Cyberbezpieczeństwo w działalności laboratorium

SNOWZET

Agenda

- Cyberbezpieczeństwo
- Skutki cyberincydentów
- Cyberzagrożenia
- Cyberzagrożenia w laboratorium
- Jak się bronić
- Gdzie szukać pomocy

CYBERBEZPIECZEŃSTWO

- **64,17%** właścicieli firm potwierdza cyberincydenty – to wzrost o 19 proc. w porównaniu z danymi sprzed roku;
- **23,75%** właścicieli firm potwierdza, że firmowa sieć w ich firmie nie jest prawidłowo zabezpieczona;
- **92%** pracowników firm potwierdza korzystanie ze sprzętu firmowego do celów prywatnych;
- Mniej niż co druga firma korzysta ze wsparcia specjalistów w zakresie cyberbezpieczeństwa.

Źródło: Raport VECTO Systemy Informatyczne
„Cyberbezpieczeństwo w polskich firmach 2021„
https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2021.pdf

Skutki cyberincydentów

Źródło: : Raport PWC Polska
„5. edycja Badania Stanu Bezpieczeństwa Informacji"
https://pwc.pl/badaniebezpieczeństwa

Przyczyny incydentów

Źródło: : Raport PWC Polska

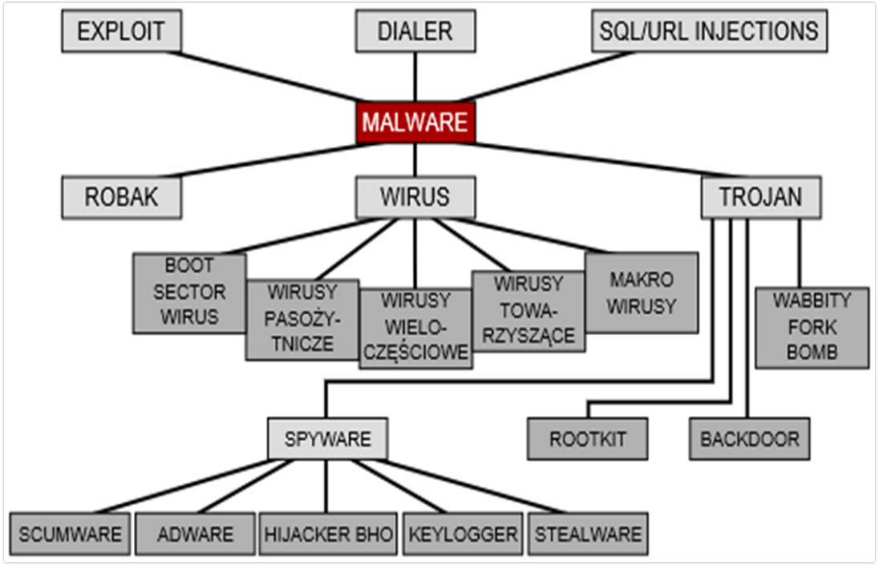
„5. edycja Badania Stanu Bezpieczeństwa Informacji”

https://pwc.pl/badaniebezpieczeństwa

CYBERZAGROŻENIA

Oprogramowanie złośliwe (MALWARE): wirusy, robaki, ransomware, trojany, …

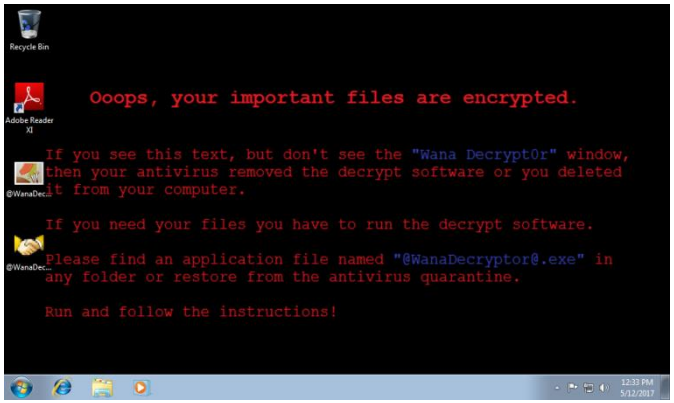
- wykonywanie działań szpiegowskich w postaci uruchamiania skanera klawiatury, wykonywania zdjęć wbudowanym aparatem, nagrywania filmów wbudowaną kamerą, …
- wykradanie kodów autoryzujących transakcje elektroniczne, a w szczególności kodów zatwierdzeń operacji bankowych,
- wysyłanie nieautoryzowanych wiadomości SMS na numery premium i generowanie w ten sposób wysokich kosztów abonamentu,
- zaszyfrowanie danych zawartych w pamięci telefonu (w skutek działania ransomware),
- działalność szpiegowska (dostęp do kontaktów, zdjęć, danych, filmów, lokalizacji, wiadomości e-mail, SMS, itp.)



http://pl.wikipedia.org/wiki/Plik:Malwaregraph.png

CYBERZAGROŻENIA

RANSOMWARE



WANNACRY

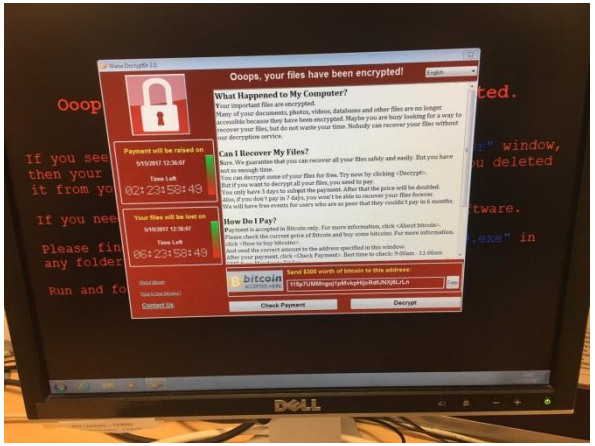
https://www.cert.pl/news/single/wannacry-ransomware/

Instrukcja wylaczenia protokolu SMBv1: https://sekurak.pl/wannacrypt-wana-decrypt0r-2-0-wanacry-jak-sie-chronic/

Link do pobrania latki jest dostepny w biuletynie MS17-010 (na dole strony nalezy wybrac swoj system operacyjny):

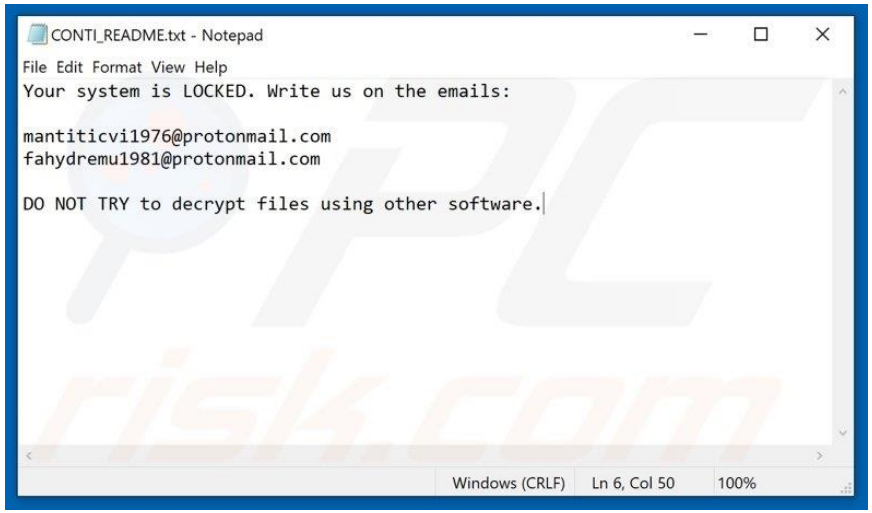
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

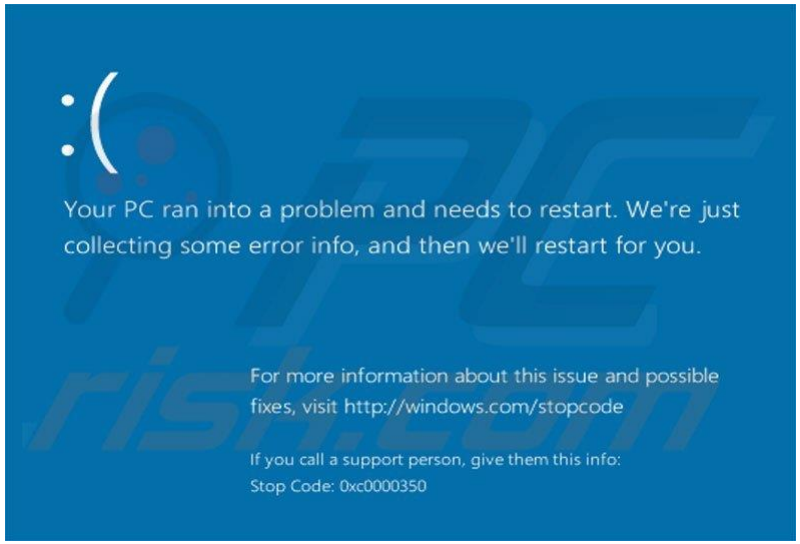
Oprogramowanie szantażujące – zbitka angielskich słów ransom – okup i software – oprogramowanie. Złośliwy kod infekujący komputery jest rozsyłany przez cyberprzestępców za pomocą specjalnie przygotowanych załączników do e-maili lub stron, oferujących fałszywe aktualizacje popularnych programów. W wyniku ataku typu ransomware zaszyfrowany zostaje twardy dysk komputera, na który został ściągnięty kod, oraz inne komputery w tej samej sieci. Za ich odblokowanie cyberprzestępcy żądają okupu, najczęściej w bitcoinach.

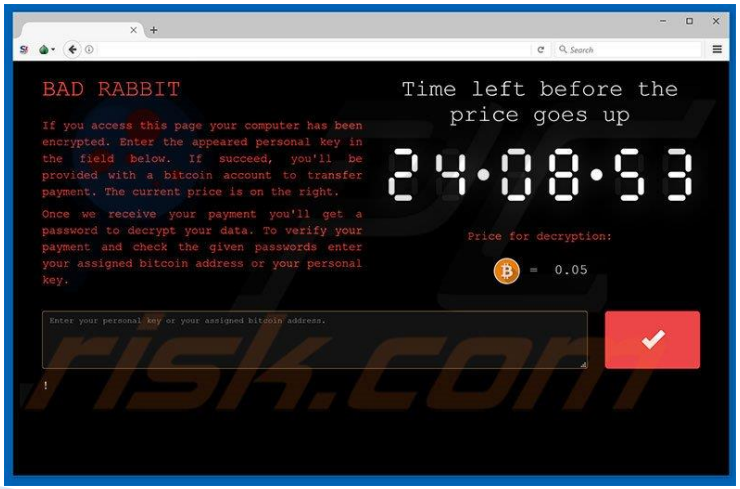


CYBERZAGROŻENIA

RANSOMWARE





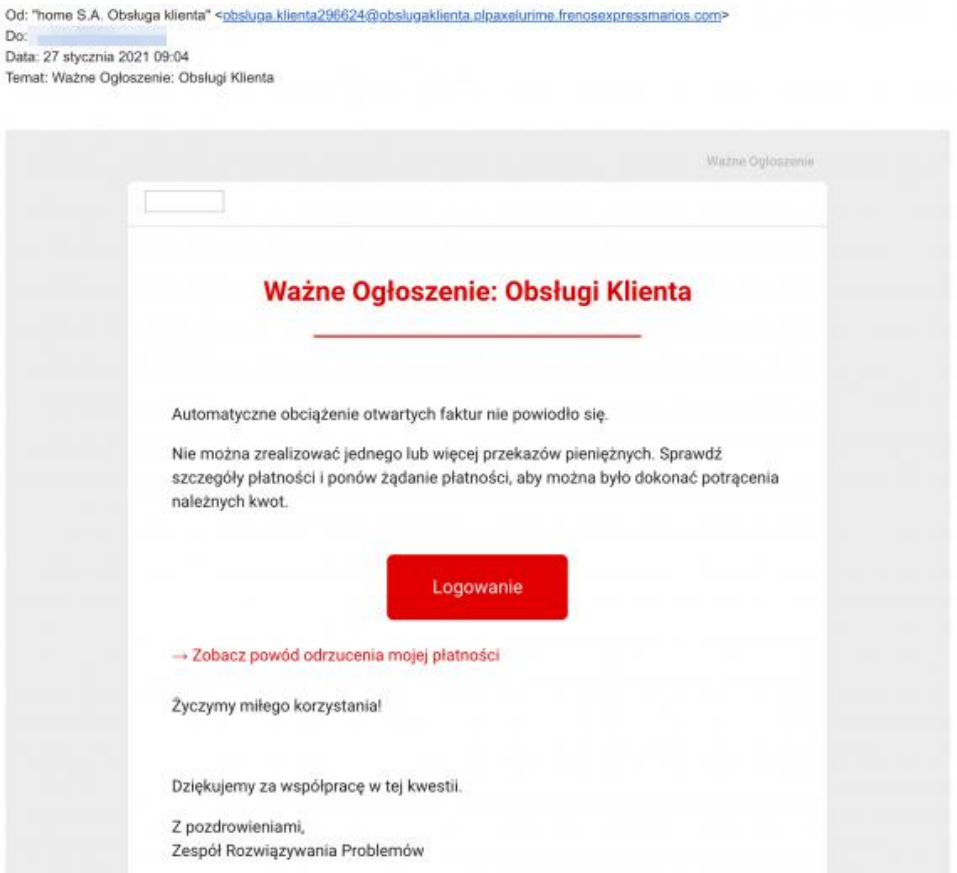


Źródło: : https://www.pcrisk.pl

CYBERZAGROŻENIA

PHISING *z ang. password harvesting fishing czyli „łowienie haseł”*

Wyłudzanie poufnych danych.
Osoby, które chcą pozyskać sekretne informacje podszywają się pod instytucje godne zaufania i proszą o ich potwierdzanie lub aktualizowanie


Od: "home S.A. Obsługa klienta" <obsługa.klienta296624@obslugaklienta.plpaxelurime.frenosexpressmarios.com>
Do:
Data: 27 stycznia 2021 09:04
Temat: Ważne Ogłoszenie: Obsługi Klienta

Ważne Ogłoszenie

Ważne Ogłoszenie: Obsługi Klienta

Automatyczne obciążenie otwartych faktur nie powiodło się.

Nie można zrealizować jednego lub więcej przekazów pieniężnych. Sprawdź szczegóły płatności i ponów żądanie płatności, aby można było dokonać potrącenia należnych kwot.

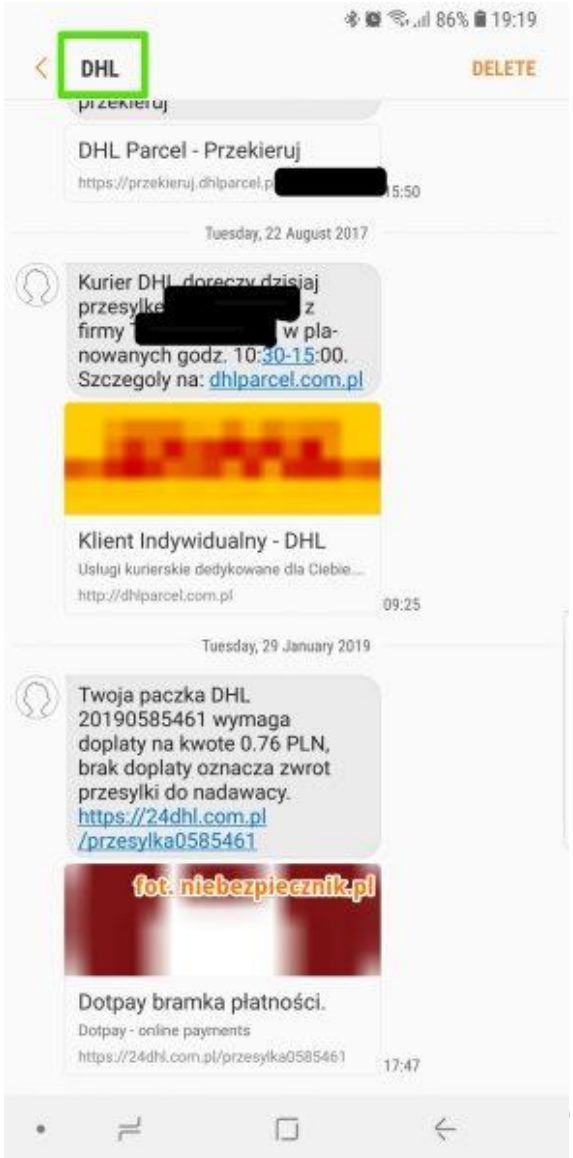
Logowanie

→ Zobacz powód odrzucenia mojej płatności

Życzymy miłego korzystania!

Dziękujemy za współpracę w tej kwestii.

Z pozdrowieniami,
Zespół Rozwiązywania Problemów



CYBERZAGROŻENIA

CYBERZAGROŻENIA

INTERNATIONAL BUSINESS TIMES | World

SEARCH IBTIMES

News | Markets | Life & Style | Topics | TV | Tools

World | UK | Economy | Companies | Tech | Science | Law | Real Estate | Sports | Slideshows | Picture This

Russia's Spy Plot: Bugged USB Drives Found in G20 Leaders' Welcome Packs

Kremlin reportedly attempted to spy on world leaders and advisers with 'Trojan horse' welcome pack

By UMBERTO BACCHI : Subscribe to Umberto's RSS feed | October 29, 2013 1:32 PM GMT

Dane & Metadane

- ✓ Podaj swoje nazwisko i dwa dodatkowe dane o sobie (wiek&miejsce zamieszkania)

CYBERZAGROŻENIA

Dane & Metadane

```
[+]  List of users found:
---------------------------
Preferred Customer, Łucja M. [redacted] Monika [redacted] ks3797, OI, ks0169, ks1477, ks0169,
supervisor, Kancelaria Sejmu

[+]  List of software found:
---------------------------
Microsoft Office Word,                  Microsoft Word 9.0
Acrobat Distiller 5.0.5 (Windows),      PScript5.dll Version 5.2
Acrobat Distiller 6.0 (Windows),        PScript5.dll Version 5.2.2,
ADOBEPS4.DRV Version 4.50,              EPSON Scan
Acrobat Distiller 4.05 for Windows,     Microsoft Word 8.0

[+]  List of paths and servers found:
---------------------------
Normal.dotm
'C:\Documents and Settings\ks2454\Dane aplikacji\Microsoft\Word\Zapisywanie informacji
potrzebnych do odtworzenia Dokument1.asd'
'C:\5kad_strona_www\temp\test.doc'
'C:\Documents and Settings\ks2454\Dane aplikacji\Microsoft\Word\Zapisywanie informacji
Potrzebnych do odtworzenia test.asd'
Normal
```

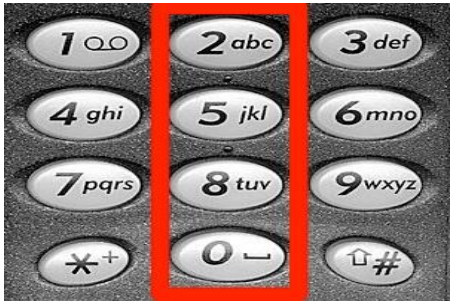
```
ISO Speed Ratings       56
Exif Version    2.20
Date/Time Original      2010:01:05 17:02:39
Date/Time Digitized     2010:01:05 17:02:39
Components Configuration        YCbCr
Shutter Speed Value     1/134 sec
Aperture Value  F 2,8
Brightness Value        1493/256
Exposure Bias Value     0
Metering Mode   Center weighted average
Light source    21
Flash   Flash did not fire, Auto
FlashPix Version        1.00
Color Space     sRGB
Exif Image Width        2592 pixels
Exif Image Height       1936 pixels
Exposure Index  56
Sensing Method  One-chip color area sensor
File Source     Digital Still Camera (DSC)
Scene Type      Directly photographed image
Custom Rendered 1
Exposure Mode   Auto exposure
White balance mode      Auto white balance
Scene Capture Type      Standard
Gain Control    Low gain up
Contrast        None
Saturation      None
Sharpness       None
Image Unique ID
Compression     JPEG (old-style)
Thumbnail Offset        2658 bytes
Thumbnail Length        11215 bytes
Thumbnail Data  [11215 bytes of thumbnail data]

Exif Interoperability Makernote:
Interoperability Index  Recommended Exif Interoperability Rules (ExifR98)
Interoperability Version        1.00

GPS Makernote:
GPS Version ID  2 2 0 0
GPS Latitude Ref        N
GPS Latitude    37"46'22
GPS Longitude Ref       W
GPS Longitude   122"30'41
```

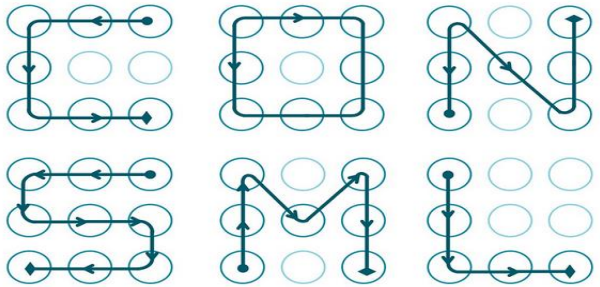
CYBERZAGROŻENIA

Dane Logowania & Hasła

Najpopularniejsze hasła 2020 – lista wg. NordVPN

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha





- **43 imiona: 18 damskich, 25 męskich (6 z „1” na końcu”),**
- **17 różnych „wzorków z klawiatury” takich jak np. zaq12wsx czy qwerty,**
- **16 haseł składających się z samych cyfr,**
- **8 słów „miłosnych” (misiek, kochanie, myszka, misiaczek, niunia, kochamcie, kocham, misiek1),**
- **3 razy występuje nieśmiertelna dupa (dupa, dupadupa, dupa123),**
- **3 razy samo hasło (haslo, haslo1, password),**
- **3 razy to co mamy przed nosem (komputer, komputer1, samsung),**
- **2 hasła patriotyczne (polska, polska1),**
- **1 klub sportowy (barcelona),**
- **plus cztery hasła z kategorii „inne” (lol123, dragon, matrix, master).**

Inne cechy haseł:

- **tylko małe litery: (45.43%),**
- **tylko duże litery: (0.43%),**
- **tylko cyfry: (6.65%),**
- **pojedyncza cyfra na końcu: (10.29%),**
- **dwie cyfry na końcu: (11.06%),**
- **trzy cyfry na końcu: (5.57%).**

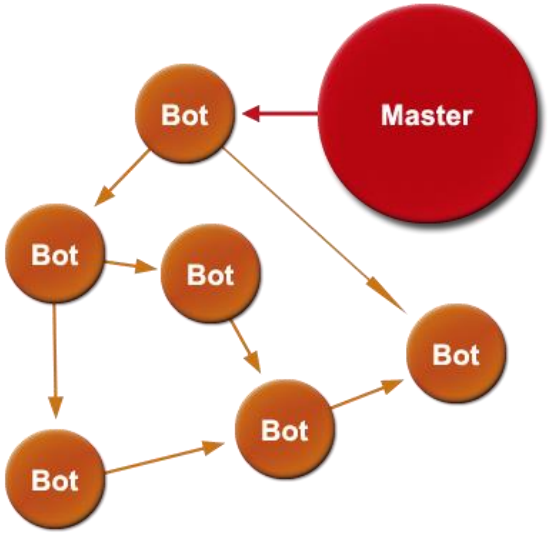
ATAKI UKIERUNKOWANE – APT (ang. Advanced Persistant Threats)

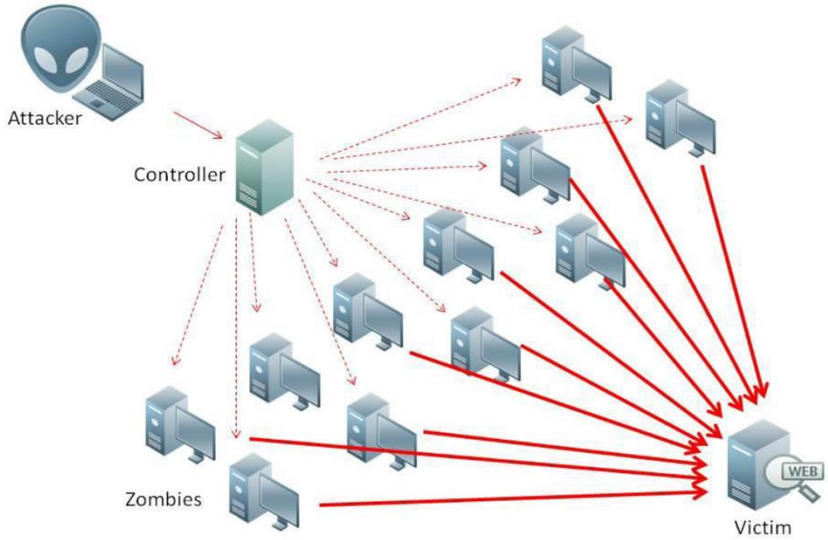
Zaawansowane trwałe zagrożenia. Ataki typu APT ukierunkowane są na konkretne firmy i przeprowadzane do skutku, czyli momentu znalezienia słabego punktu, przez który uda się cyberprzestępcom wniknąć do atakowanego systemu. Wtedy prowadzone są działania mające na celu otwarcie w nim jak największej ilości „furtek". System infiltracji stworzony jest tak, żeby działał jak najdyskretniej, dzięki czemu może funkcjonować w atakowanym systemie nawet wiele miesięcy niezauważony. W tym czasie zbiera i przesyła przestępcom poufne informacje lub trwa w uśpieniu w oczekiwaniu na właściwy moment do rozpoczęcia właściwego ataku.

APT28 Domain	Real Domain
standartnevvs[.]com	Bulgarian Standart News website **(standartnews.com)**
novinitie[.]com, n0vinite[.]com	Bulgarian Sofia News Agency website **(novinite.com)**
qov[.]hu[.]com	Hungarian government domain **(gov.hu)**
q0v[.]pl, mail[.]q0v[.]pl	Polish government domain **(gov.pl)** and mail server domain **(mail.gov.pl)**
poczta.mon[.]q0v[.]pl	Polish Ministry of Defense mail server domain **(poczta.mon.gov.pl)**

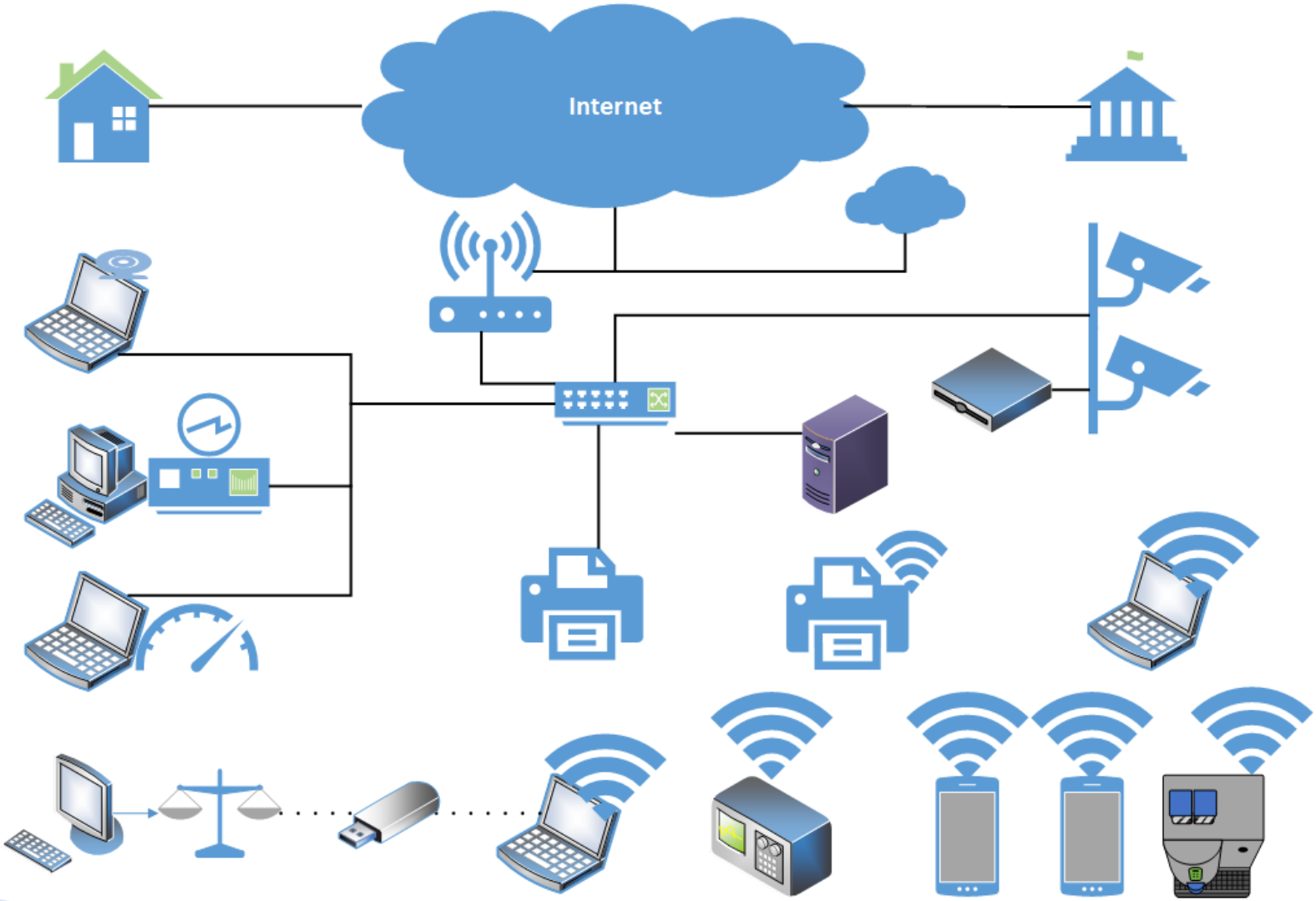
Ataki typu DDoS – odmowa usługi

Zasypanie systemu komputerowego ofiary ogromną liczbą wywołań z komputerów na całym świecie. Do każdego z nich system musi przydzielić pewne zasoby i w końcu ulega zawieszeniu.





Cyberzagrożenia w laboratorium



JAK SIĘ BRONIĆ

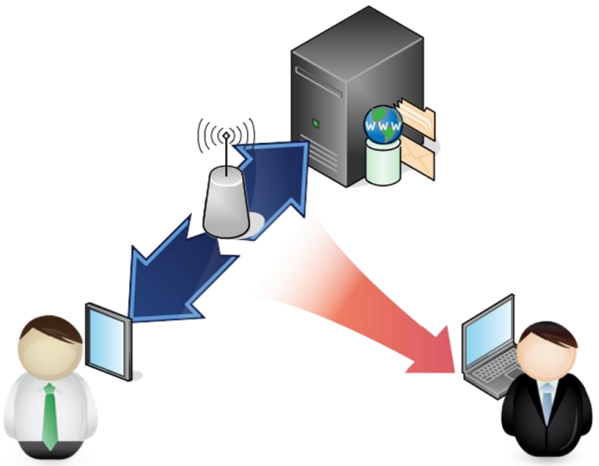
- Edukuj siebie i personel
- Uważaj co wrzucasz do Sieci
- Przygotuj się wcześniej na sytuację, że Twoje dane wyciekną
- Inwestuj w zabezpieczenia
- Monitoruj swoją infrastrukturę teleinformatyczną
- Testuj swoje środowisko teleinformatyczne
- Korzystaj ze wsparcia specjalistów w zakresie cyberbezpieczeństwa

- ZACHOWAJ ZDROWY ROZSĄDEK

JAK SIĘ BRONIĆ

UNIKAJ

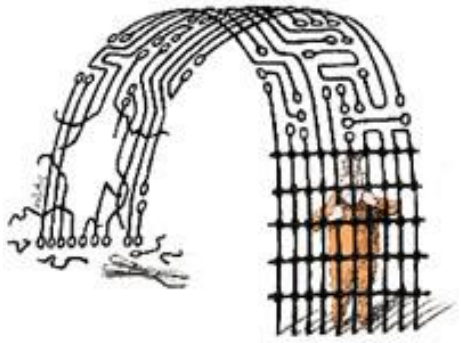
- Korzystania z publicznych sieci Wi-Fi;
- Komunikowania się przez nieszyfrowane łącza;
- Programów pochodzących z nieznanego źródła;
- Pozostawiania sprzętu bez nadzoru;
- Korzystania z niezaufanych urządzeń w celu wymiany wrażliwych danych;
- Posiadania i korzystania ze zbędnych lub nieaktualnych programów i aplikacji;
- Pułapek socjotechnicznych;



JAK SIĘ BRONIĆ

WYKRYWAJ

- **Ingerencję w integralność pobieranych plików;**
- **Poprawność nazw domen i certyfikatów;**
- **Poprawność rozszerzeń plików, które uruchamiasz;**
- **Wiadomości o treści podejrzanej z pozornie zaufanych źródeł;**
- **Urządzenia w Twoim otoczeniu niewiadomego pochodzenia;**
- **Posiadania i korzystania ze zbędnych lub nieaktualnych programów i aplikacji;**
- **Nadmierne zainteresowanie Twoją osobą kierowane drogą elektroniczną z obcych adresów, numerów, profili i instytucji;**
- **Nietypowe zachowanie urządzenia np.:**
  - ***Wyskakujące okienka.***
  - ***Częste zawieszanie się, restart urządzenia.***
  - ***Duże obciążenie CPU, wolno działające urządzenie.***
  - ***Częste crashe systemu bądź aplikacji (możliwy indykator obecności oprogramowania złośliwego).***



JAK SIĘ BRONIĆ

WYKORZYSTUJ

- **Zdrowy rozsądek;**
- **Wyłącznie zaufane, sprawdzone i bezpieczne źródła oprogramowania;**
- **Najnowsze wersje oprogramowania, systemów i aplikacji, aktualizacje przeglądarek internetowych oraz oprogramowania antywirusowego;**
- **Bezpieczny sposób logowania i niestandardowe hasła (blokada ekranu; >4 litery, cyfry, znaki specjalne);**
- **Narzędzia do komunikacji szyfrowanej np.: Signal, WhatsApp, Viber, PGP, Kleopatra.**

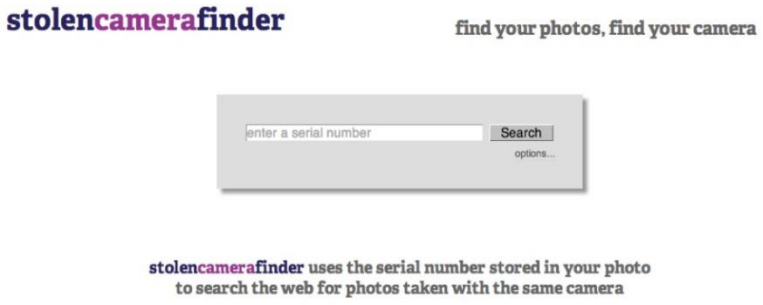
JAK SIĘ BRONIĆ

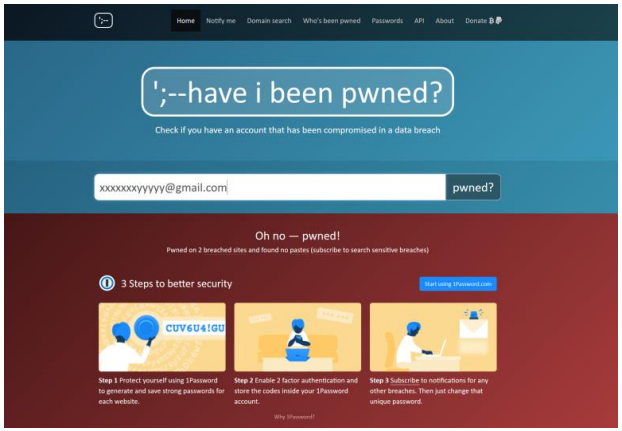
REAGUJ

(w przypadku zidentyfikowania wycieku danych, podejrzenia próby ataku lub inwigilacji)

- **W przypadku incydentu związanego z naruszeniem ochrony danych osobowych** „chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych” (art. 33 ust. 1 RODO)
  Nie później niż 72 godziny po stwierdzeniu naruszenia
  Powiadom Urząd Ochrony Danych Osobowych;
- **Powiadom Policję;**
- **Zgłoś incydent do CERT Polska (CESIRT NASK) https://incydent.cert.pl**
  Nie później niż 24 godziny od momentu wykrycia – podmiot publiczny
- **Zgłoś incydent do CERT GOV (CESIRT GOV) incydent@csirt.gov.pl**
  Nie później niż 24 godziny od momentu wykrycia – podmiot publiczny

JAK SIĘ BRONIĆ





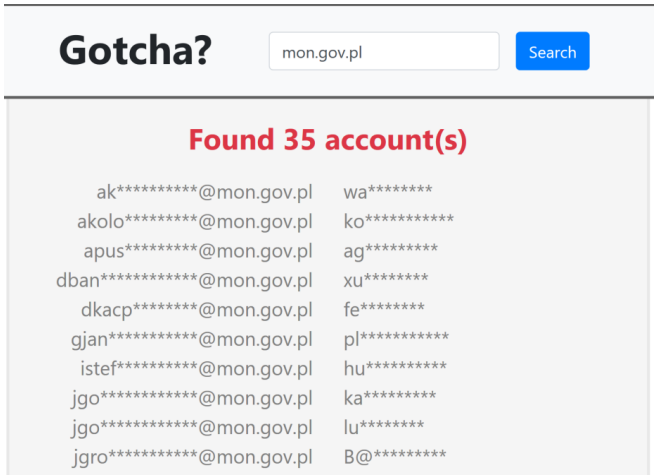
https://www.stolencamerafinder.com

https://weleakinfo.to

https://gotcha.pw

https://haveibeenpwned.com/

https://dehashed.com



- **Alert BIK**
  https://www.bik.pl/klienci-indywidualni/alerty-bik
- **e-sąd Lublin – powiadomienia mailowe**
  https://www.e-sad.gov.pl

Dziękuję za uwagę

snowzet@outlook.com