


**Wybrane problemy
cyberbezpieczeństwa na przykładach
scenariuszy ataków opartych na
COVID-19**

Dr inż. Agnieszka Gryszczyńska
Katedra Prawa Informatycznego
WPiA UKSW

Anty-Covid. Informatyka w zwalczaniu Covid-19, 22-23 czerwca 2020 r.

Inicjowanie i integrowanie działań zmierzających do przezwycięzania problemów związanych z Covid-19 metodami informatycznymi.

- 
- Pandemia COVID -19 znacząco wpłynęła na metody pracy, nauki czy realizacji zadań publicznych.
 - COVID-19 jest nie tylko poważnym problemem zdrowotnym, ale także niesie ryzyka dla cyberbezpieczeństwa.
 - Przestępcy szybko skorzystali z rozprzestrzeniania się wirusa i nadużywają popytu na informacje i zasoby.
 - Pandemia COVID – 19 dla cyberprzestępców stała się okazją do zwiększenia skuteczności ataków opartych na socjotechnice.

Jaka jest skala zagrożeń?

- Od 2018 do 2019 podwoiła się ilość incydentów zarejestrowanych przez zespół CERT Polska z 3739 incydentów w 2018 r. do 6 484 incydentów w 2019 r.
- W 2018 roku phishing stanowił 44 % wszystkich incydentów.
- Zgodnie z zapowiedzią raportu CERT Polska za 2019 na 6 484 przeanalizowane incydenty stwierdzono 3 516 przypadków phishingu.

Krajobraz bezpieczeństwa polskiego internetu, Raport roczny z działalności CERT Polska 2018, s. 13, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (dostęp 20.6.2020)

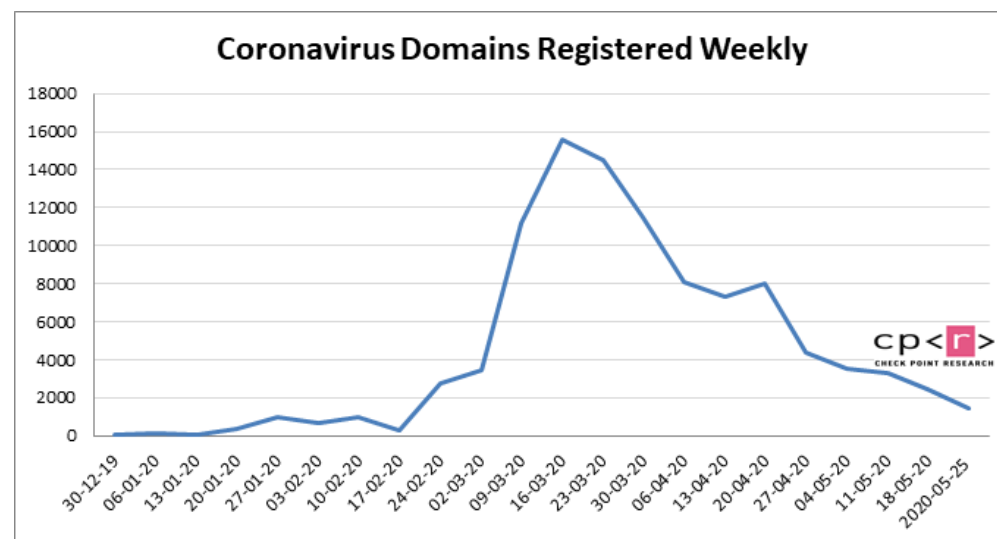
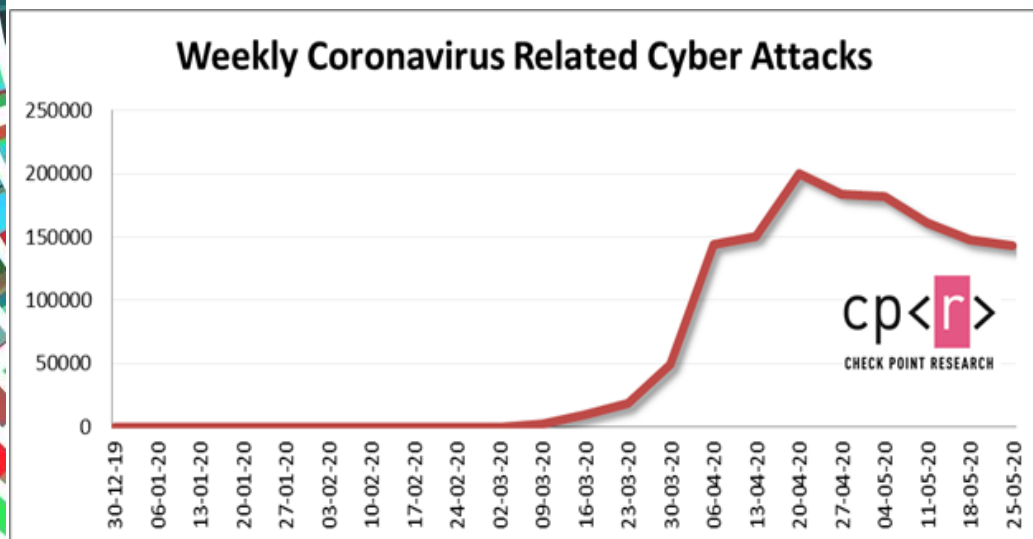
- Indeks zagrożenia w Polsce wg raportu Check Point wynosi 42,7 pkt, co daje Polsce 26 miejsce w Europie i 51. na świecie
- W maju 2020 polskie przedsiębiorstwa były atakowane średnio ponad 300 razy dziennie
- Ogólna ilość cyberataków wzrosła w maju o 16% w związku z ponownym otwieraniem gospodarki.
- <https://www.rp.pl/CYFROWA-IT/306179901-Polska-cyberniebezpieczna-Druzgocacy-ranking.html> (dostęp 20.6.2020)
- <https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/> (dostęp 20.6.2020)

Jaka jest skala ataków związanych z COVID-19?

- W kwietniu Google zaobserwował 18 mln wiadomości phishingowych oraz złośliwego oprogramowania powiązanych z COVID-19 dziennie

<https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams> (dostęp 20.6.2020)

Uwagę zwraca również znaczący wzrost rejestracji domen wykorzystujących pandemię do infekowania użytkowników internetu, wyłudzenia danych, środków finansowych, dezinformacji



<https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/> (dostęp 20.6.2020)

Przykładowe incydenty

- Infekowanie złośliwym oprogramowaniem (głównie trojanami bankowymi) przy pomocy wiadomości e-mail zawierających złośliwe pliki imitujące CV, zwolnienia lekarskie lub dokumenty związane ze wsparciem finansowym podczas COVID-19
- Tworzenie stron fikcyjnych sklepów internetowych sprzedających środki ochronne
- Tzw. „oszustwa nigeryjskie” z wykorzystaniem w wiadomości e-mail scenariusza związanego ze wsparciem finansowym związanym z COVID-19
- Organizowanie fałszywych zbiórek pieniędzy na cele związane z ochroną zdrowia i wsparciem dla szpitali
- Tworzenie fałszywych stron agentów rozliczeniowych wyłudzających dane do logowania do bankowości elektronicznej
- Tworzenie fałszywych stron wyłudzających dane do logowania to portali społecznościowych
- Tworzenie fałszywych stron podszywających się pod WHO, Zoom, Microsoft, Google w celu wyłudzenia danych
- Infekowanie placówek ochrony zdrowia oprogramowaniem ransomware w celu wyłudzenia okupu (przykład Szpital Uniwersytecki w Brnie)



Przykładowe scenariusze
ataków

Fałszywe zbiórki:

Adres fałszywej strony:

[https://pomoc\[.\]sie-pomaga\[.\]net/koronawirus?SS52](https://pomoc[.]sie-pomaga[.]net/koronawirus?SS52)

siepo❤️aga.pl

Zbiórka na Siepomaga | English | Logowanie | Rejestracja



Potrzebujący

Organizacje

Zwierzęta



Wspieramy polską służbę zdrowia w czasie walki z epidemią COVID-19



ZBIÓRKA NA CEL

Doposażenie ośrodków medycznych w niezbędny sprzęt

cała Polska

Rozpoczęcie: 3 Marca 2020

15 Marca 2020, 15:11

Jesteście naszymi Bohaterami! Swoją pracą pomagacie nam wszystkim ❤️

Kochani, otrzymujemy mnóstwo wiadomości z prośbą o pomoc od lekarzy i pielęgniarek z całej Polski. Sytuacja jest dramatyczna. Ze względu na liczbę podejrzeń wiele szpitali przekształcających jest w zakłady, a zdanie „brakuje w nich wszystkiego” jest

Zbiórka zweryfikowana przez Fundację Siepomaga

371 431,00 zł

WSPARŁO 10 217 OSÓB



Wesprzyj

Zańń skarbonkę

Wyślij sms

Pomóż nagłośnić zbiórkę



Udostępnij



Tweetuj




Dziękuję



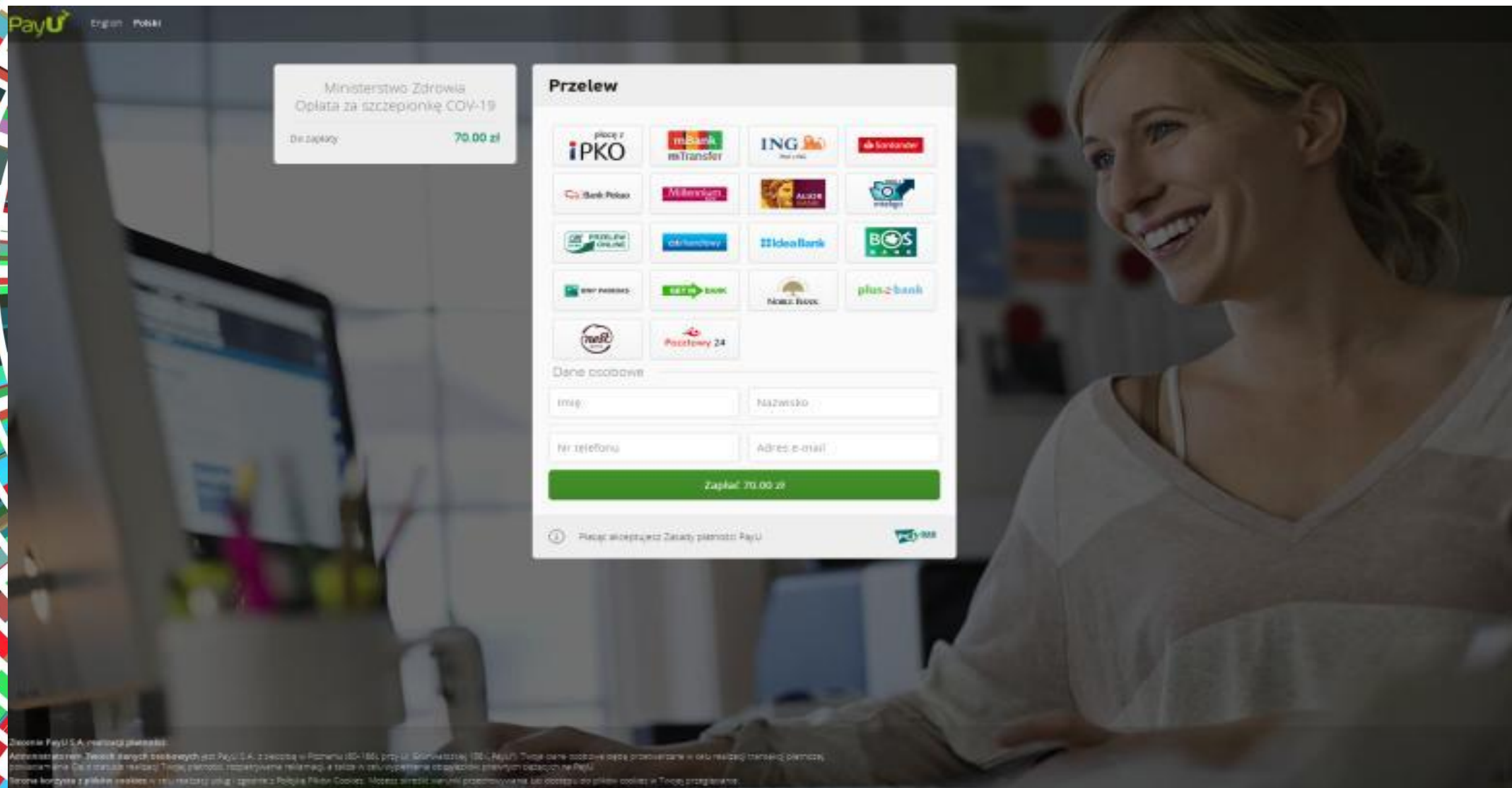
Wyślij sms

18 332 udostępnienia

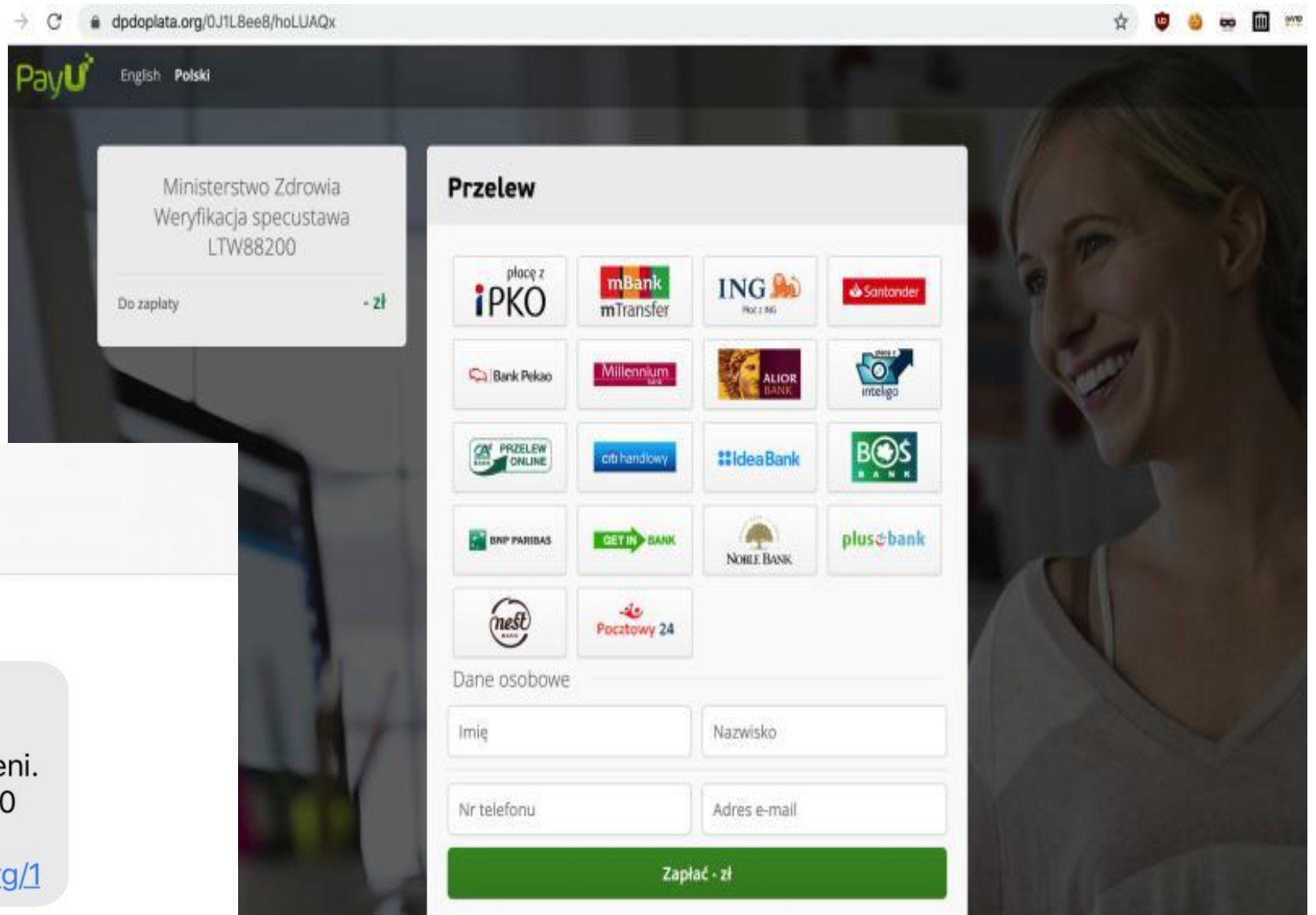


Ataki z wykorzystaniem
fałszywych stron
agentów rozliczeniowych
i banków

Fałszywa strona PAYU (atak aktywny w dniu 13 marca 2020)



Fałszywa strona PAYU!





→ ↻ dpdoplata.org/0J1LBee8/hoLUAQx ☆ 🔒 📱 🌐 🗄

PayU English Polski

Ministerstwo Zdrowia
Weryfikacja specustawa
LTW88200

Do zapłaty - zł

Przelew

placę z iPKO	mBank mTransfer	ING Poc 24	Santander
Bank Pekao	Millennium	ALIOR BANK	inteligo
PRZELEW ONLINE	cbi handlowy	IdeaBank	BOS BANK
BRP PARIBAS	GET IN BANK	NOBLE BANK	plus bank
nest BANK	Pocztowy 24		

Dane osobowe

Imię Nazwisko

Nr telefonu Adres e-mail

Zapłać - zł

←  **Infosms** ⋮

Wiadomość tekstowa
piątek, dzisiaj

Informujemy, iż zgodnie z specustawa dt. koronawirusa Państwa środki na rachunku zostają przekazane do rezerw krajowych NBP. Zaloguj się, aby zatrzymać **1000 PLN**.
<https://dpdoplata.org/0>

23 minut temu





Login

Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów



Login

Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów

W celu otrzymania świadczenia prosimy o potwierdzenie danych osobowych poprzez profil zaufany.

Zaloguj się przy pomocy banku



Przykładowe SMSy z linkami

RP informuje o obowiązkowych szczepieniach na koronawirusa. Szczepienia zaczyna się 20.03.2020. Koszt 10 zł, opłac aby uniknąć kolejek
<https://nfz582.com/1259>

czwartek, 16 kwietnia 2020



Przesyłka nr 002887399112 wymaga opłaty dezynfekcyjnej w kwocie 0.80 PLN. Opłac, aby otrzymać dostawę
<https://eplatnosc.com/1>

17:14

Paczka nr 00772990012 wymaga dezynfekcji. Oplata dodatkowa wynosi 1.70 PLN. Opłac, aby otrzymać przesyłkę.
<https://paczkadpd.com/1>

Twoja paczka została wstrzymana.

W celu zapewnienia bezpieczeństwa, wymagana jest dezynfekcja przesyłki. W celu wykonania dezynfekcji *prosimy o wpłatę kwoty 0.50zł (50 groszy)*.

Po dokonaniu płatności przesyłka natychmiastowo zostanie przekazana kurierowi do doręczenia.

Brak wpłaty oznacza skierowanie przesyłki na 30 dniową kwarantannę, po upływie tego czasu paczka ruszy w dalszą drogę.

Za utrudnienia przepraszamy

PLACĘ

Przykładowe fałszywe strony pośredników płatności

dotpay[®]



Odbiorca płatności: **DPD POLSKA SP Z.O.O (NIP: 5260204110)**
Opis: **OPŁATA KURIERSKA #2736193**

Kwota całkowita: **19.99 PLN**

Wybierz metodę płatności

Szybkie transfery



Przelewy Online



Zatwierdź regulamin

- Akceptuję Regulamin płatności i politykę cookies Dotpay sp. z o.o.
- Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 983 z późn. zmianami) przez Dotpay sp. z o.o. 30-552 Kraków (Polska), Wielicka 72. Mam prawo wglądu i poprawiania swoich danych.

https://dpd-payment.com/?997582=2&kwota=15.11

dotpay[®]



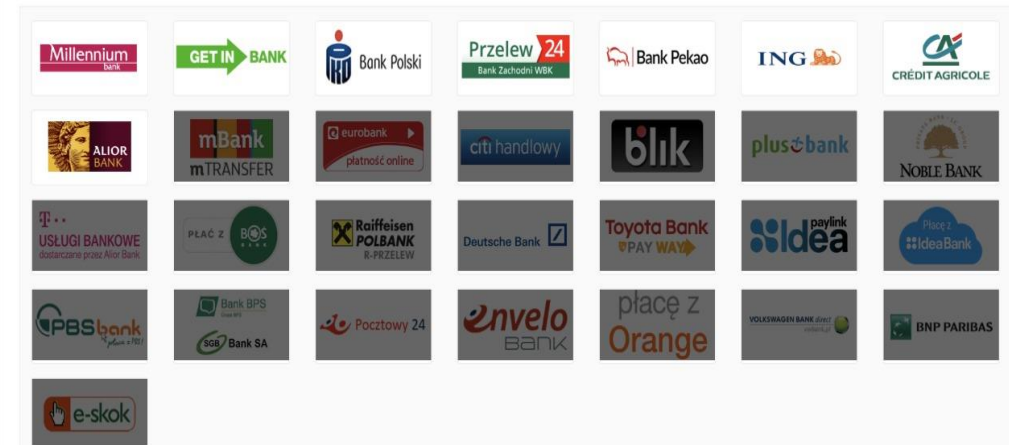
Odbiorca płatności: **DPD POLSKA SP Z.O.O (NIP: 5260204110)**

Opis: **OPŁATA KURIERSKA #2736193**

Kwota całkowita: **15.11 PLN**

Wybierz metodę płatności


Szybkie transfery



Przykładowe fałszywe strony pośredników płatności

🏠 dhl24.online/?997582=2&k 📱 ☰

dotpay



Odbiorca płatności::
DHL POLSKA SP Z.O.O (NIP: 5260204110)

Opis:
OPLATA KURIERSKA #18465684732

Kwota całkowita:
15.11 PLN

Wybierz metodę płatności

Szybkie transfery









PayU


Płatność dla PayU - szybkie płatności
F/20838493/10/2018 - niedopłata 1,01

Do zapłaty **1.01 zł**

Płatność

Przelew

 płacę z iPKO	 mBank mTransfer
 ING Płać z ING	 Santander
 Bank Pekao	 Millennium bank
 ALIOR BANK	 płacę z inteligo


Poczty 24



Dane osobowe

Imię Nazwisko

Adres e-mail

Zapłać 1.01 zł

English Polski

 Płacąc akceptujesz [Zasady płatności PayU.](#) 

Administratorem Twoich danych osobowych jest PayU S.A. z siedzibą w Poznaniu (60-166), przy ul. Grunwaldzkiej 182 („PayU”). Twoje dane osobowe będą przetwarzane w celu realizacji transakcji płatniczej, powiadamiania Cię o statusie realizacji Twojej płatności, rozpatrywania reklamacji, a także w celu wypełnienia obowiązków prawnych ciążących na PayU.

Strona korzysta z plików cookies w celu realizacji usług i zgodnie z [Polityką Plików Cookies](#). Możesz określić warunki przechowywania lub dostępu do plików cookies w Twojej przeglądarce.

Przykładowe fałszywe strony pośredników płatności

https://in-post.tk/h6svg

dotpay

Informacja o płatności:
Odbiorca: DotPay S.A.
Opis: Dopłata do przesyłki
Kwota: 1 PLN

Wybrany kanał płatności:

Karty płatnicze

Szybkie transfery

Logos of various banks and payment methods: VISA, Mastercard, mBank, mTRANSFER, Inteligo, iPKO, Citi Handlowy, Bank Zachodni WBK, Bank Pekao.

https://in-post.tk/h6svg

Logos of various banks: Bank Zachodni WBK, Bank Pekao, ING, Millennium bank, ALIOR BANK, Toyota Bank, eurobank, BOS, Deutsche Bank, Pocztowy 24, Bank BPS, SGB Bank SA, GET IN BANK, IdeaBank.

https://in-post.tk/h6svg

Raiffeisen POLBANK

Przelewy online

BNP PARIBAS VOLKSWAGEN BANK direct

BANK SPÓŁDZIELCZY

Informacja o posiadaczu konta

Imię:

Nazwisko:

Email:

Kraj:

Akceptuję Regulamin dokonywania wpłat w Dotpay

Akceptuję Regulamin dokonywania wpłat w Dotpay

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay S.A. (Wielicka 72, Kraków) dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 883 z późn. zmianami). Mam prawo wglądu i poprawiania swoich danych.

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay S.A. (Wielicka 72, Kraków, dalej: "Dotpay") w celach marketingowych Dotpay i jej partnerów biznesowych oraz na otrzymywanie od Dotpay informacji handlowych Dotpay i jej partnerów na podany przeze mnie adres email. Dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie przepisów prawa. Podanie danych jest dobrowolne. Mam prawo wglądu i poprawiania swoich danych.

Polityka cookies.

Dokonaj płatności

Copyright © 2001-2018 by dotpay

VERIFIED by VISA MasterCard SecureCode JCB J/Secure

Przykładowe fałszywe strony pośredników płatności


https://in-post.tk/h6svg43/cc119fce7602b9c1605fc_payment_3de887...

Połączenie jest bezpieczne


Informacje, które wysyłasz tej witrynie (na przykład hasła lub numery kart kredytowych), pozostają prywatne. [Szczegóły](#)

[USTAWIENIA WITRYNY](#)

Karty płatnicze



Szybkie transfery



Bank Zachodni WBK Bank Pekao

<https://in-post.tk/h6svg>

in-post.tk

Chrome sprawdził, że wydawcą certyfikatu tej witryny jest Let's Encrypt Authority X3.

[Informacje o certyfikacie](#)

in-post.tk

Połączenie z in-post.tk jest szyfrowane przy użyciu nowoczesnego zestawu szyfrów.

Połączenie z szyfrowaniem TLS 1.2.

Połączenie jest szyfrowane i uwierzytelnianie algorytmem AES_128_GCM, a mechanizm wymiany kluczy to ECDHE_RSA.

[Co to oznacza?](#)

placę z **iPKO** **citi handlowy**

Bank Zachodni WBK

Przeglądarka certyfikatów

in-post.tk

WYSTAWIONY DLA

Nazwa pospolita (CN)
in-post.tk

Numer seryjny

03:E9:36:EC:18:3D:A2:DF:
98:10:7E:ED:A9:D4:DD:4B:7E:D7

WYSTAWIONY PRZEZ

Nazwa pospolita (CN)
Let's Encrypt Authority X3

Organizacja (O)

Let's Encrypt

OKRES WAŻNOŚCI

Wystawiony dnia
27.11.2018

Wygasa dnia
25.02.2019

ODCISKI CYFROWE

Odcisk cyfrowy SHA-256

Przeglądarka certyfikatów

sni.cloudflaressl.com

CloudFlare, Inc.

OKRES WAŻNOŚCI

Wystawiony dnia
04.12.2018

Wygasa dnia
04.12.2019

ODCISKI CYFROWE

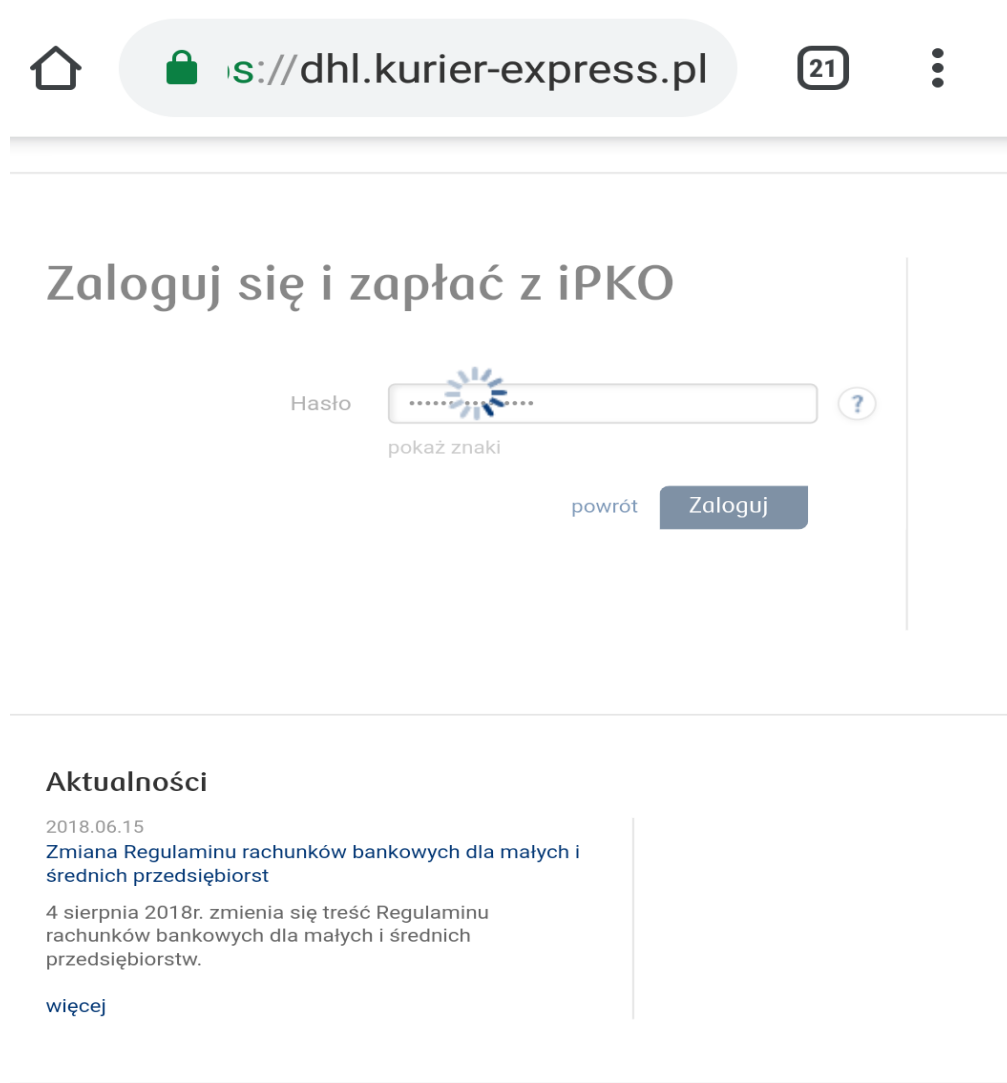
Odcisk cyfrowy SHA-256
BF BB B8 C0 39 C5 96 93 89 FE 63 33 14
22 5E 6A 03 F9 96 43 89 B8 6E 93 34 E8
47 C8 2D 76 42 67

Odcisk cyfrowy SHA-1
56 CB D9 59 65 6B 0E 94 01 0D A0 5C 25
FD CA 8D EE 8E 4E D8

ROZSZERZENIA

Alternatywna nazwa podmiotu certyfikatu
*.payu-platnosci.ml
sni.cloudflaressl.com
payu-platnosci.ml

Przykładowe fałszywe strony banków



The image shows a browser window with the address bar displaying 'https://dhl.kurier-express.pl'. The page content includes a login form with the heading 'Zaloguj się i zapłać z iPKO'. The password field is masked with dots and has a 'pokaż znaki' (show characters) link below it. There is a 'Zaloguj' button and a 'powrót' (back) link. At the bottom, there is a section titled 'Aktualności' (News) with a date '2018.06.15' and a link to 'Zmiana Regulaminu rachunków bankowych dla małych i średnich przedsiębiorstw' (Change of terms and conditions for small and medium enterprises). A 'więcej' (more) link is also present.

Przeglądarka certyfikatów

sni.cloudflaressl.com

CloudFlare, Inc.

OKRES WAŻNOŚCI

Wystawiony dnia

04.12.2018

Wygasa dnia

04.12.2019

ODCISKI CYFROWE

Odcisk cyfrowy SHA-256

70 30 07 FA 2D A3 4D 9F 4F 90 1C DA 61
0F 5C B6 DC 4C CC BB DE 3A C3 C0 90 DF
5D A9 47 48 05 D7

Odcisk cyfrowy SHA-1

EF A1 4C F6 3D 49 94 19 A7 36 F9 6D 10
9E DD F3 E9 10 7E ED

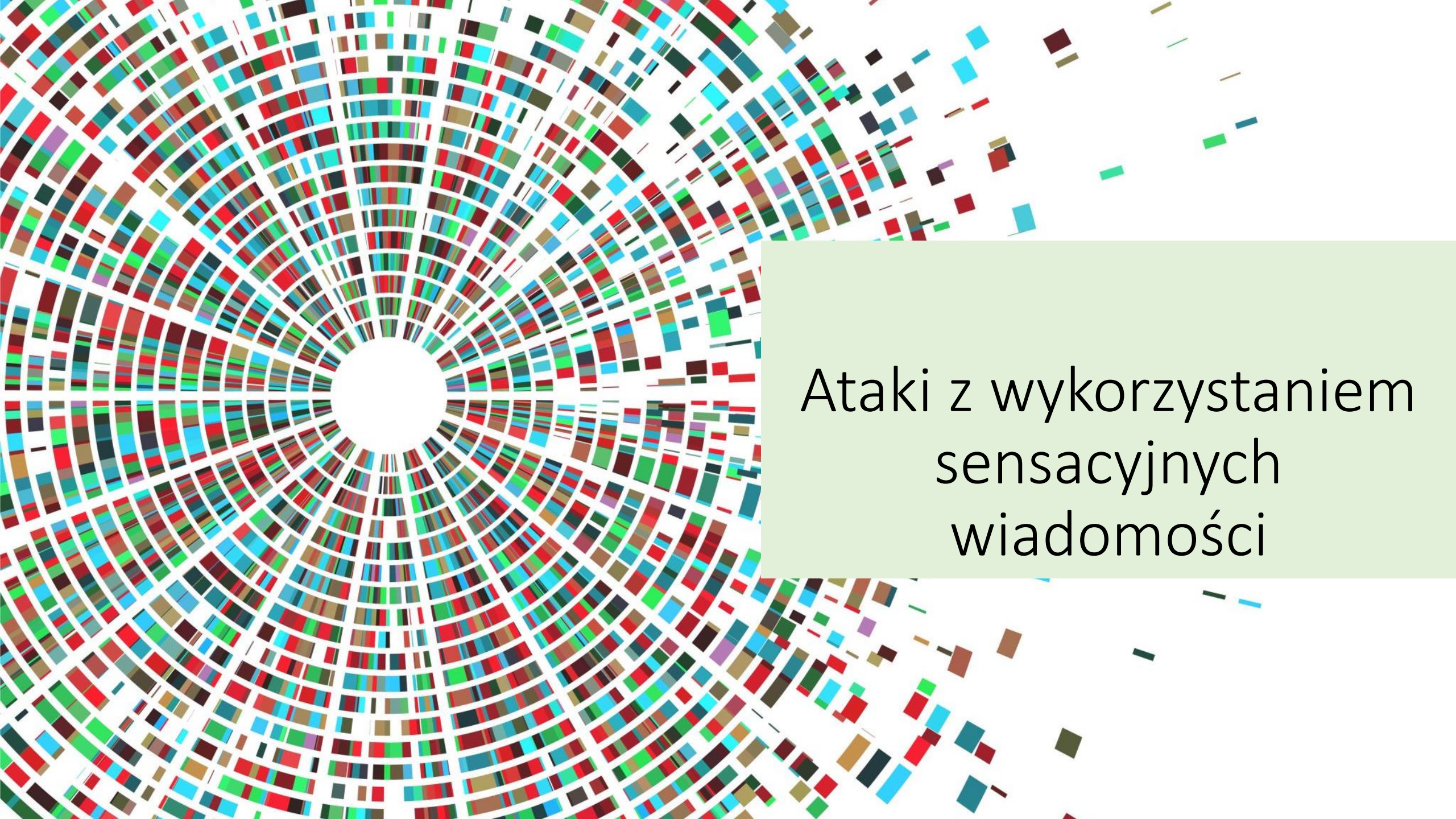
ROZSZERZENIA

Alternatywna nazwa podmiotu certyfikatu

*.kurier-express.pl

sni.cloudflaressl.com

kurier-express.pl



Ataki z wykorzystaniem
sensacyjnych
wiadomości

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

f PODZIEL SIĘ



Koronawirus nadal rozprzestrzenia się na świecie. Liczba zachorowań w Polsce wzrosła do 17 (prawdopodobnie liczba ta jest mocno zaniżona). Kolejna zakażona osoba to kobieta, która przebywa w szpitalu w Poznaniu. Rząd postanowił wprowadzić kontrole sanitarne na granicach z Czechami i Niemcami, a od jutra na pozostałych przejściach granicznych. Tymczasem pierwsze dwa przypadki zakażenia koronawirusem odnotowano na Cyprze co oznacza, że Covid-19 pojawił się już we wszystkich 27 krajach Unii Europejskiej. Z punktu widzenia zagrożenia epidemiologicznego, Główny Inspektor Sanitarny nie zaleca podróżowania do Chin, Hongkongu oraz Korei Południowej, Włoch, Iranu, Japonii, Tajlandii, Wietnamu, Singapuru i Tajwanu. Ciężki przebieg choroby obserwuje się u ok. 15-20% osób. Do zgonów dochodzi u 2-3% osób chorych. Prawdopodobnie dane te zaniżono, gdyż u wielu osób z lekkim przebiegiem zakażenia nie dokonano potwierdzenia laboratoryjnego. Zdaniem ekspertów liczba chorych w Polsce to około 250 przypadków, we wszystkich województwach. Poniżej materiał dający do myślenia na temat obiegu informacji i ich rzetelności w naszym kraju.

WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT

Przykładowe phishingowe nazwy domenowe: koronawirusnews[.]com[.]pl koronawirusnews[.]net[.]pl
ikoronawirusnews[.]pl e-koronawirusnews[.]pl

Porwanie dziecka ze szpitala zakaźnego. [WIDEO]

Porwanie dziecka ze szpitala zakaźnego. [WIDEO]

 PODZIEL SIĘ





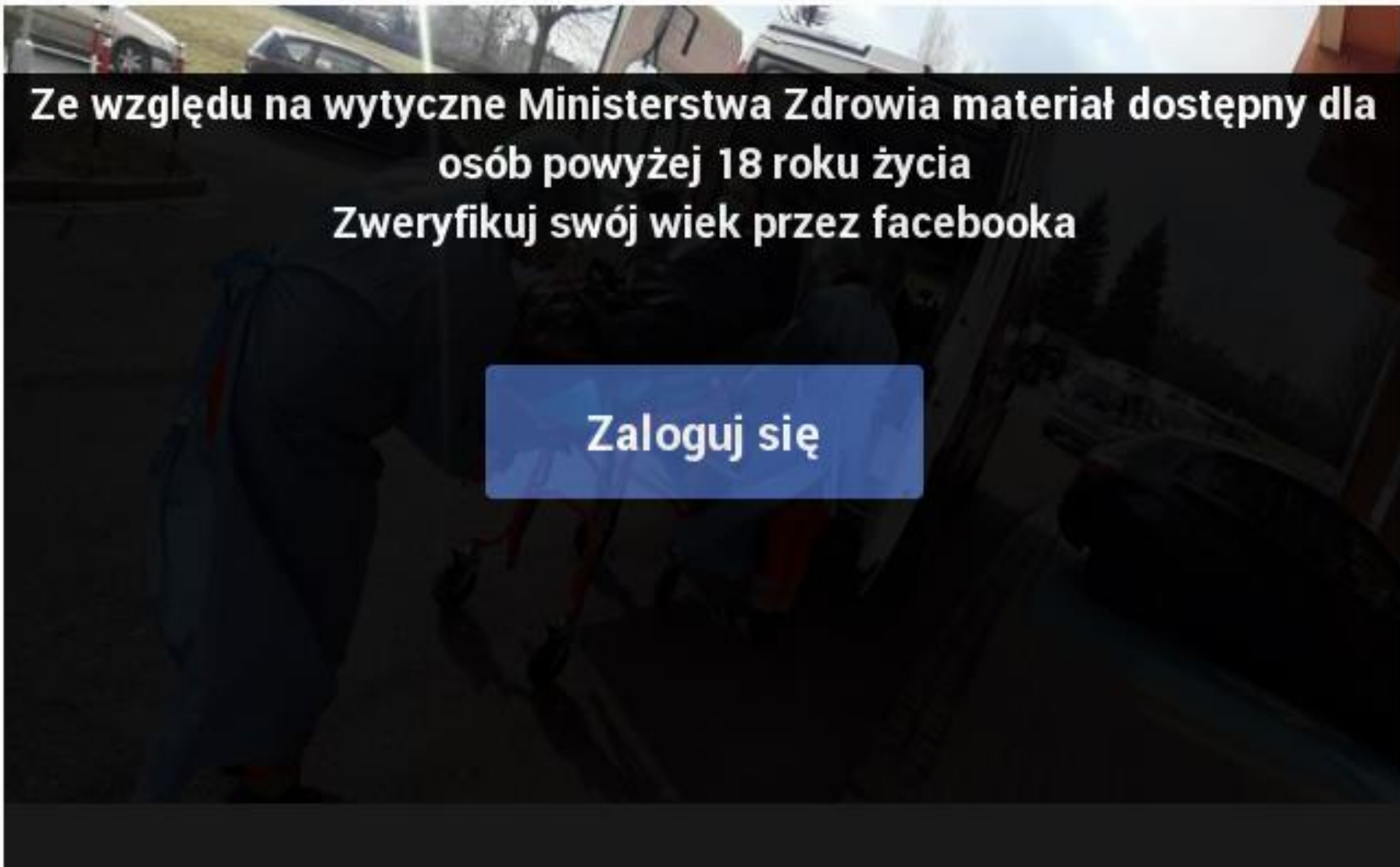


Dziewczynka w wieku 3 lat została porwana ze szpitala Zakaźnego w Warszawie przy ul. Wolskiej 37 przez ojca Krzysztofa K. z konkubiną. Dzisiaj o około godziny 10 ojciec 3-letniej

Wendy, chorując na zakaźne dziecko leżące w izolatce z powodu wirusa SARS-CoV-2.
www.fakt.pl/wydarzenia/polska/rzeszow



WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT NAMNAŻAJĄCEJ SIĘ LICZBY ZARAŻONYCH W POLSCE.



Ze względu na wytyczne Ministerstwa Zdrowia materiał dostępny dla
osób powyżej 18 roku życia
Zweryfikuj swój wiek przez facebooka

Zaloguj się



Co ułatwia sprawcom ataki i utrudnia ustalenie ich tożsamości?

- Możliwość anonimowego korzystanie z usług świadczonych drogą elektroniczną
- Wykorzystanie tożsamości innych osób (z uwagi na brak weryfikacji tożsamości przy korzystaniu z e-usług)
- Ograniczenie zakresu danych publikowanych w bazach WHOIS – utrudniające m.in. atrybucje ataku oraz prowadzenie postępowań karnych
- Obrót zarejestrowanymi na dane innych osób kartami SIM
- Brak przepisów regulujących gromadzenie logów, ich struktury oraz ustalenia okresu ich przechowywania
- Brak retencji danych „internetowych” – w szczególności w zakresie logów oraz danych abonentów usług
- Stosowanie NAT w sieciach (przy jednoczesnym niegromadzeniu przez większość podmiotów -w tym banki numerów portów)
- Łatwość pozyskania rachunków bankowych do prania pieniędzy pochodzących z przestępstwa
- Dostępność anonimowych usług płatniczych (płatności w kryptowalucie, płatności przy pomocy SMS Premium)
- Brak ogólnych regulacji dotyczących blokowania domen podszywających się pod inne podmioty lub służących do popełnienia przestępstwa
- Wadliwa regulacja karnoprawnych znamion kradzieży tożsamości
- Bardzo niskie zagrożenie karne przestępstwa „hackingu”



Czy i jak zablokować dostęp do stron internetowych wyludzających dane?

POROZUMIENIE z dnia 23 marca 2020 o współpracy w zakresie ochrony użytkowników internetu przed stronami wyludzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej

między
Orange Polska S.A.
Polkomtel Sp. z o.o.
P4 Sp. z o.o.
T-Mobile Polska S.A.

a
Ministrem Cyfryzacji oraz Prezesem Urzędu Komunikacji Elektronicznej (zwanymi dalej „Stroną rządową”)

a także

Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym

- W okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, NASK-PIB będzie opracowywał, prowadził i utrzymywał jawną listę ostrzeżeń dotyczących domen internetowych, które służą do wyludzeń danych i środków finansowych użytkowników internetu (dalej „Lista Ostrzeżeń”). Lista Ostrzeżeń jest prowadzona w formie publikacji na stronie internetowej www.cert.pl/ostrzezenia_phishing.
- Na Listę Ostrzeżeń wpisywane są domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i w ten sposób doprowadzenie ich do niekorzystnego rozporządzenia środkami finansowymi albo do wyludzenia ich danych osobowych
- Każdy może zgłosić domenę internetową służącą do wyludzeń danych i środków finansowych do NASK-PIB. Zgłoszenia powinny zawierać uzasadnienie dotyczące każdej zgłoszonej domeny
- Zgłoszeń domen internetowych, o których mowa w niniejszym Porozumieniu, dokonuje się na stronie <https://incydent.cert.pl/phishing> lub emailiem na adres: cert@cert.pl.
- Każde zgłoszenie jest weryfikowane przez NASK-PIB. NASK-PIB dołoży najwyższej staranności, aby weryfikacja zgłoszenia trwała najkrócej jak to możliwe w celu zapewnienia realizacji celów niniejszego Porozumienia. Po dokonaniu weryfikacji NASK-PIB niezwłocznie wpisuje na Listę Ostrzeżeń domeny, które pozytywnie przeszły weryfikację



Techniczna implementacja blokowania na podstawie porozumienia

Operatorzy oświadczają, że od dnia udostępnienia Listy Ostrzeżeń przez NASK-PIB dołożą należytej staranności, by:

- a) uniemożliwić dostęp do stron internetowych wykorzystujących nazwy domen internetowych opublikowanych na Liście Ostrzeżeń **poprzez ich usunięcie ze swoich systemów teleinformatycznych służących do zamiany nazw domen internetowych na adresy IP**, w najkrótszym możliwym czasie od otrzymania informacji o wpisaniu nowej domeny internetowej na Listę Ostrzeżeń,
- b) **przekierować połączenia odwołujące się do nazw domen internetowych opublikowanych na Liście Ostrzeżeń do strony internetowej prowadzonej przez NASK-PIB zawierającej komunikat** skierowany do użytkowników internetu lub do innej strony o analogicznym komunikacie z wykorzystaniem narzędzi dostępnych po stronie Operatorów, obejmujący w szczególności informacje o lokalizacji Listy Ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na Listę Ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub środków finansowych. W przypadku przekierowania do strony Operatora, Operator przekazuje NASK dane statystyczne dotyczące liczby wywołań danej domeny od momentu jej zablokowania



W dniu 20.6.2020 na liście znajdowało się 2 357 nazw domenowych

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

Wybrane statystyki Listy Ostrzeżeń:

Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod agentów rozliczeniowych i banki, rejestrują nazwy domenowe podszywające się pod pocztę, podmioty świadczące usługi transportowe, rozliczeniowe i banki, na Liście Ostrzeżeń znajdują się m.in. nazwy domenowe zawierające następujące ciągi znaków:

„poczta” (148)

„pay” (113)

„kurier” (85)

„dotpay” (75)

„paczka” (63)

„allegro” (43)

„pocztex” (35)

„dhl” (28)

„inpost” (28)

„platnosc” (20)

„payu” (19)

„bank” (18)

„dpd” (18)

„paczki” (13)

„dostawa” (13)

„ssl” (9)

Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod portale informacyjne i wyłudniają dane do logowania do portali społecznościowych (zwykle kolejnym etapem jest podszywanie się pod osoby, których dane do logowania pozyskano i wysłanie próśb o pożyczanie pieniędzy poprzez wysłanie kodu BLIK), rejestrowane są głównie nazwy domenowe zawierające następujące ciągi znaków”

• „fakt” (261)

• „porwan” (203)

• „gwałt” (156)

• „poszukiwan” (60)

• „news” (59)

• „dziennik” (40)

• „korona” (10)




Postulaty *de lege ferenda*

- Celowe jest wprowadzenie obowiązków związanych z przechowywaniem logów dostępowych oraz danych abonentów usług świadczonych drogą elektroniczną przez okres 12 miesięcy (retencja danych).
- Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi drogą elektroniczną.
- Z uwagi na to, że w części z omówionych powyżej ataków wykorzystano nazwy domenowe z domeny *.pl lub domeny gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski należy dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących domeny (abonentów).
- Jawny rejestr domeny .pl powinien zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta.
- Celowe jest wprowadzenie w sytuacji nabycia karty przedpłaconej (SIM) od innego podmiotu obowiązku ponownej rejestracji takiej karty pod rygorem dezaktywacji usługi. Aktualna regulacja w zestawieniu z praktyką pokazuje, że cel wprowadzenia rejestracji abonentów usług przedpłaconych ustawą o działaniach antyterrorystycznych nie został osiągnięty, a zarejestrowane na dane innych osób karty SIM można kupić na powszechnie dostępnych portalach ogłoszeniowych oraz na forach w sieci TOR.
- Celowe jest dalsze prowadzenie Listy Ostrzeżeń, należy jednak jej dalsze prowadzenie oprzeć o przepisy prawa powszechnie obowiązującego i wprowadzić procedurę odwoławczą.



Postulaty *de lege ferenda*

- W związku z narastającym negatywnym zjawiskiem kradzieży tożsamości i wykorzystywaniem tożsamości innych osób przez cyberprzestępców celowe jest rozszerzenie odpowiedzialności karnej za czyn z art. 190 a § 2 KK.
- Aktualnie z uwagi na wąsko określony w art. 190a § 2 KK cel działania sprawcy, poza zakresem penalizacji pozostaje sytuacja, w której sprawca działa w celu ukrycia własnej tożsamości lub wyrządzenia szkody innej osobie niż ta, której danymi się posługuje.
- *De lege ferenda* można postulować zmianę art. 190a § 2 KK poprzez użycie zamiast wyrażenia "w celu" sformułowania "w zamiarze". Analiza *sposobów działania* sprawców wskazuje również na zasadność odstąpienia od zasady tożsamości podmiotu, pod który sprawcy się podszywają i któremu chcą wyrządzić szkodę.
- Mając na względzie skalę oraz skutki ataków niezbędne jest również podniesienie górnej granicy odpowiedzialności karnej za czyn z art. 267 § 1 kk. Aktualne zagrożenie karne wynosi do 2 lat pozbawienia wolności.



Dziękuję za uwagę!

Kontakt:
a.gryszczynska@uksw.edu.pl