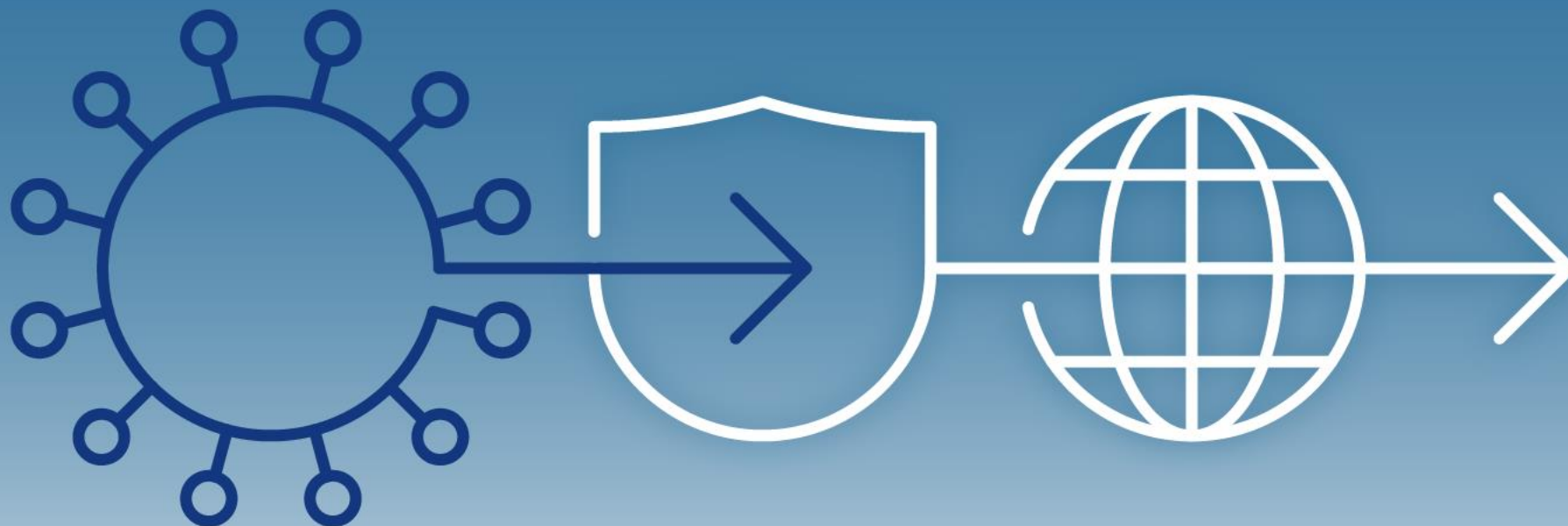


Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

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



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne

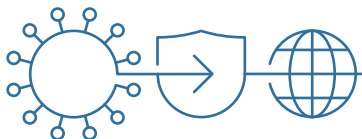


Pandemia COVID -19 znacząco wpłynęła na metody pracy, nauki czy realizacji zadań publicznych.

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.

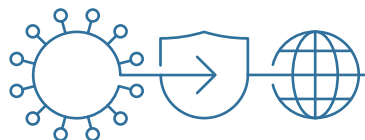
W 2019 r. CERT Polska
zarejestrował 6 484 incydenty.
Oznacza to lawinowy wzrost ilości
incydentów – o **73 %** w
porównaniu z 2018 r.

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

Typ incydentu	Liczba incydentów	%	Liczba incydentów	%
	2018	2018	2019	2019
Obraźliwe i nielegalne treści	431	11,53	812	12,5
<u>Złośliwe oprogramowanie</u>	<u>862</u>	<u>23,05</u>	<u>969</u>	<u>14,9</u>
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
<u>Oszustwa komputerowe</u>	<u>1 878</u>	<u>50,23</u>	<u>4 086</u>	<u>63,0</u>
- 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

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)



EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic

19 June 2020



European Monitoring Centre
for Drugs and Drug Addiction

EU Drug Markets Impact of COVID-19

May 2020

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

1.2 COVID-19 DEMONSTRATES CRIMINAL OPPORTUNISM

While discussions and models have emerged over several decades surrounding the threats posed by a pandemic crisis, the outbreak of COVID-19 has demonstrated the unfortunate impact potential of such crises on our daily lives across the globe. As physical lockdowns became the norm, cybercrime became more popular than before. There is no denying that the arrival of COVID-19 was a crucial factor in any development discussed with respect to 2020. However, COVID-19 in connection to cybercrime needs to be placed within its context. If anything, COVID-19 demonstrated how cybercrime – at its core – remains largely the same but criminals change the narrative. They adapt the specifics of their approach to fit the societal context as a means to enhance their rate of success. This is not new, in many ways this is business as usual. The difference with COVID-19 is that due to the physical restrictions enacted to halt the spread of the virus, with a subsequent increase in working from home and remote access to business resources, many individuals and businesses that may not have been as active online before the crisis became a lucrative target.

Traditional cybercrime activities such as phishing and cyber-enabled scams quickly exploited the societal vulnerability as many citizens and business were looking for information, answers and sources of help during this time. There were even more challenges for both individuals and business as teleworking during the pandemic became the norm. Europol followed all developments closely and shared its findings through frequent *corona strategic reports*².

Spread of disinformation enhances cybercrime opportunities

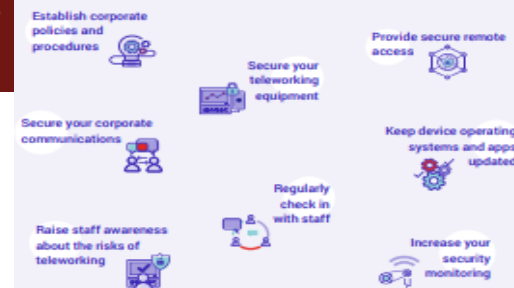
The pandemic also gave rise to disinformation campaigns and activities. Disinformation efforts are often associated with hybrid threats, which are defined as threats combining conventional and unconventional, military and non-military activities which may be used by non-state or state actors to achieve political aims³. A wide range of measures applied in hybrid campaigns include cyber-attacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities. The presence of disinformation became a crucial feature in the overall threat landscape during the crisis. Many Member States reported problems with respect to the spread of disinformation.

Users become vulnerable and receptive to disinformation and fake news due to the paradoxical oversaturation with available information combined with a perceived lack of trustworthy sources of news that reinforce some of the users' preconceived notions and beliefs. Disinformation can also be linked to cybercrime in efforts to make social engineering and phishing attacks more impactful.

Both seasoned cybercriminals and opportunistic individuals spread disinformation to benefit from it in different ways. Significant political motives can drive disinformation to influence elections or referendums affecting entire countries. However, for criminals the

SAFE TELEWORKING

FOR BUSINESSES



FOR EMPLOYEES



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

Ataki związane z edukacją zdalną



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



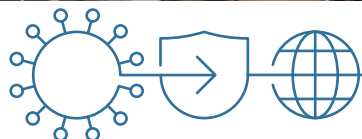
Naukowe Centrum
Prawno-informatyczne

Nastolatki 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,nastolatki-wlamali-sie-do-dziennika-elektronicznego-grozi.html>

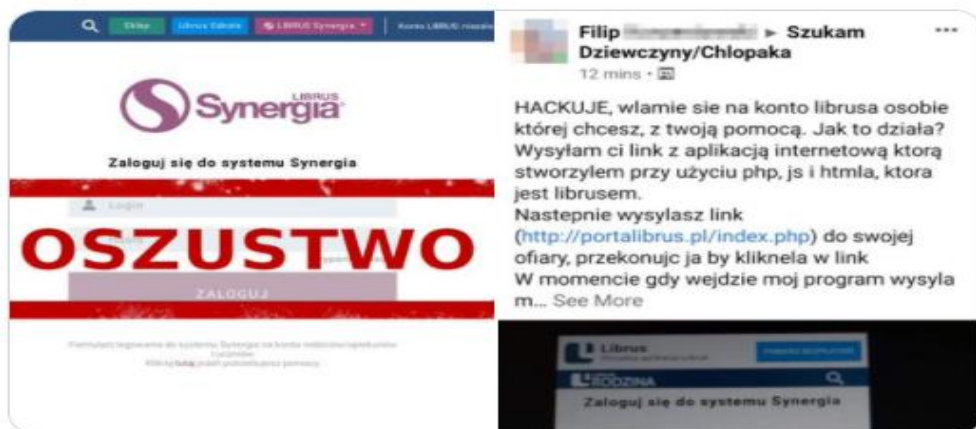


Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia, 22-23 października 2020 r.

Przejmowanie danych do logowania do konta Librus (maj 2020)

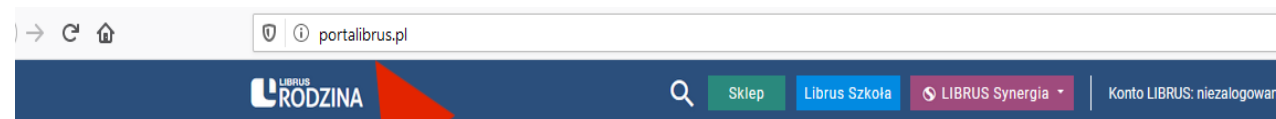


Uwaga nauczyciele i uczniowie! Ostrzegamy przed nowym scenariuszem wyłudzenia danych - tym razem napastnicy wyłudniają dane do portalu Librus. Domena phishingowa to portalibrus[.]pl i jest bardzo podobna do prawdziwej, jedynie brakuje jednej litery "l". Podajcie dalej!



10:17 AM · 5 maj 2020

27 28 użytkowników tweetuje na ten temat



Zaloguj się do systemu Synergia

Login

Hasło

przypomnij hasło

ZALOGUJ

Formularz logowania do systemu Synergia na konta rodziców/opiekunów i uczniów.
Kliknij [tutaj](#) jeżeli potrzebujesz pomocy.



Ataki z wykorzystaniem fałszywych stron agentów rozliczeniowych i banków



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



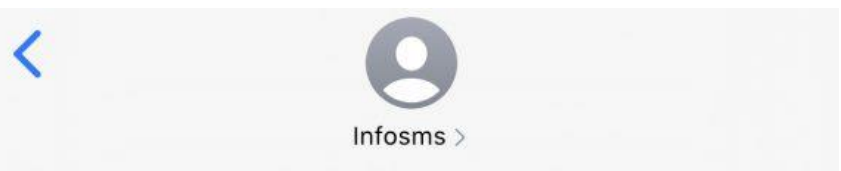
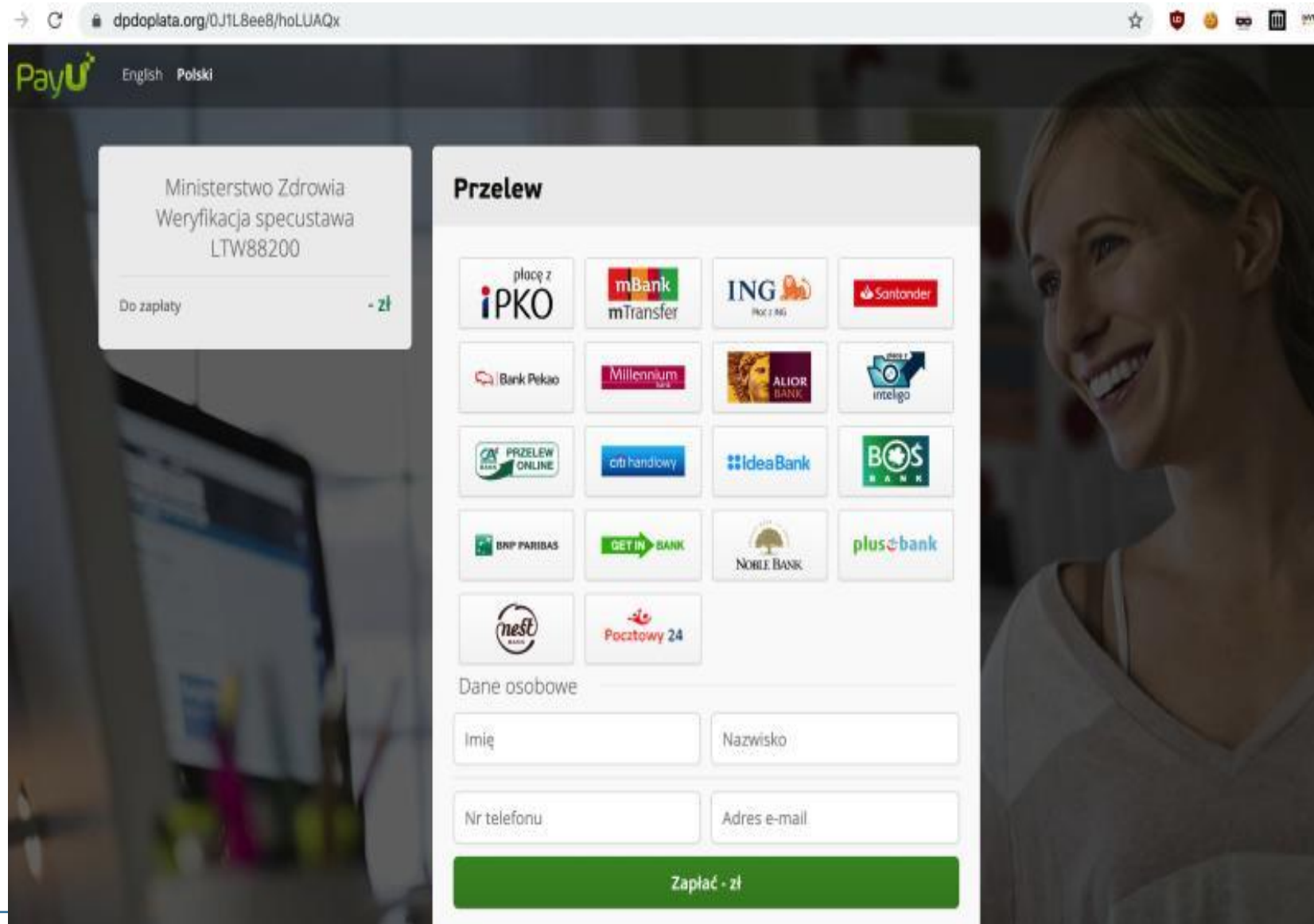
UNIwersytet Kardynała
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE

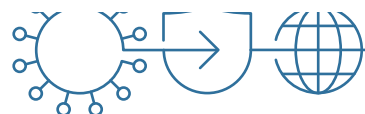


Naukowe Centrum
Prawno-informatyczne



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>



Ataki z wykorzystaniem sensacyjnych wiadomości



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet Kardynała
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne

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

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



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIWERSYTET KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne

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.

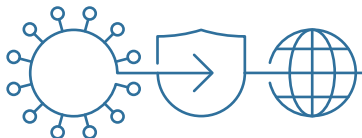
Na Listę Ostrzeżeń wpisywane są domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i w ten sposób doprowadzenie ich do niekorzystnego rozporządzenia środkami finansowymi albo do wyłudzenia ich danych osobowych

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 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

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 wyłudniają 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



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne