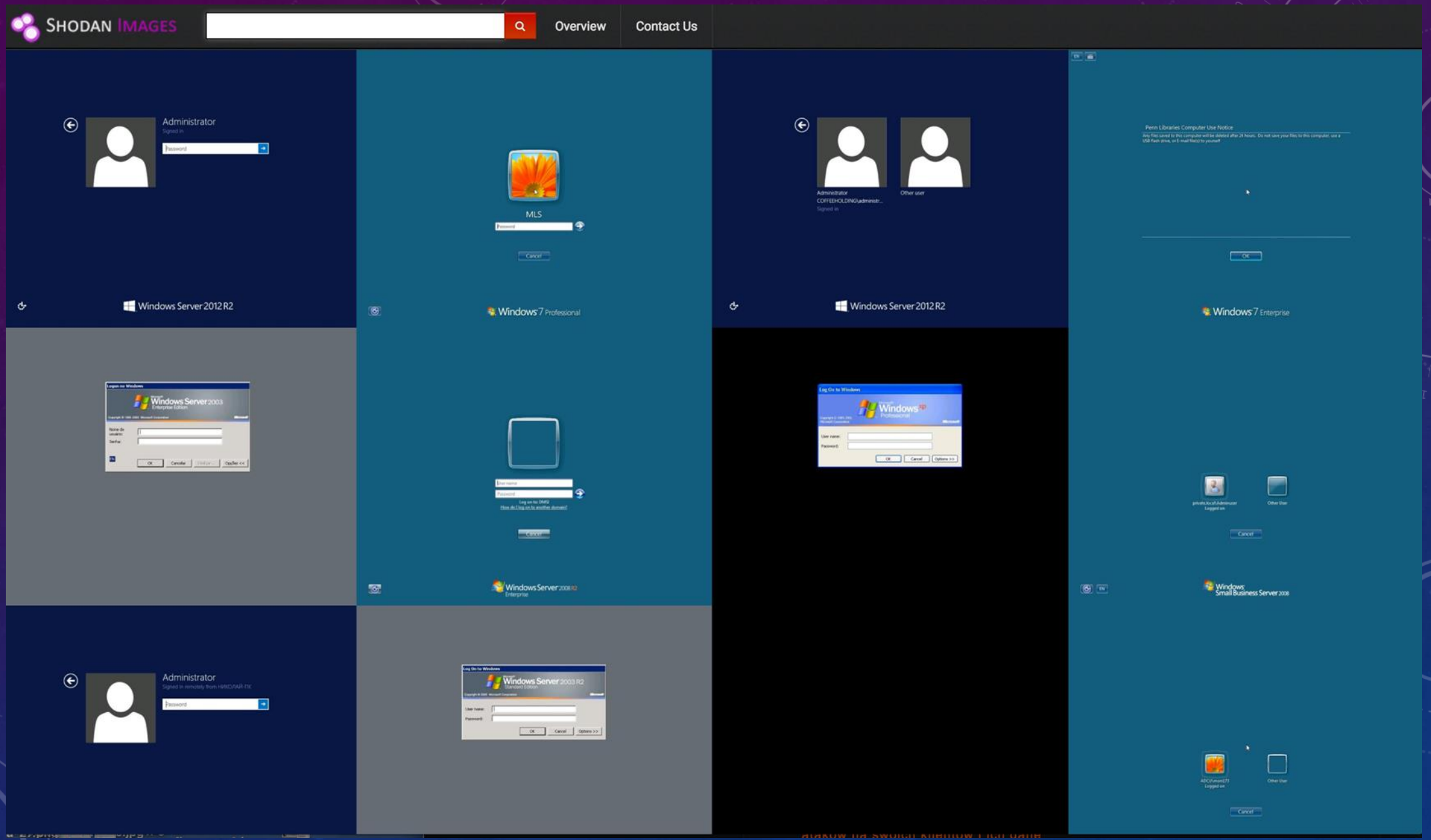
Kwota 100 | Wpisz kod kuponu ... | Zapłacić i odblokować

fot. niebezpiecznik.pl

Grzywny mogą być wypłacane w ciągu 48 godzin!

PaySafeCard można kupić w wielu supermarketach, kioskach ruchu i na stacjach benzynowych. Do wyboru są PIN-y o wartości 100 lub 300 zł.


http://
.com


SHODAN IMAGES
Overview
Contact Us
Administrator
Windows Server 2012 R2
MLS
Windows 7 Professional
Administrator
Other user
Windows Server 2012 R2
Penn Libraries Computer Use Notice
Windows 7 Enterprise
Windows Server 2003 Enterprise Edition
Windows Server 2008 R2 Enterprise
Windows Server 2003 R2 Standard Edition
Windows Small Business Server 2008
Administrator

ATAK RANSOMWARE - SCENARIUSZE

Fakt zastosowania ataku typu Ransomware najczęściej stwierdzamy w momencie utraty dostępu do danych, gdy są one zaszyfrowane.

Powyższe nie wyjaśnia jednak faktu samego ataku oraz jego momentu. Najczęściej zaszyfrowanie danych jest tylko zasłoną dymną i elementem zacierania śladów.

Atak Ransomware w większości przypadków rozpoczyna się znacznie wcześniej niż następuje jego stwierdzenie. Najczęściej do ataku dochodzi około miesiąca wcześniej.

Sam okup (ransom) jest tylko po to aby często zmylić ofiarę co do faktycznego zamiaru sprawców. Zapłacenie okupu nie gwarantuje dostępu do danych.

Kilka słów o szyfrowaniu

encrypted

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail lockhelp@qq.com
Write this ID in the title of your message 7A001C3A-1096
If there is no response from our mail, you can install the Jabber client and write to us in support of lockhelp@xmpp.jp
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Jabber client installation instructions:

- Download the jabber (Pidgin) client from https://pidgin.im/download/windows/
- After installation, the Pidgin client will prompt you to create a new account.
- Click "Add"
- In the "Protocol" field, select XMPP
- In "Username" - come up with any name
- In the field "domain" - enter any jabber-server, there are a lot of them, for example - exploit.im
- Create a password
- At the bottom, put a tick "Create account"
- Click add
- If you selected "domain" - exploit.im, then a new window should appear in which you will need to re-enter your data:
  - User
  - password
  - You will need to follow the link to the captcha (there you will see the characters that you need to enter in the field below)
- If you don't understand our Pidgin client installation instructions, you can find many installation tutorials on youtube - https://www.youtube.com/results?search_query=pidgin+jabber+install

ID Ransomware | Identyfikacja | Najczęściej zadawane pytania | Notify Me | $ Donate | Polski

https://id-ransomware.malwarehunterteam.com

ID Ransomware

Prześlij plik z żądaniem okupu oraz/lub dowolny plik zaszyfrowany przez ransomware, który chcesz rozpoznać.

Przesyłanie plików

Plik z żądaniem okupu

Plik zawierający informacje na temat okupu i sposobu zapłaty.

Wybierz plik | Nie wybrano pliku

Prześlij

https://www.nomoreransom.org

Partnerzy | O Projekcie | Polski

NO MORE RANSOM

Strona główna | Crypto Sheriff | Ransomware: FAQ | Jak zapobiegać | Narzędzia deszyfrujące | Zgłoś przestępstwo

Crypto Sheriff

Wypełnij poniższy formularz, aby pomóc nam określić, do jakiej rodziny należy ransomware, który zainfekował Twoje urządzenie. Pomoże nam to sprawdzić czy możemy zdeszyfrować Twoje pliki. Jeśli tak, otrzymasz link, który umożliwi Ci pobranie deszyfratora.

Przesyłając plik do skanowania, akceptuję POLITYKĘ PRZETWARZANIA DANYCH.

Prześlij zaszyfrowane pliki tutaj (rozmiar nie może być większy niż 1MB)

Wybierz pierwszy plik

Wybierz drugi plik

Poniżej wpisz dowolne dane, które widzisz w ŻĄDANIU OKUPU, czyli adres e-mail, URL strony, adres onion/bitcoin. Dane muszą być wpisane bezbłędnie, uważaj na literówki.

Prewencja dotycząca cyberbezpieczeństwa
O czym należy przypominać?

- W praktyce nie ma systemów teleinformatycznych w 100% odpornych na działanie czynników szkodliwych dla jego działania.
- Jeżeli nie uda się atak na infrastrukturę sprzętową atakuje się poprzez tzw. Interfejs białkowy

Ludzie – najsłabsze ogniwa w łańcuchu bezpieczeństwa

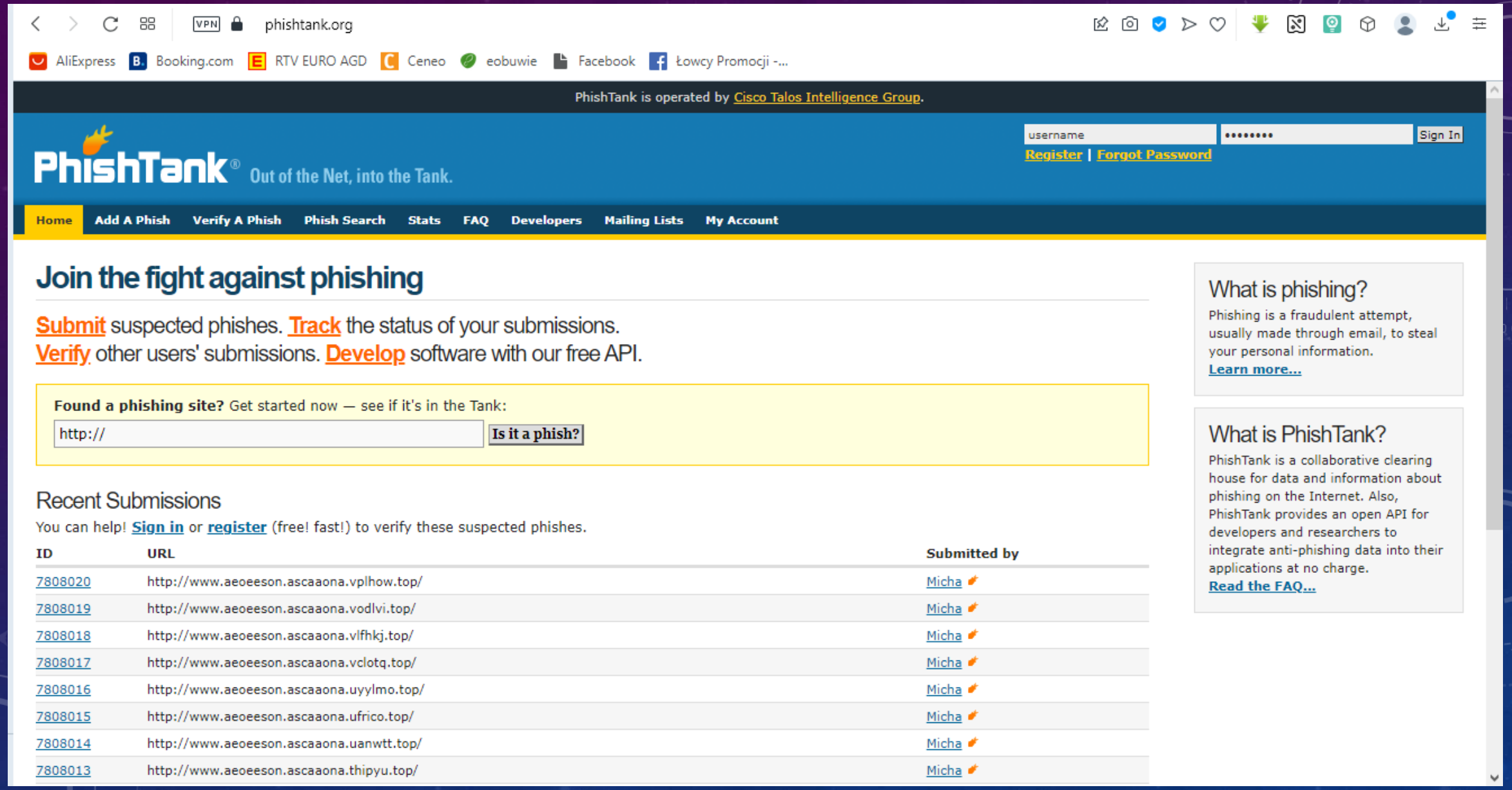
Prewencja dotycząca cyberbezpieczeństwa
O czym należy przypominać?

- Żaden Bank czy Urząd, serwis sprzedażowy nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- korzystanie z oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- aktualizacja oprogramowania antywirusowego.
- aktualizacja systemu operacyjnego i aplikacji.
- nie otwierać plików od nieznanych nadawców.
- nie korzystać ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- nie używać niesprawdzonych programów zabezpieczających.

Prewencja dotycząca cyberbezpieczeństwa
O czym należy przypominać?

- w miarę możliwości częste skanowanie komputera i sprawdzanie procesów sieciowych – czasami złośliwe oprogramowanie nawiązuje własne połączenia z Internetem, wysyła hasła i inne prywatne dane do sieci i może się zainstalować na komputerze mimo dobrej ochrony.
- w miarę możliwości nie korzystać zbyt często ze stron oferujących darmowe filmiki, muzykę – na takich stronach mogą znajdować się ukryte wirusy, trojany i inne zagrożenia.
- sprawdzać pliki pobrane z Internetu za pomocą skanera.
- nie przekazywać swoich danych osobowych w niesprawdzonych serwisach i na stronach, gdy nie mamy absolutnej pewności, że nie są one widoczne dla osób trzecich.
- nie wysyłać w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane, a hasło przekażmy w inny sposób.
- wykonywanie kopii zapasowych ważnych danych.

Sprawdzenie czy domena jest phishingowa



Wyciek danych

Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

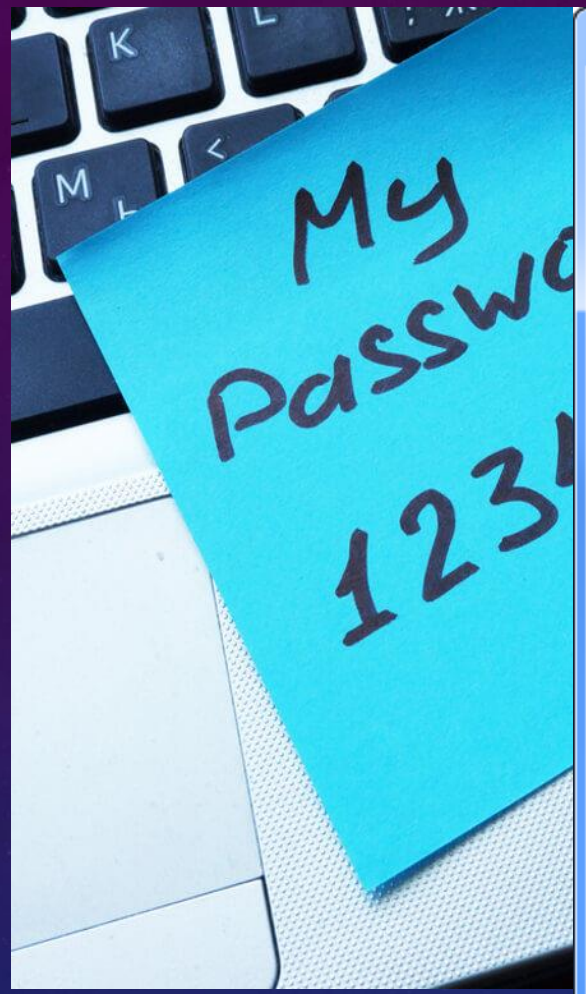
Morele.net: In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes.

Compromised data: Email addresses, Names, Passwords, Phone numbers

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began

HASŁA I ZABEZPIECZENIA

HIGIENA BUDOWY HASEŁ


My
Passwo
123


Add Entry
Add Entry
Create a new entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
My eMail account at MyProvider
Icon:
User name:
me@myprovider.net
Password:
Repeat:
Quality:
110 bits
18 ch.
URL:
http://www.myprovider.net/
Notes:
Here you can write some comments...
Here you can write some comments...
Here you can write some comments...
Here you can write some comments...
KeePass
Expires:
26.10.2020 12:00:00
Tools
OK
Cancel


Prevx
RISING
ca
Free
3 months
trial
BullGuard
Norton
by Symantec
FREE TRIAL
KASPERSKY
Emsisoft
Anti-Malware
AVG
VIPRE
from GFI Software
Quick Heal
McAfee
PANDA
SECURITY

POPULARNE SŁABE HASŁA

- qwerty
- 123456
- adminadmin
- password
- hasło
- michał
- kasia
- i inne imiona, imiona zwierzaków, czy data urodzin, albo numer telefonu.

TWORZENIE HASEŁ

1.Etap: wybieramy np. fragment wiersza, cytat, itp..

wlazł kotek na płotek i mruga piękna to piosneczka niedługa

2. Etap: tworzymy hasło

włkknapkimapatopana

3.Etap: wzmacniamy hasło cyframi

włkknapkimapatopana20221214

4.Etap: wzmacniamy hasło dużymi literami i znakami specjalnymi

WłKkNaPkImApAtOpAnA20221214!

5.Etap: tworzymy bardzo silne hasło !

WłKkN@Pk1m@p@t0p@n@20221214!

ZGŁASZANIE INCYDENTÓW

Każdą próbę oszustwa wysłaną za pośrednictwem SMS-a warto zgłosić do CSIRT NASK.

Należy to zrobić używając w swoim telefonie funkcji "przekaż" albo "udostępnij" i przesyłając treść wiadomości na numer *799-448-084*. Trafi ona do analityków CERT Polska, którzy zdecydują o dopisaniu podejrzanej domeny do listy ostrzeżeń.

ZGŁASZANIE INCYDENTÓW

799-448-084

* Z jednego numeru można zgłosić maksymalnie 3 wiadomości w ciągu 4 godzin.

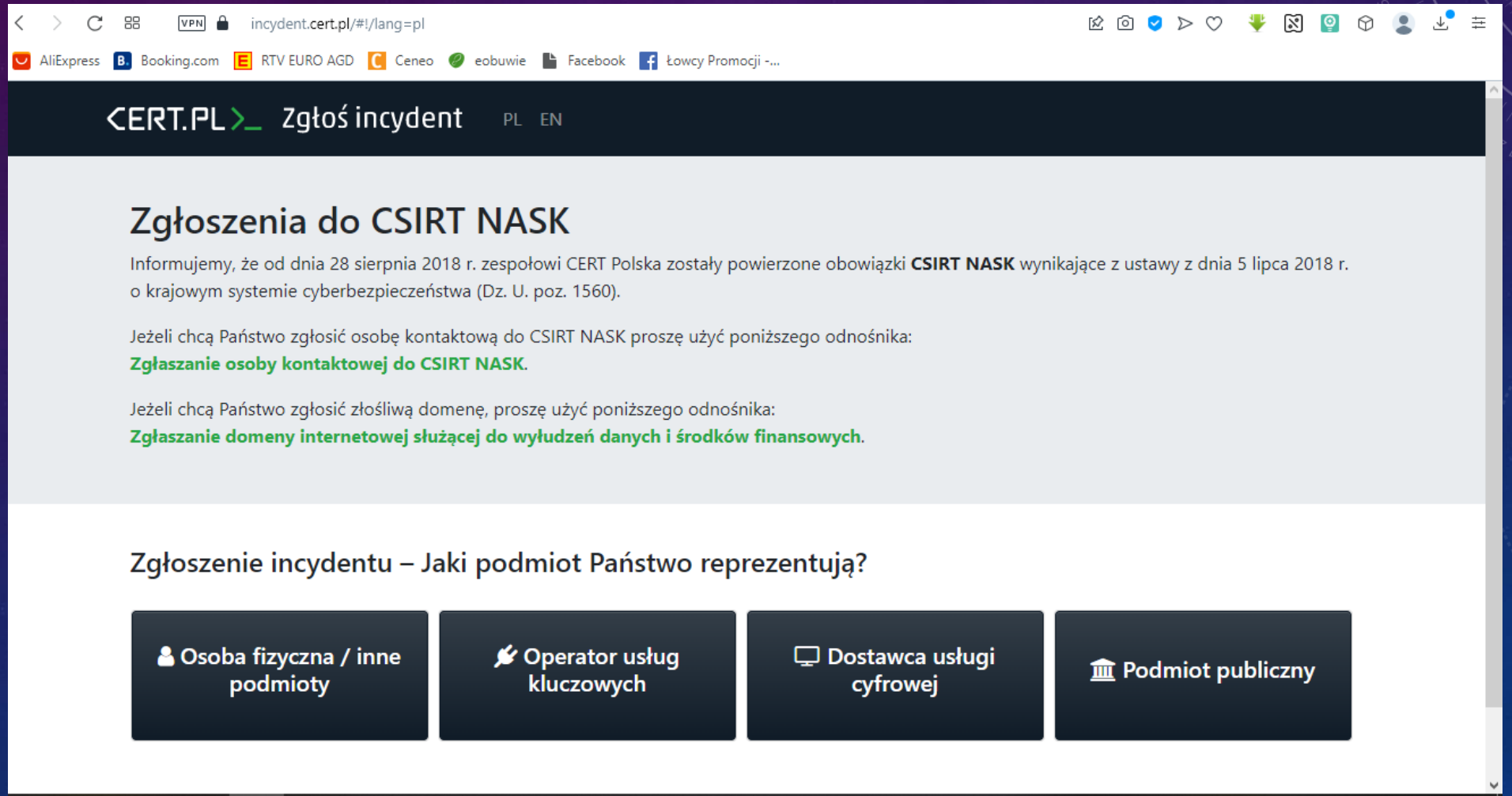
- Numer służy do zgłaszania prób wyłudzeń internetowych (phishingu, fałszywych aplikacji)
  - nie służy do zgłoszeń dotyczących usług SMS premium.

* Przekaż całą wiadomość w oryginalnej formie - nie wycinaj odnośnika ani treści.

Incydenty dot. np. fałszywych sklepów, ataków ransomware, należy zgłaszać pod adresem https://incydent.cert.pl/

ZGŁASZANIE INCYDENTÓW

Incydenty dot. np. fałszywych sklepów, ataków ransomware, należy zgłaszać pod adresem https://incydent.cert.pl/



KRADZIEŻ TAJEMNICY PRZEDSIĘBIORSTWA

Działania, które w znacznym stopniu usprawniają proces wykrywczy:

- Przypisanie sprzętu informatycznego do osoby, w tym urządzeń mobilnych takich jak telefony komórkowe
- Wykaz pracowników wraz z ich uprawnieniami dostępowymi do zasobów informatycznych
- Wykaz podmiotów zewnętrznych, które mają dostęp do zasobów informatycznych firmy

Z NASZEGO PODWÓRKA

- Zgłaszać, czy nie zgłaszać?
- Inne oczekiwania przedsiębiorców a inne organów ścigania po wystąpieniu incydentu

- Brak w firmach procedur wewnętrznych tworzonych dla działów bezpieczeństwa związanych z zabezpieczaniem cyfrowego materiału na potrzeby postępowania karnego.

- Zanotowano przypadki spraw w których dane analizowane są bezpośrednio na nośnikach mających stanowić dowód w sprawie.

Co takie działanie niesie za sobą w praktyce?

Dziękuję za uwagę

Wydział w Łodzi
Centralne Biuro Zwalczania Cyberprzestępczości