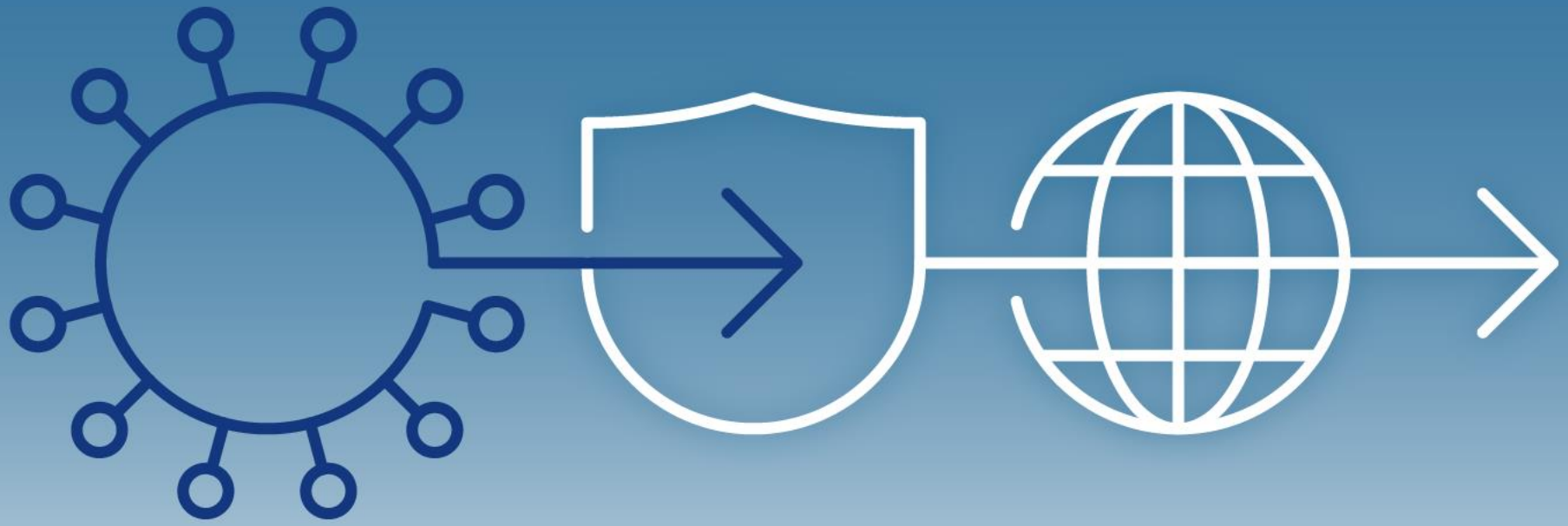
Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Wykorzystanie pandemii przez cyberprzestępców na przykładach wybranych ataków

Dr inż. Agnieszka Gryszczyńska
Katedra Prawa Informatycznego
WPiA UKSW

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.

W 2018 r. zespół CERT Polska przyjął **19 439 zgłoszeń** i odnotował **3 739 incydentów bezpieczeństwa**, co daje wzrost ilości incydentów o 17,5% w stosunku do 2017 r.

W 2019 r. CERT Polska zarejestrował **6 484 incydenty**. Oznacza to lawinowy wzrost ilości incydentów – o 73 % w porównaniu z 2018 r.

Typ incydentu	Liczba incydentów	%	Liczba incydentów	%
	2018	2018	2019	2019
Obraźliwe i nielegalne treści	431	11,53	812	12,5
Złośliwe oprogramowanie	862	23,05	969	14,9
Gromadzenie informacji	101	2,7	95	1,5
Próby włamań	153	4,09	77	1,2
Włamania	125	3,34	160	2,5
Dostępność zasobów	49	1,31	57	0,9
Atak na bezpieczeństwo informacji	46	1,23	41	0,6
Oszustwa komputerowe	1 878	50,23	**4 086**	**63,0**
- w tym phishing	1655	44,26	3 516	54,2
Podatne usługi	69	1,85	102	1,6
Inne	25	0,67	85	1,3

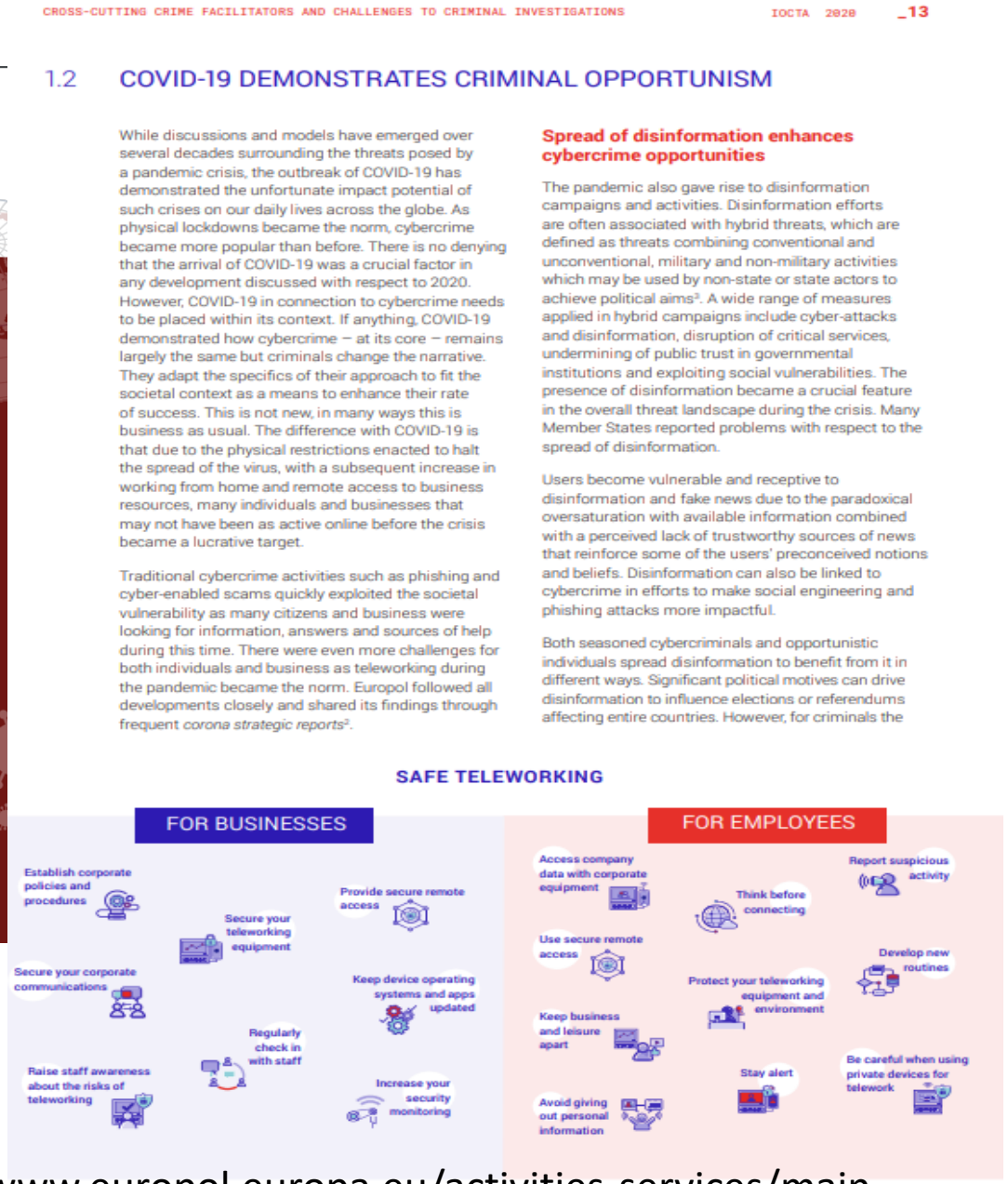
Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, s. 10, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf
Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, s. 9, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf

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)

https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know



https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Ataki związane z edukacją zdalną

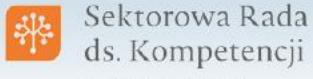
Nastolatkowie włamali się do dziennika elektronicznego. Grozi im 8 lat więzienia

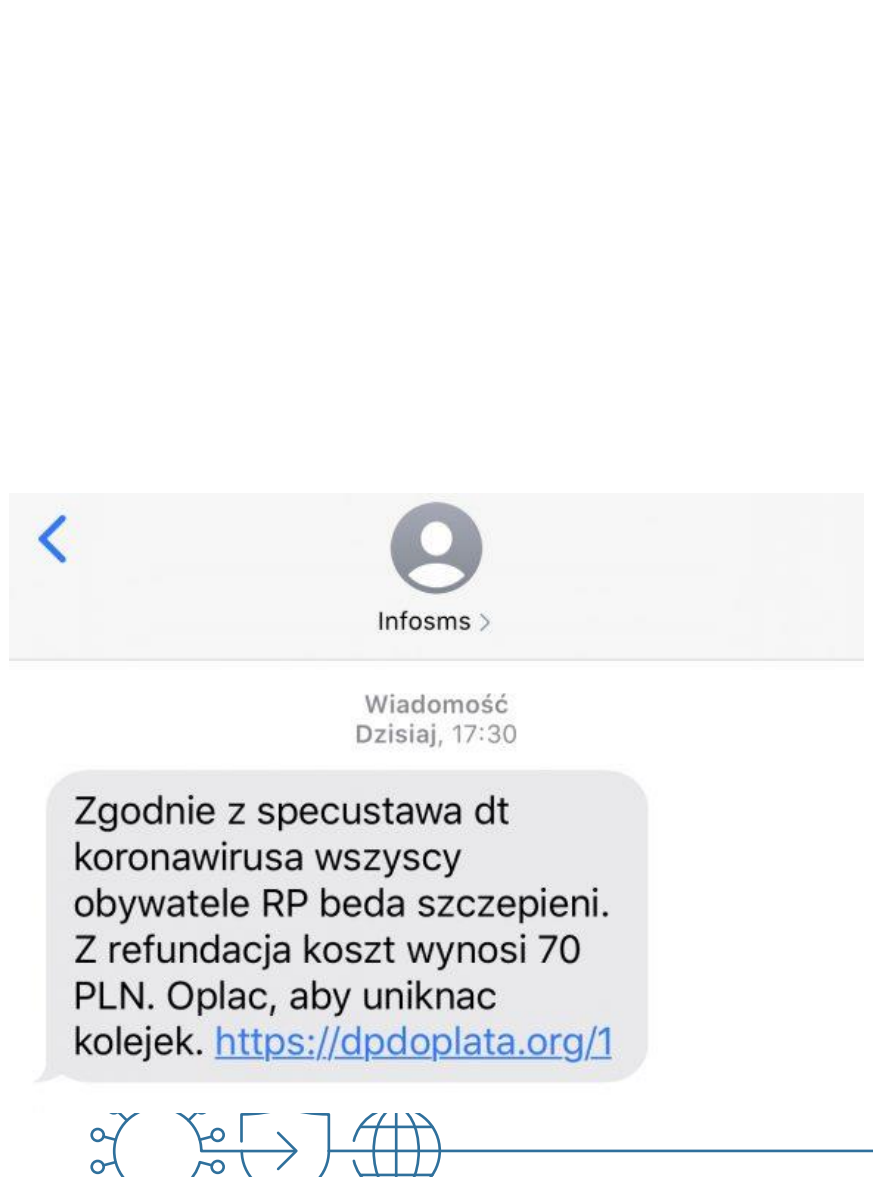
Marcin Pietraszewski 31 sierpnia 2020 | 09:40

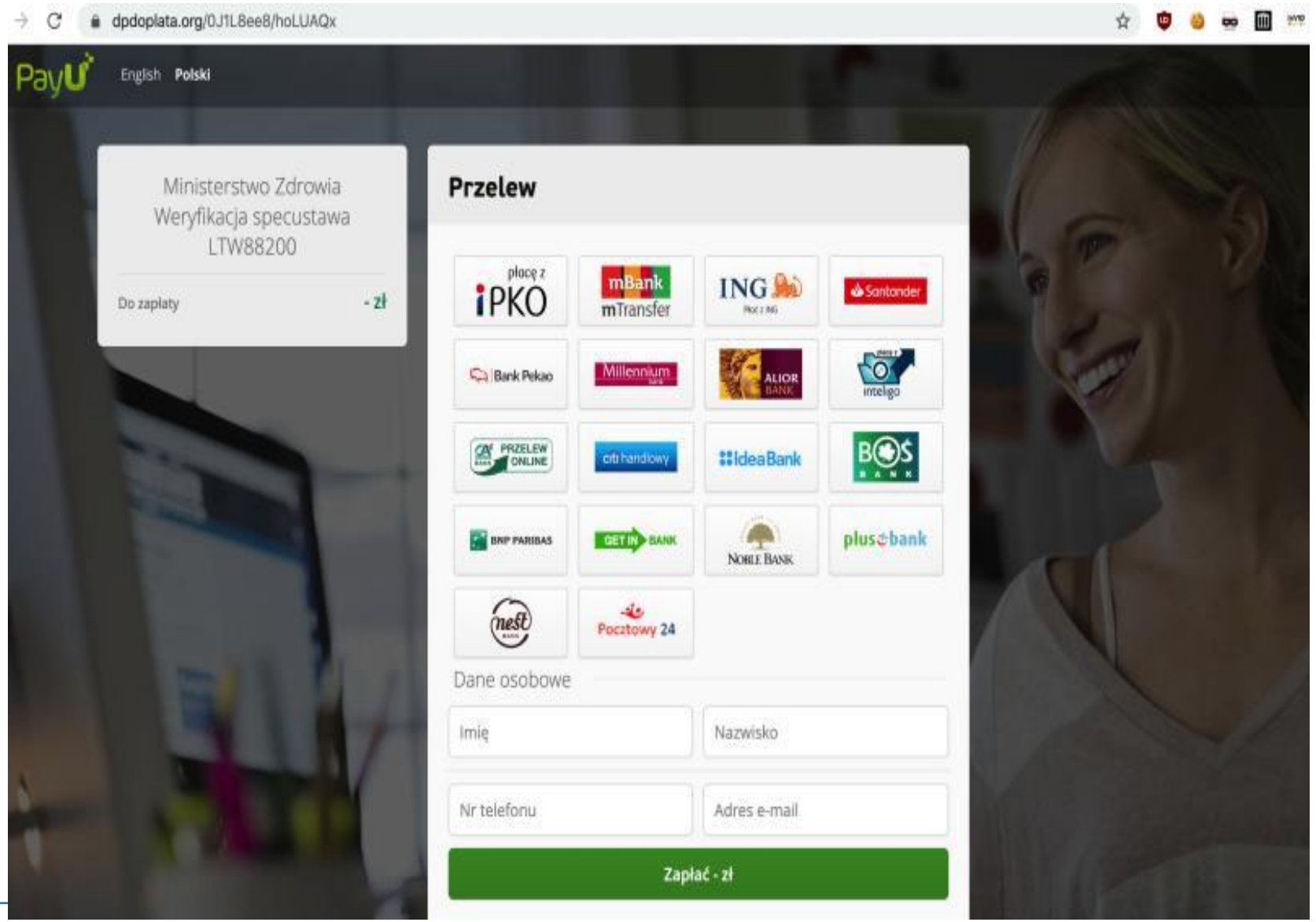
https://katowice.wyborcza.pl/katowice/7,35063,26254257,nastolatkowie-wlamali-sie-do-dziennika-elektronicznego-grozi.html

Przejmowanie danych do logowania do konta Librus (maj 2020)

Ataki z wykorzystaniem fałszywych stron agentów rozliczeniowych i banków




Infosms
Wiadomość
Dzisiaj, 17:30
Zgodnie z specustawa dt koronawirusa wszyscy obywatele RP beda szczepieni. Z refundacja koszt wynosi 70 PLN. Oplac, aby uniknac kolejek. https://dpdoplata.org/1


dpdoplata.org/0J1L8ee8/hoLUAQx
PayU
English Polski
Ministerstwo Zdrowia
Weryfikacja specustawa
LTW88200
Do zaplaty - zł
Przelew
płacę z iPKO
mBank mTransfer
ING
Santander
Bank Pekao
Millennium
ALIOR BANK
inteligo
PRZELEW ONLINE
citi handlowy
IdeaBank
BOS BANK
BNP PARIBAS
GET IN BANK
NOBLE BANK
plus bank
nest BANK
Pocztowy 24
Dane osobowe
Imię
Nazwisko
Nr telefonu
Adres e-mail
Zapłać - zł

Ataki z wykorzystaniem sensacyjnych wiadomości

FAKT24.PL

WYDARZENIA FACET KOBIETA SPORT PIENIĄDZE HOBBY WIDEO NAJNOWSZE GALERIE ZDROWIE

POLSKA ŚWIAT POLITYKA WARSZAWA WROCŁAW POZNAŃ TRÓJMIASTO ŚLĄSK ŁÓDŹ KRAKÓW BIAŁYSTOK RZESZÓW

FAKT24.PL > Wydarzenia > Polska > NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO] 10 MARCA, 11:00

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

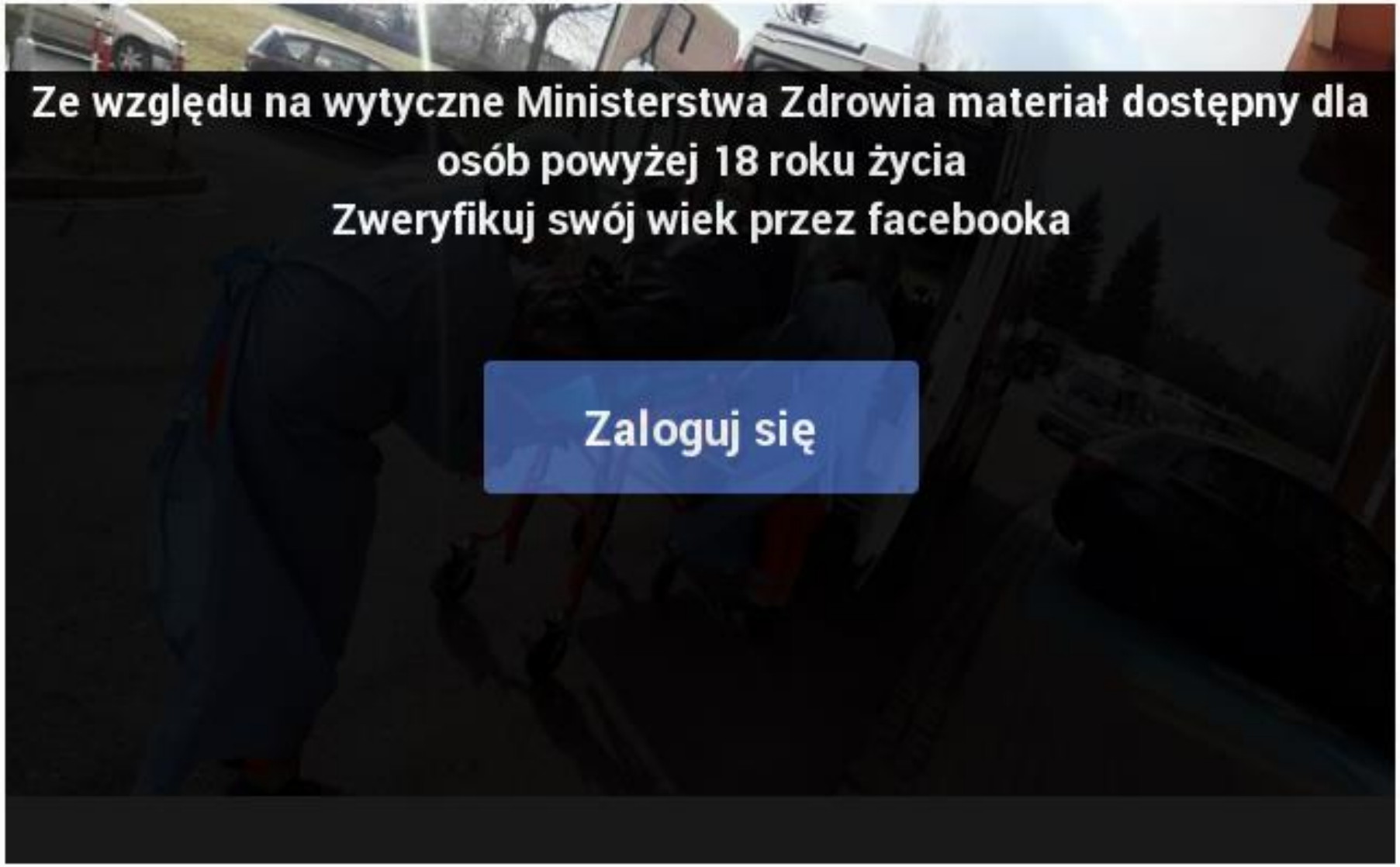
PODZIEL SIĘ

Koronawirus nadal rozprzestrzenia się na świecie. Liczba zachorowań w Polsce wzrosła do 17(prawdopodobnie liczba ta jest mocno zanižona). 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 material 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

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



Czy i jak zablokować dostęp do stron internetowych wyłudzających dane?

POROZUMIENIE z dnia 23 marca 2020 o współpracy w zakresie ochrony użytkowników Internetu przed stronami wyłudzającymi 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

pomiędzy
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 wyłudzeń 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 wyłudzenia ich danych osobowych
Każdy może zgłosić domenę internetową służącą do wyłudzeń 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 emailem 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 zapewniania realizacji celów niniejszego Porozumienia. Po dokonaniu weryfikacji NASK-PIB niezwłocznie wpisuje na Listę Ostrzeżeń domeny, które pozytywnie przeszły weryfikację

W dniu 22.10.2020 – 4 818 nazw domenowych (https://hole.cert.pl/domains/domains.txt).

- 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”
- „pay”
- „kurier”
- „dotpay”
- „paczka”
- „allegro”
- „pocztex”
- „dhl”
- „inpost”
- „platnosc”
- „payu”

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

- „fakt”
- „porwan”
- „gwałt”
- „poszukiwan”
- „news”
- „dziennik”
- „korona”

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”

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.

Dziękuję za uwagę!

Kontakt: a.gryszczynska@uksw.edu.pl