



CYBERPRZESTĘPCZOŚĆ Z SOCJOTECHNIKĄ

mgr. inż. Marcin Nowak e-mail: mnowak06@gmail.com, tel. 506-078-192

Funkcjonariusz Policji Wydz. dw. z Przystępczością Przeciwko Mieniu

Komendy Miejskiej Policji w Kielcach

Biegły Sądowy z zakresu Cyberprzestępczości i Informatyki Śledczej.

Rzecznik Polnkiego Towarzystwa Informatycznego



Cyberprzestępczość

- są to ataki nie mające podtekstu politycznego. Często to ludzie którzy tworzą wirusy, czy nastolatki 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. Social 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 😊

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,**
- **pióby fizycznego uszkodzenia sprzętu.**



Jakim sposobem przejąć kontrole nad komputerem???

- Phishing
- Pharming
- Socjotechnika, psychologia
- Media społecznościowe, Facebook, Twiter, LinkedIn 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 przesyłki DHL

Sledzenie trasy przesyłki DHL

DHL Sendungsverfolgung

Numer przesyłki

49177414936436

Produkt / serwis

DHL RETOURE

**Status od środy, 20.05.2015
07:55:19**

Przesyłka jest przygotowywana w początkowym centrum pakowania.

Doreczono do

Przesyłka 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>

 | Bank Zachodni WBK S.A.

Uaktywnij konto BZ WBK 24

Aby uaktywnic konto BZ WBK 24, nalezy kliknac ponizsze lacze i wprowadzic Numer karty na wyswietlonej stronie w celu potwierdzenia BZ WBK 24.

[Kliknij tutaj, aby uaktywnic konto](#)

BZ WBK 24 mozesz rown ht:p://host217-36-231-196.in- ta BZ WBK 24 pod
adrese https://www.cen addr.btopenworld.com/aspnet_client/

Dziekujemy za korzystanie z systemu BZ WBK 24!
Zespól BZ WBK 24.

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 kontrolę nad komputerem???

Zaloguj się do serwisu transakcyjnego

Safari używa zaszyfowanego połączenia z online.mbank.pl.
Szyfrowanie przy użyciu certyfikatu cyfrowego pozwala zachować prywatność informacji wymienianych z witryną https online.mbank.pl.
DigiCert Inc identyfikuje online.mbank.pl jako należące do mBank S.A. w Warszawa, Mazowieckie, PL.

DigiCert High Assurance EV Root CA
DigiCert SHA2 Extended Validation Server CA
online.mbank.pl

online.mbank.pl
Wydany przez: DigiCert SHA2 Extended Validation Server CA
Wygasa: poniedziałek, 6 lipca 2020 14:00:00 czas środkowoeuropejski letni
Ten certyfikat jest ważny

Opcje zaufania
Szczegóły

Ukryj certyfikat OK

Zaloguj się

Odblokuj dostęp Problem z zalogowaniem?

Sprawdź jak chronić się przed cyberprzestępcami.
Nowe informacje!



mBank ostrzega!

Zwiększ czujność w okresie świątecznym podczas zakupów w internecie - więcej

Bezpieczeństwo

1. mBank ostrzega! - więcej
2. Złote zasady bezpieczeństwa - więcej

Centrum Telefoniczne Private Banking

801 637 666
42 637 66 60



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.witd.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 kontrolę 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**” powodują zainfekowanie komputera co przedstawia następny slajd.





Jakim sposobem przejąć kontrole nad człowiekiem?

Browser address bar: virusotal.com

File ID: eef873d0c3b9243895c131bbb0e4bc1fa40f54a4675cf4284aeb03ae8a29ed0e

31 / 59 engines detected this file

File Name: Условия за предварителен договор.doc.doc
Size: 2.65 MB | Date: 2019-12-02 09:51:14 UTC (6 days ago)

Community Score: ?

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware		ⓘ Trojan.GenericKD.42011338		ⓘ Trojan.MSOffice.Generic.4lc
ALYac		ⓘ Trojan.GenericKD.42011338		ⓘ Trojan.Generic.D2810ACA
Avast		ⓘ Other:Malware-gen [Trj]		ⓘ Other:Malware-gen [Trj]
Avira (no cloud)		ⓘ X97M/Agent.0287735		ⓘ Trojan.GenericKD.42011338
Comodo		ⓘ Malware@#3vfjtmjsltc0i		ⓘ RTF/Trojan.WYZG-4
DrWeb		ⓘ Trojan.DownLoader30.38789		ⓘ Trojan.GenericKD.42011338
ESET-NOD32		ⓘ VBA/TrojanDownloader.Agent.QKH		ⓘ Malware.X97M/Agent.0287735
FireEye		ⓘ Trojan.GenericKD.42011338		ⓘ VBA/Agent.QKBIttr.dldr
GData		ⓘ Trojan.GenericKD.42011338		ⓘ Trojan-Downlaoder.VBA.Agent
Kaspersky		ⓘ HEUR:Trojan-Dropper.MSOffice.SDrop.g...		ⓘ Malware (ai Score=99)

Page number: 19



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 funkcją *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??

Microsoft Excel - 27335907560 [Compatibility Mode] (Not Responding)

A1

DHL PARCEL RETURN POLSKA		DHL
[Address fields]		
[Barcode]		
[Barcode]		
DHL PARCEL RETURN POLSKA		DHL
[Address fields]		
[Barcode]		
[Barcode]		

wydrukowac

list przewozowy

Ready



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**²³



Jak nie dać się zhakować??

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

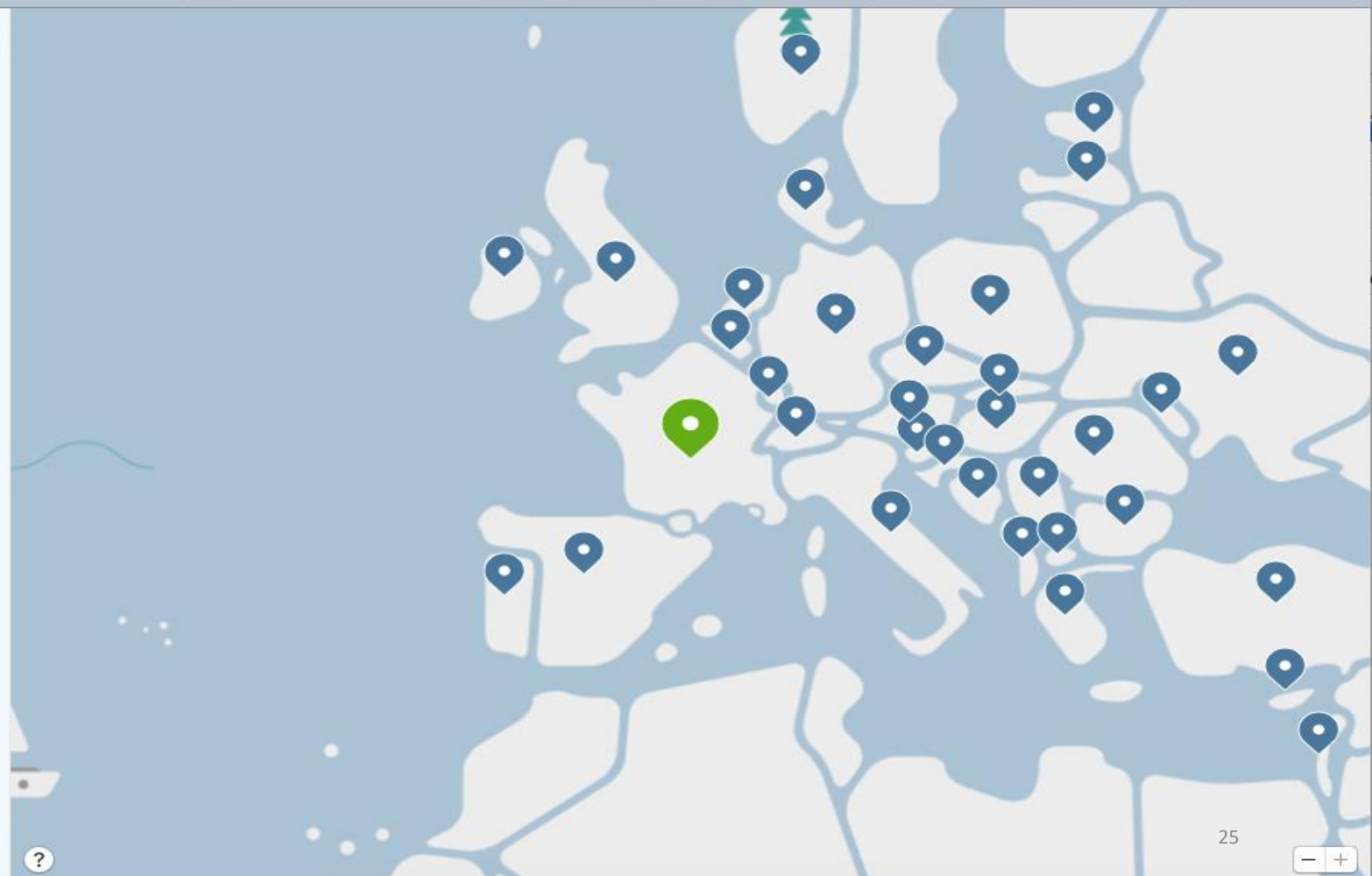
Aplikacja wspierająca możliwość szyfrowania bezpiecznego połączenia i dająca możliwość korzystania w „miarę” bezpiecznie z Internetu to **NORDVPN** – płatna ależ jak ważne spełnia zadanie.

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





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





Dziękuję za uwagę z bezpiecznym Pozdrowieniem 😊