CYBERPRZESTĘPCZOŚĆ Z SOCJOTECHNIKĄ

mgr. inż. Marcin Nowak e-mail: mnowak06@gmail.com, tel. 506-078-192
Funkcjonariusz Policji Wydz. dw. z Przestępczością Przeciwko Mieniu
Komendy Miejskiej Policji w Kielcach
Biegły Sądowy z zakresu Cyberprzestępczości i Informatyki Śledczej.
Rzeczoznawca Polskiego Towarzystwa Informatycznego

Cyberprzestępczość

- są to ataki nie mające podtekstu politycznego. Często to ludzie którzy tworzą wirusy, czy nastolatkowie zakłócający działanie sieci komputerowych „dla sportu”. Pojęcie cyberprzestępstwa odnosi się również do działań motywowanych - ekonomicznie, społecznie lub religijnie. Cyberprzestępcy nie ograniczają się jednak tylko do ukrytej sieci, oni używają np. mediów społecznościowych, by szerzyć złośliwe oprogramowanie, terroryści zaś – propagandę. Twitter w drugiej połowie zeszłego roku zawiesił ponad 125 tys. kont należących do terrorystów.

Możliwe ataki Cybernetyczne

- Potencjalne ataki cybernetyczne w cyberprzestrzeni mogą obejmować oprogramowanie przeciwnika (software) lub systemy informacyjne i sprzęt komputerowy (hardware).

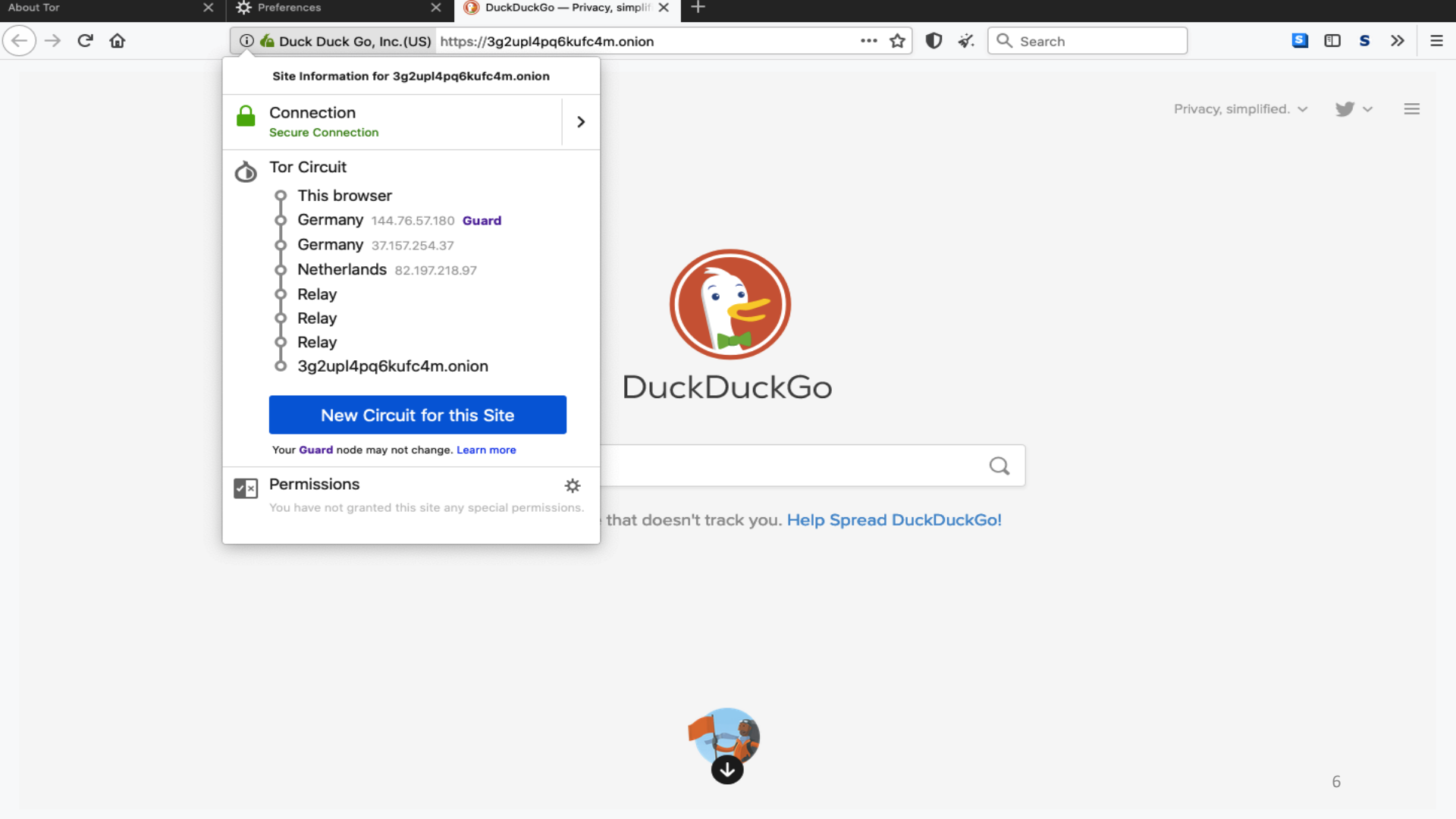
1. Stealing passwords – uzyskanie haseł dostępu do sieci.
2. Sodal engineering – wykorzystanie niekompetencji osób, które mają dostęp do systemu.
3. Bugs and backdoors – korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł.
4. Authentication failures – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji.
5. Protocol failures – wykorzystanie luk w zbiorze reguł sterujących

Powody wykorzystania cyberprzestępczości dla osiągnięcia konkretnych celów:

- Niskie koszty działalności
- Cyberprzestrzeń pozwala dokonywać ataków bez narażania własnego życia
- Zanikanie wszelkich granic
- Możliwości dokonywania nagłych i nieprzewidywalnych akcji
- Całkowita anonimowość
- Minimalne ryzyko wykrycia przygotowanego ataku
- Zamiast uderzać w niewinnych ludzi można sparalizować system wrogiego państwa

Gdzie to wszystko znaleźć??

- Sieć TOR
- Wirtualna **sieć** komputerowa implementująca trasowanie cebulowe drugiej generacji. **Sieć** zapobiega analizie ruchu sieciowego i
- w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów Internetu anonimizując połączenie internetowe maskując adres IP.
- Wymagania!!!!!!! specjalna przeglądarka internetowa i dostęp do mrocznego Darknetu gotowy ☺


About Tor
Preferences
DuckDuckGo — Privacy, simplif
Duck Duck Go, Inc.(US)
https://3g2upl4pq6kufc4m.onion
Search
Site Information for 3g2upl4pq6kufc4m.onion
Connection
Secure Connection
Tor Circuit
This browser
Germany 144.76.57.180 Guard
Germany 37.157.254.37
Netherlands 82.197.218.97
Relay
Relay
Relay
3g2upl4pq6kufc4m.onion
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.
Privacy, simplified.
DuckDuckGo
that doesn't track you. Help Spread DuckDuckGo!

Jakim sposobem przejąć kontrole nad komputerem??? c.d.n

Jakim sposobem przejąć kontrole nad komputerem???

Wirus jest programem komputerowym o niewielkich rozmiarach, zdolnym do rozmnażania się poprzez doczepianie swojego kodu do innych plików:

- **Przygotowywanie botnetów komputerowych**
- **generowanie** dziwnych komunikatów, melodii ,
- **zakłócanie** wyświetlania informacji na ekranie,
- **próby** fizycznego uszkodzenia sprzętu.

Jakim sposobem przejąć kontrole nad komputerem???

- **Phishing**
- **Pharming**
- **Socjotechnika, psychologia**
- **Media społecznościowe, Facebook, Twiter, Linkedln itp.**

Jakim sposobem przejąć kontrole nad komputerem???

Phishing jest to podszywanie się pod strony banków lub innych instytucji. Użytkownik dostaje emailem informację z prośbą o zalogowanie się na danej stronie i sprawdzenie, np. stanu konta, przy czym w tymże emailu podany jest link na stronę spreparowaną. Gdy, logujemy się na niej, oszust otrzymuje nasze hasła i dostaje możliwość dostępu do naszego prawdziwego konta.

Jakim sposobem przejąć kontrole nad komputerem???

From: Kundenservice DHL Logistik [mailto:stegnitz@silometal.sk]
Sent: Wednesday, May 20, 2015 9:56 AM
To:
Subject: Obecny stan przesylki DHL

Sledzenie trasy przesylki DHL

DHL Sendungsverfolgung

Numer przesylki	49177414936436
Produkt / serwis	DHL RETOURE
Status od środa, 20.05.2015 07:55:19	Przesylka jest przygotowywana w początkowym centrum pakowania.
Doreczono do	Przesylka zwrotna do nadawcy

http://www.cetil.com.uy/4if30oexj8y
Kliknij, aby śledzić łącze

Sprawdź informacje od odbiorcy
(ZIP Format)

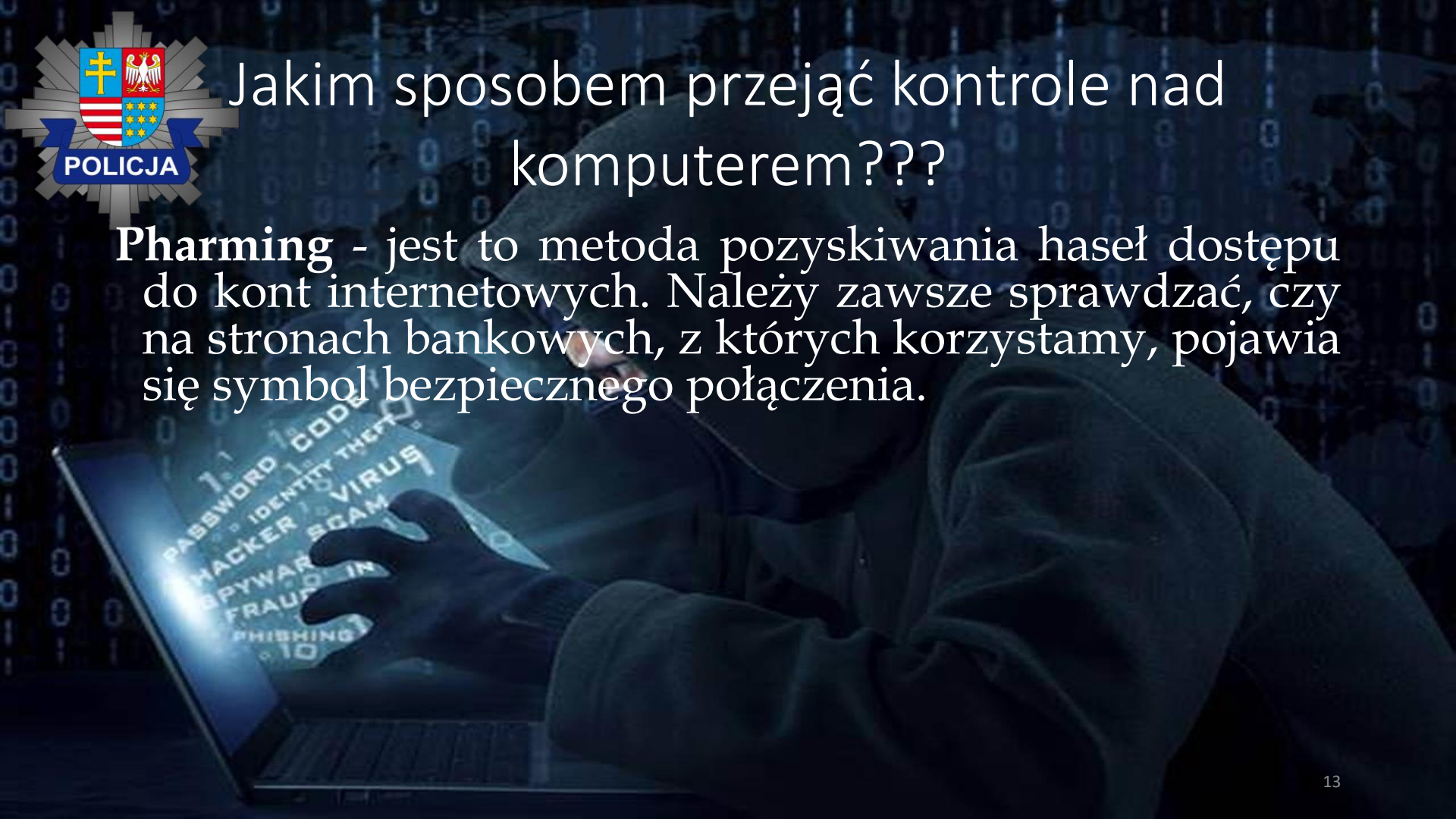
Jakim sposobem przejąć kontrole nad komputerem???

From: <bzwbk@bzwbk.pl>
Date: 14 maja 2008 02:12:43 GMT+02:00
To: <webmaster@kaspersky.pl>
Subject: **Uaktywnij konto BZ WBK 24**
Reply-To: <bzwbk@bzwbk.plz>

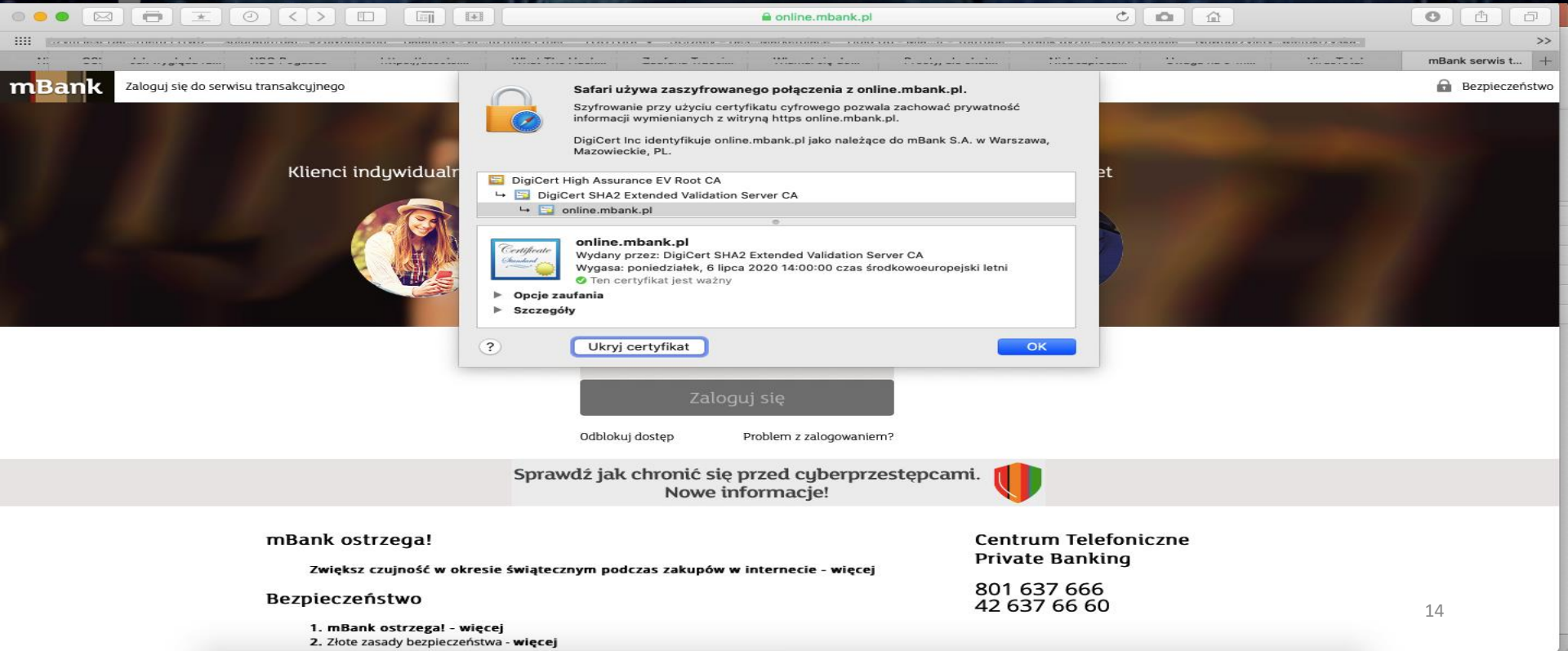
Przykład phishingu

Jakim sposobem przejąć kontrole nad komputerem???

Pharming - jest to metoda pozyskiwania haseł dostępu do kont internetowych. Należy zawsze sprawdzać, czy na stronach bankowych, z których korzystamy, pojawia się symbol bezpiecznego połączenia.



Jakim sposobem przejąć kontrole nad komputerem???

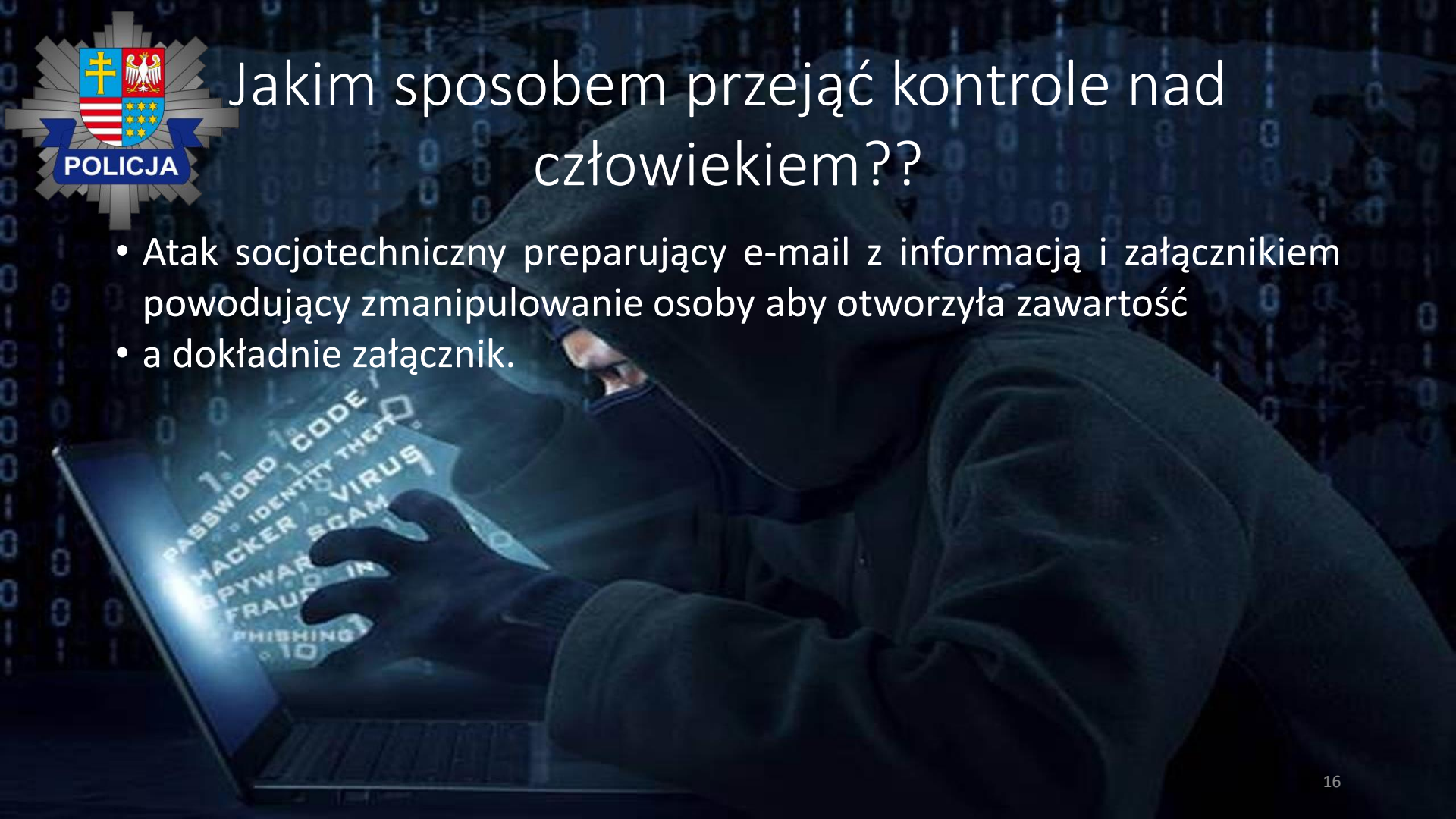


Jakim sposobem przejąć kontrole nad człowiekiem??

- Socjotechnika - to zespół technik służących osiągnięciu określonych celów poprzez manipulację społeczeństwem.
  - www.rnbank.pl
  - www.mbank.pl
  - www.witd.pl
  - www.wltd.pl
- Socjotechniczny Pendrive co w sobie ma i z czym się to wiąże!!!!

Jakim sposobem przejąć kontrole nad człowiekiem??

- Atak socjotechniczny preparujący e-mail z informacją i załącznikiem powodujący zmanipulowanie osoby aby otworzyła zawartość
- a dokładnie załącznik.



Jakim sposobem przejąć kontrole nad człowiekiem??

office@citylawyers.pl Kosz - k...smart-kom.pl 12 listopada 2019 08:16

E-mail: Warunki przed zawarciem umowy.doc

Do: undisclosed-recipients:;

Zwrot podpisany i ostemplowany.

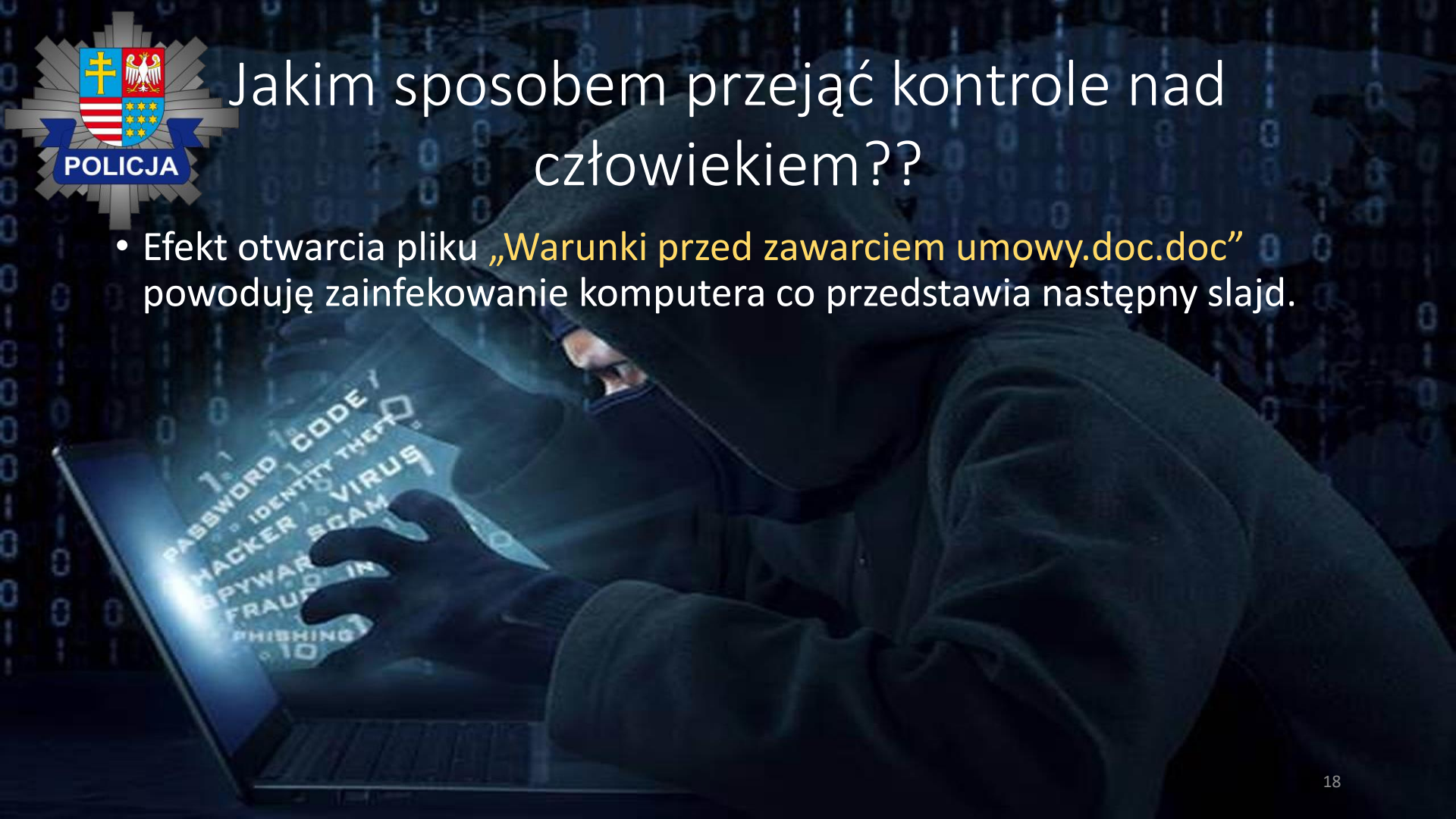
Z góry dziękuję,
Dariusz P.

Wysłane ze smartfona Samsung Galaxy.

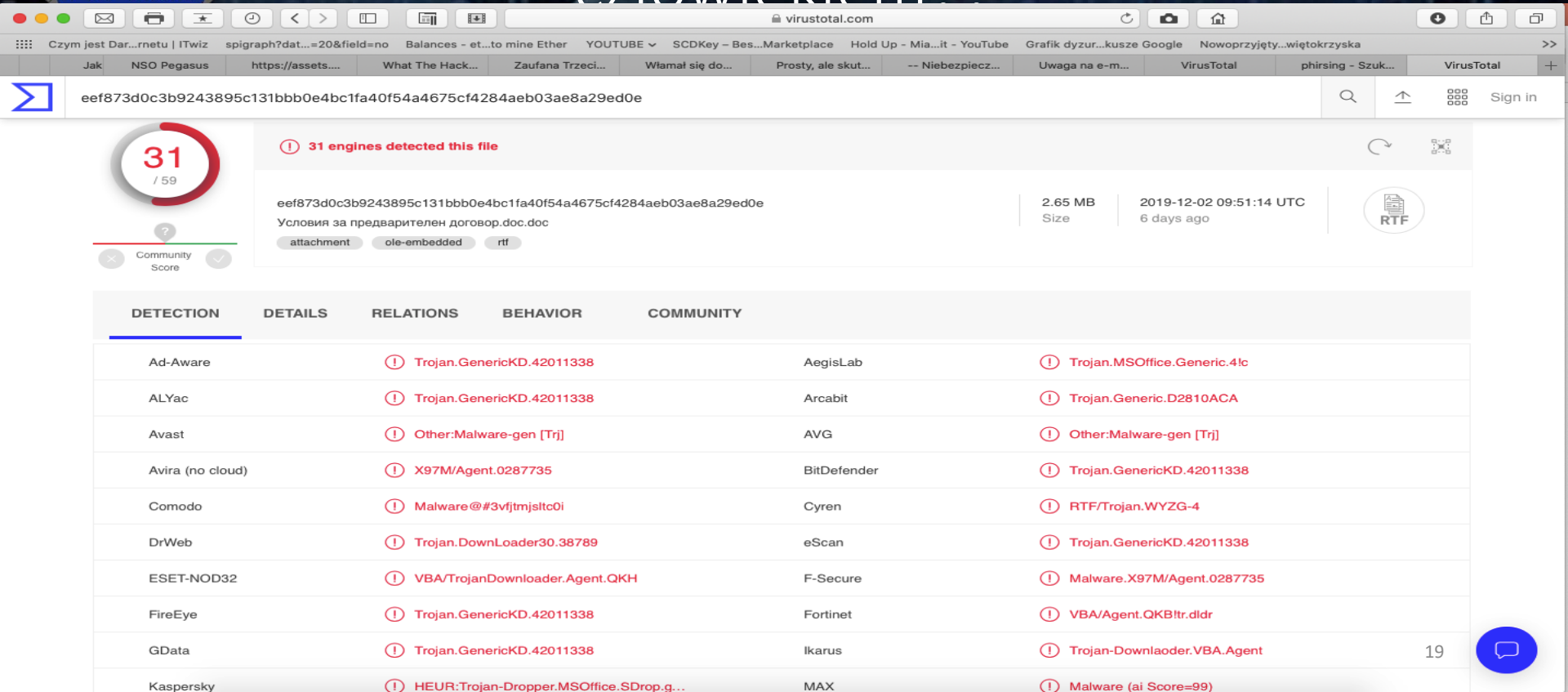
Warunki przed zawarc...oc.doc

Jakim sposobem przejąć kontrole nad człowiekiem??

- Efekt otwarcia pliku „Warunki przed zawarciem umowy.doc.doc” powoduję zainfekowanie komputera co przedstawia następny slajd.

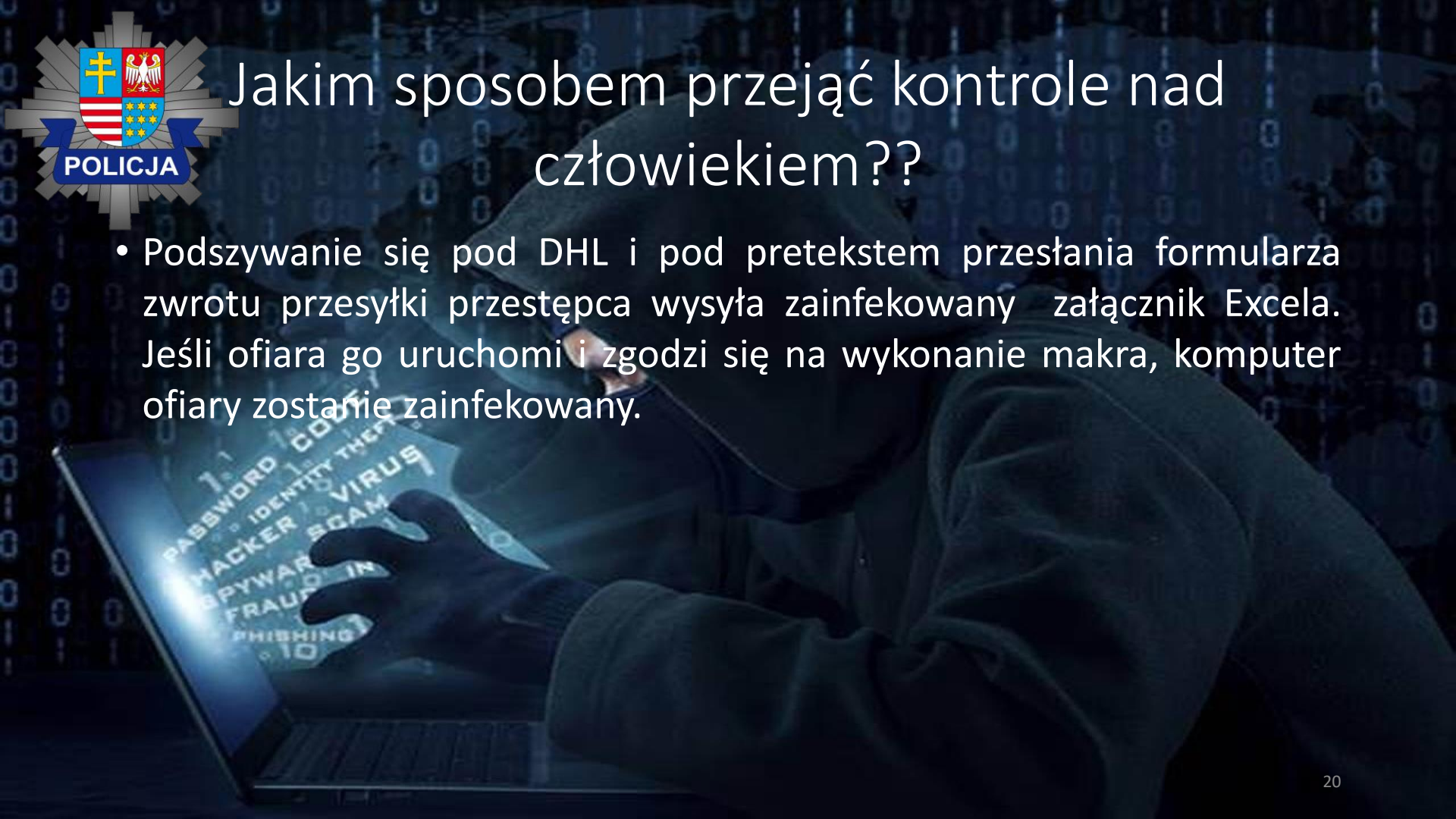


Jakim sposobem przejąć kontrole nad człowiekiem??



Jakim sposobem przejąć kontrole nad człowiekiem??

- Podszywanie się pod DHL i pod pretekstem przesłania formularza zwrotu przesyłki przestępca wysyła zainfekowany załącznik Excela. Jeśli ofiara go uruchomi i zgodzi się na wykonanie makra, komputer ofiary zostanie zainfekowany.



Jakim sposobem przejąć kontrole nad człowiekiem??

Od: DHL Parcel <pl.no.reply.j@dhl.com>
Temat: Zwroty DHL
Data: 18 listopada 2019 11:38:36 CET
Odpowiedź-do: DHL Parcel <pl.no.reply.j@dhl.com>

Zwroty DHL

Szanowni Państwo,

Uprzejmie informujemy, że zlecenie na odbiór przesyłki zwrotnej 29857425050 zostało zarejestrowane pod numerem: 7204451298WWW

Odbiór przesyłki nastąpi w dniu 19.11.2019, w planowanych godzinach od 10:00 do 14:00.

Prosimy o wydrukowanie załączonego listu przewozowego.
Wydrukowanie listu przewozowego jest konieczne żeby nadać paczkę.

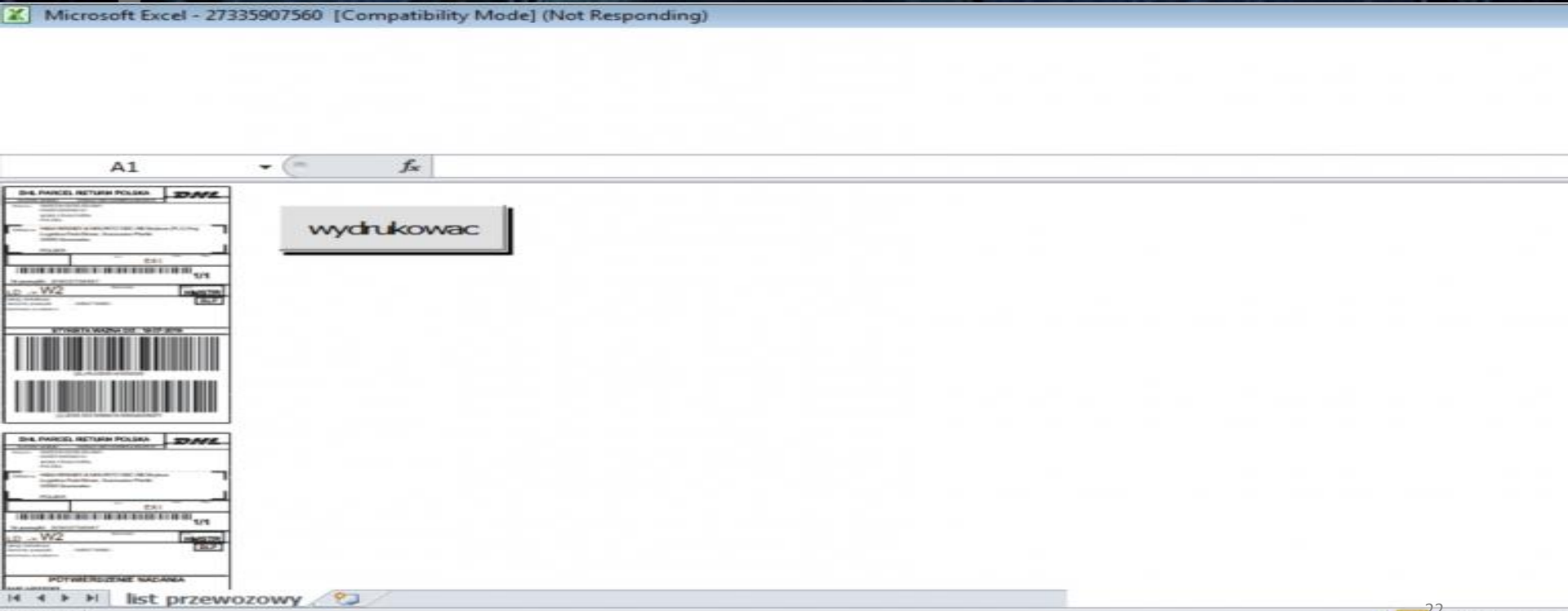
Aktualny status zlecenia mogą Państwo śledzić na stronie: DHL śledzenie przesyłki

Pozdrawiamy,
DHL Parcel
www.dhlparcel.com.pl

UWAGA: Wiadomość ta została wygenerowana automatycznie. Prosimy nie odpowiadać funkcja *Reply/Odpowiedz*

Administratorem Twoich danych adresowych oraz adresu email, które uzyskaliśmy od nadawcy przesyłki jest DHL Parcel Polska sp. z o.o. z siedzibą w Warszawie przy ulicy Osmańskiej 2 (02-823 Warszawa), dalej "DHL". DHL będzie korzystał z Twoich danych w celu dostarczenia przesyłki i badania jakości usług. Masz prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do wniesienia sprzeciwu oraz prawo wniesienia skargi do organu nadzoru Żeby dowiedzieć się więcej kliknij TUTAJ.

Jakim sposobem przejąć kontrole nad człowiekiem??



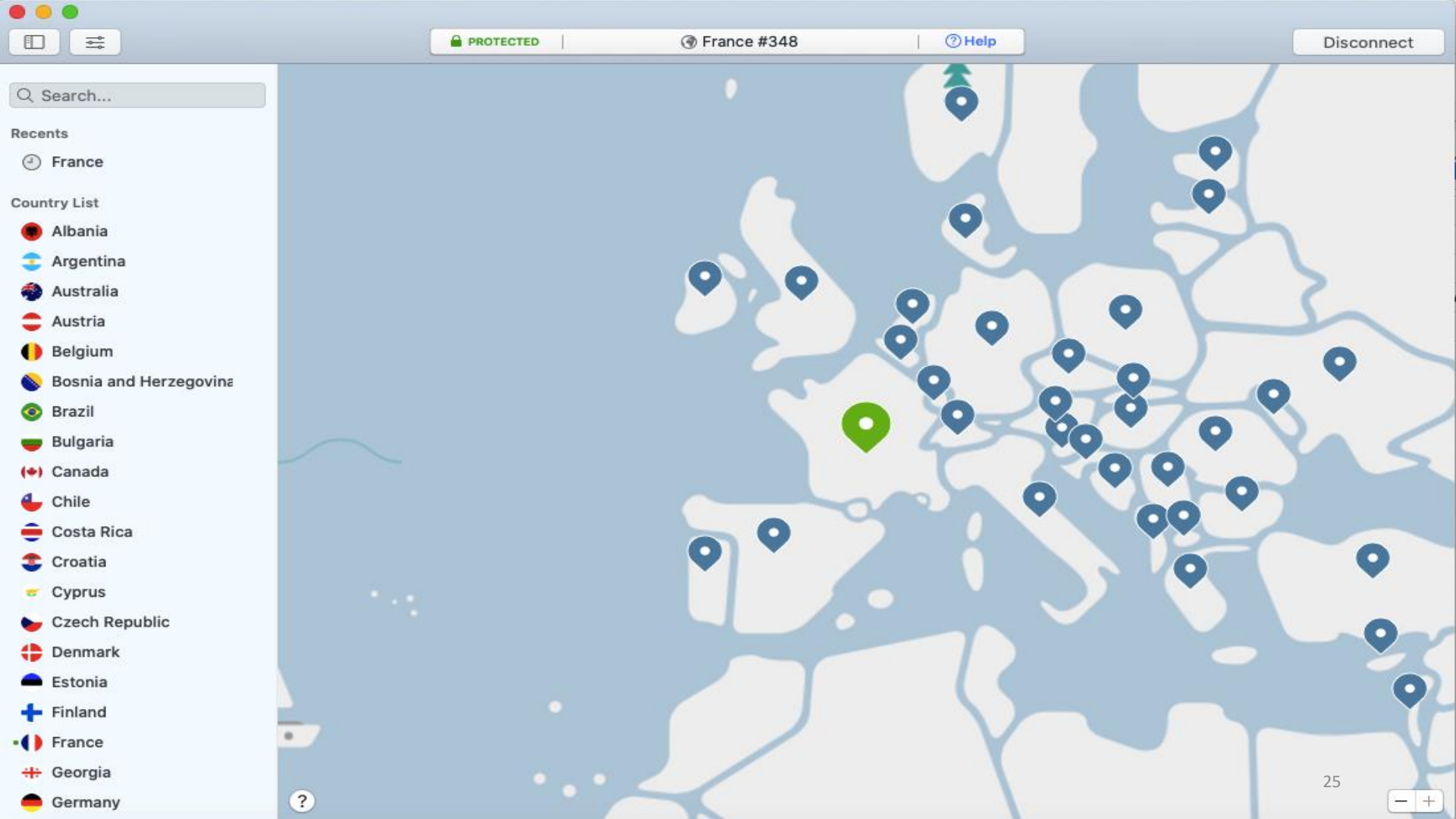
Jak nie dać się zhakować??

- Szkolenie, szkolenie i jeszcze raz szkolenie pracowników poszerzając ich horyzonty wiedzy podstaw informatycznych
- Poprawnie **zabezpieczyć komputer i smartfona**, aby nie zostały one zhackowane przez cyberprzestępców
- **Nie paść ofiarą popularnych w Polsce oszustw internetowych, scamów i przekrętów**
- **Chronić swoją prywatność** w trakcie korzystania

Jak nie dać się zhakować??

- **Zabezpieczyć swoje dane i komunikację**, aby nie zostały one przez nikogo przechwycone

Aplikacja wspierająca możliwość szyfrowania bezpiecznego połączenia i dająca możliwość korzystania w „miarę” bezpiecznie z Internetu to NORDVPN – płatna ależ jak ważne spełnia zadanie.


PROTECTED
France #348
Help
Disconnect
Search...
Recents
France
Country List
Albania
Argentina
Australia
Austria
Belgium
Bosnia and Herzegovina
Brazil
Bulgaria
Canada
Chile
Costa Rica
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
25

I na zakończenie!!
jak nie dać ukraść sobie pieniędzy z karty kredytowej

Dziękuję za uwagę z bezpiecznym Pozdrowieniem ☺