

# Cyberbezpieczeństwo w pracy oraz w życiu prywatnym

# EURid?

- EURid jest rejestrem europejskich domen internetowych .eu oraz .eu (wersja w cyrylicy). Mamy zarejestrowanych ponad 3,6 mln
- Nasz rejestr działa na rzecz zwiększania bezpieczeństwa w całym środowisku internetowym, tak aby Internet pozostawał bezpiecznym miejscem dla wszystkich jego użytkowników.
- Część naszej dzisiejszej prezentacji korzysta z materiałów przygotowanych przez naszego Security Manager, pana Dirka Jumpertza.



# Cele i zakres webinaru

- Jakie są najczęściej spotykane rodzaje ataków
- Typowe scenariusze oszustw, wyłudzeń i kradzieży wrażliwych danych
- Jak bezpiecznie korzystać z Internetu (dobre praktyki, najskuteczniejsze sposoby prewencji i ochrony przed zagrożeniami w sieci).

# Najczęstsze rodzaje ataków



# Użyteczne raporty



➤ Na świecie:

- [CERT Top Stories](#)
- [Check Point, 2018 Security Report](#)
- [Verizon, 2018 Data Breach Investigations Report](#)
- [Akamai, State of the Internet](#)
- [Trendmicro](#)



➤ W Polce:

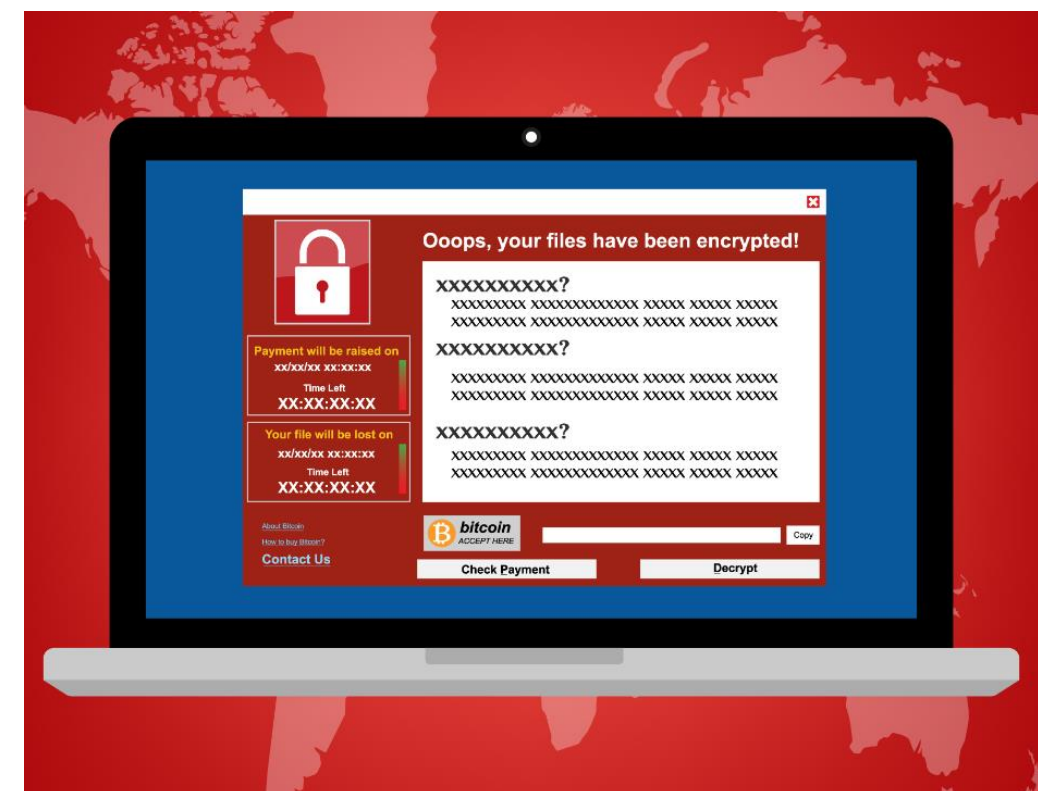
- [CERT Polska](#)
- [Raport roczny CERT, 2018](#)
- [Niebezpiecznik](#)
- **Zgłaszanie incydentów: cert@cert.pl**





# Ransomware

- Złośliwy program szyfrujący dostęp do naszego urządzenia bądź aplikacji (dla okupu)





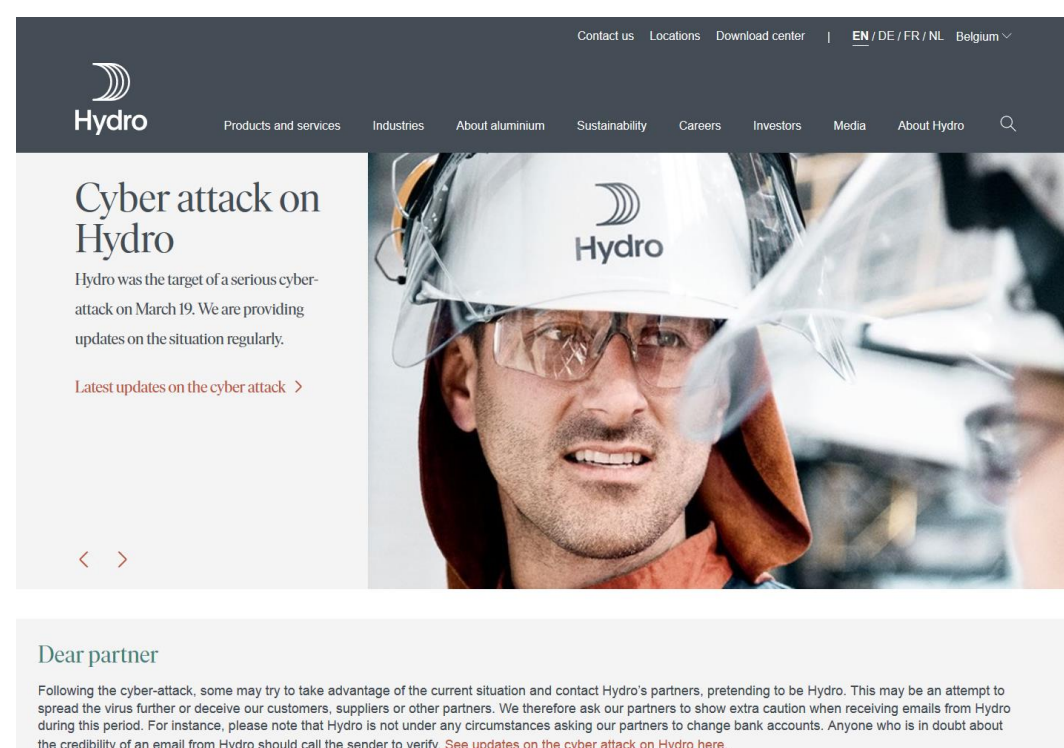
# Ransomware – w szkołach

- Wrzesień 2019: w Arizonie ponad 15 szkół i ponad 9600 uczniów, do tego przedszkola; w Oklahomie gubernator ogłosił stan wyjątkowy dla szkół; zaatakowane okręgi szkolne w Nowym Jorku i Wirginii



# Ransomware – w firmie

- Marzec 2019: atak na producenta aluminium Norsk Hydro zatrudniającego 35.000 pracowników w 40 krajach, w tym w Polsce. Firma przechodzi na ręczne sterowanie produkcją



The screenshot shows the top navigation bar of the Hydro website with links for Contact us, Locations, Download center, and language options (EN / DE / FR / NL, Belgium). The main heading is 'Cyber attack on Hydro'. Below it, a sub-heading reads: 'Hydro was the target of a serious cyber-attack on March 19. We are providing updates on the situation regularly.' A link for 'Latest updates on the cyber attack' is provided. A large image of a worker in a white hard hat with the Hydro logo is featured. Below the image, a 'Dear partner' section contains a warning: 'Following the cyber-attack, some may try to take advantage of the current situation and contact Hydro's partners, pretending to be Hydro. This may be an attempt to spread the virus further or deceive our customers, suppliers or other partners. We therefore ask our partners to show extra caution when receiving emails from Hydro during this period. For instance, please note that Hydro is not under any circumstances asking our partners to change bank accounts. Anyone who is in doubt about the credibility of an email from Hydro should call the sender to verify. See updates on the cyber attack on Hydro here.'

## Cyber attack on Hydro

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, impacting operations in several of the company's business areas.



### Update on operational status in the business areas

Updated April 1, 2019

**Energy:** Production running as normal  
**Bauxite & Alumina:** Production running as normal  
**Primary Metal:** Production running as normal, with higher degree of manual operation  
**Rolled Products:** Production running as normal, with higher

### News about the cyber attack

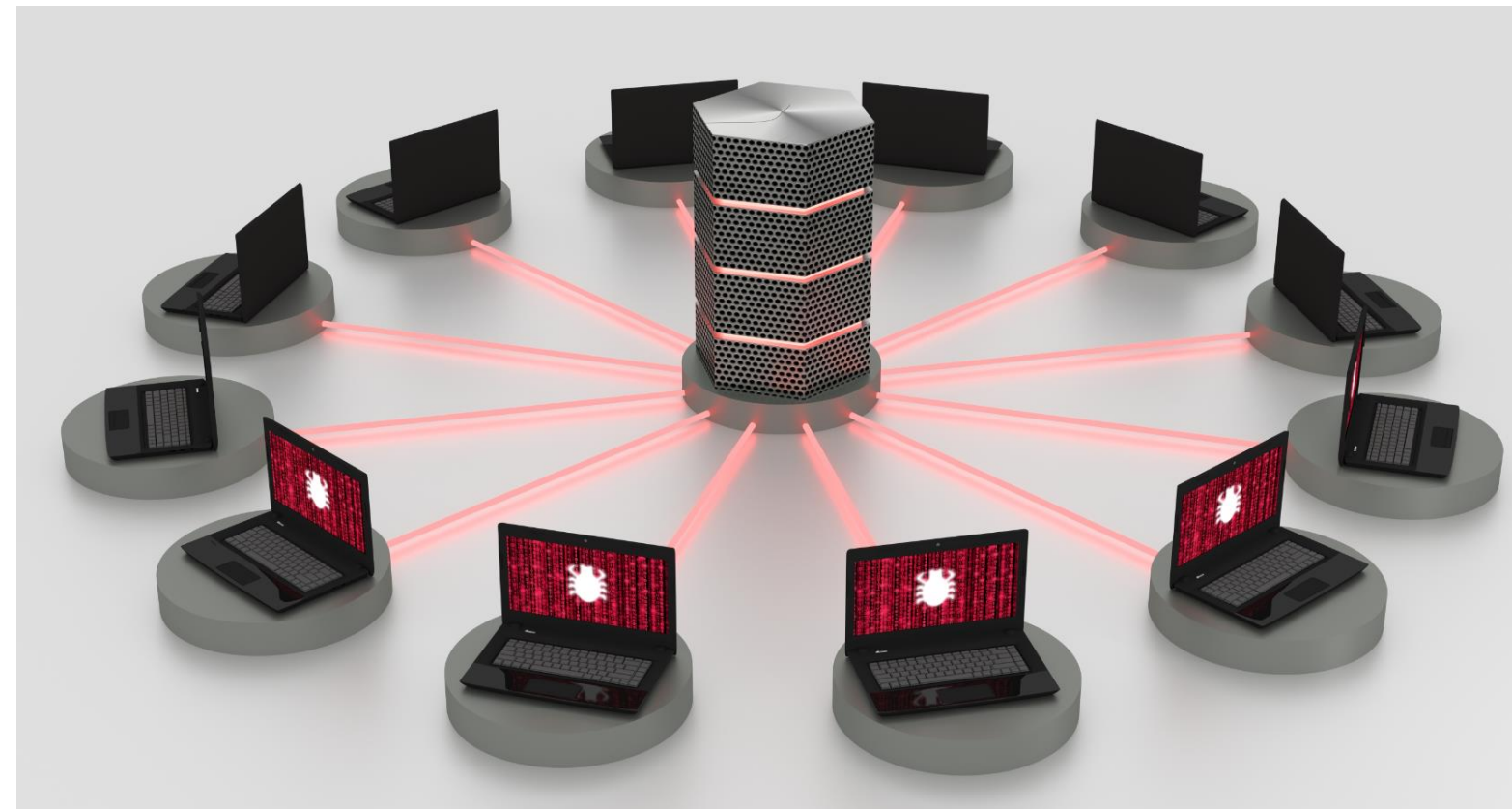
**Update on cyber attack April 5**  
April 05, 2019

**Update on cyber attack April 1**  
April 01, 2019

**Update on cyber-attack March 28**  
March 28, 2019

# Ataki DDOS

- Im więcej botów tym lepiej...



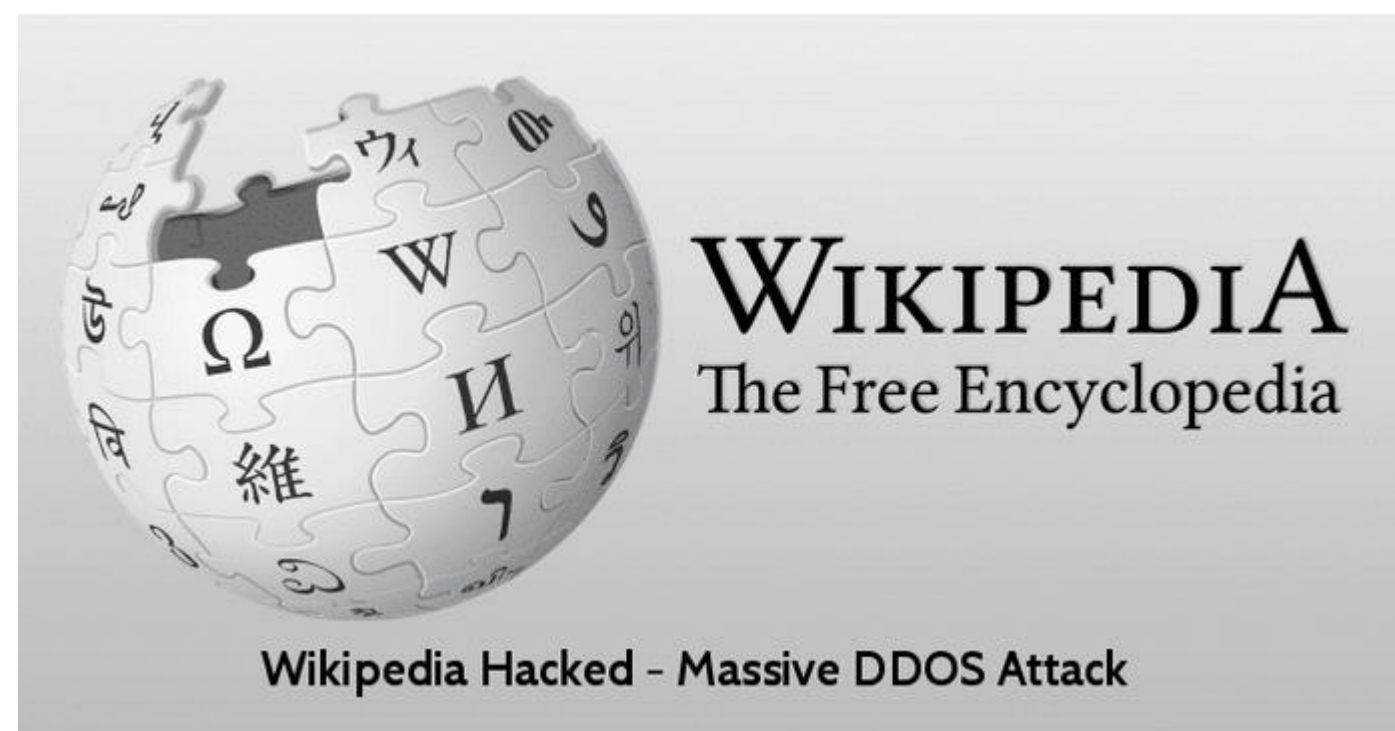


# Ataki DDOS



- Skomasowany atak botów (dla okupu)
- Mechanizm ataku na podobieństwo sytuacji, w której prelegent jest zarzucony jednocześnie tysiącem pytań i nie może udzielić odpowiedzi bo nie słyszy żadnego pojedynczego pytania

# DDOS w użyciu



- Wrzesień 2019: atak zawiesił witryny w kilku krajach w Europie (Anglia, Niemcy, Holandia, Włochy i Polska) i na Bliskim Wschodzie.

# Phishing



- Fałszywe obietnice, alarmy, reklamy oraz nowinki i przekierowania na fałszywe strony oraz usługodawców
- Na fałszywych stronach (tzw. phishingowych) podajemy w dobrej wierze nasze dane osobowe, hasła, numer karty, itd.
- Kupujemy wspaniały fikcyjny towar, a w bonusie otrzymujemy zwykle trojana albo spyware

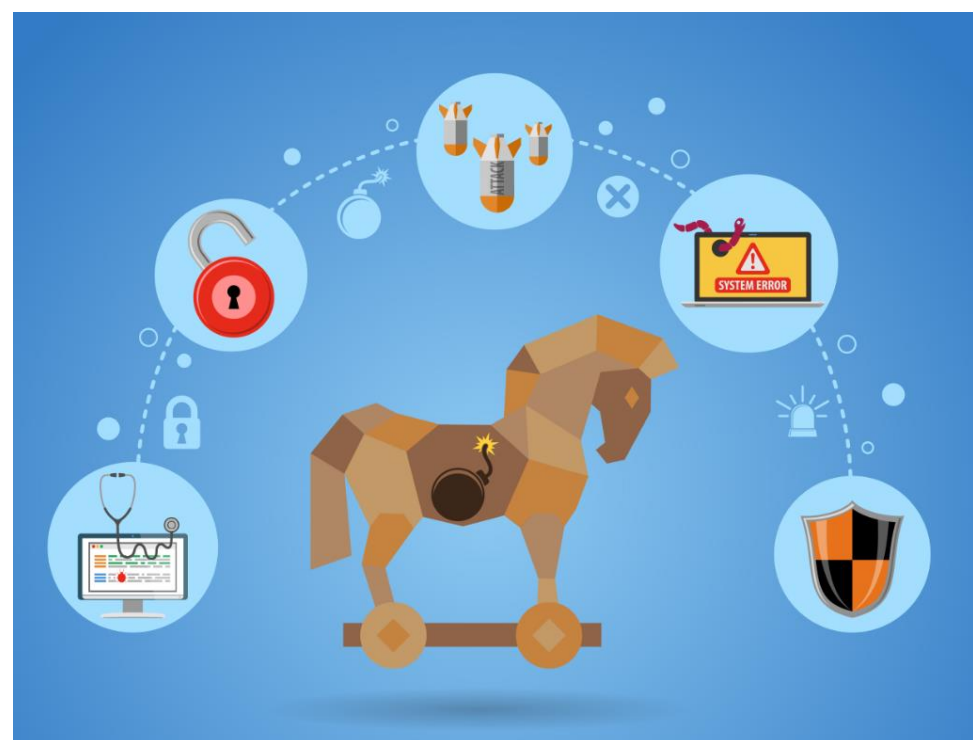
# Phishing – niezbędne składniki



- Nasza naiwność (*podatność na socjotechnikę*)
- Strona www (*podszuwająca się pod prawdziwą*)
- Link (*zmodyfikowany*)
- Przypadki cache poisoning (*zatrucie serwera*)



# Trojany czyli zostań moim przyjacielem...



- Infekcja złośliwym oprogramowaniem komputerów, urządzeń przenośnych i inteligentnych
- Od 2018 wzrosła znacząco liczba trojanów bankowych
- W sklepie Google Play pojawiają się regularnie aplikacje zarażone trojanami

# Keylogger oraz spyware czyli urządzenia szpiegowskie



- Wygodne. Tyle, że można wpaść we własną sieć...
- Spyware nie jest złośliwym oprogramowaniem
- Z powodu keyloggera banki oferują nam klawiaturę wirtualną do wpisywania haseł dostępowych podczas logowania
- Ilość instalacji spyware na smartfony rośnie z roku na rok

# Scenariusze ataków



# Socjotechnika (inżynieria społeczna)

- Szczegółowy [raport](#) przygotowany przez Proofpoint: „Roczny raport nt. czynnika ludzkiego a najważniejsze trendy w cyberprzestępczości” stwierdza, że ponad 99 % cyberataków potrzebuje współpracy ofiary (ludzkiej ręki do kliknięcia)
- WNIOSEK: problemów cyberbezpieczeństwa nie da się rozwiązać kupując jedynie produkt
- Świadomość i prawidłowe zachowanie pracowników są ostatnią i zasadniczą linią obrony

# Socjotechnika łatwiejsza niż tworzenie exploita

- Ponad 99% ataków wymagało aktywnej współpracy ofiary: włączenia makra, otwarcia pliku, dokumentu, kliknięcia linku, wpisania hasła (co prowadziło do kradzieży danych uwierzytelniających, instalowania Trojanów oraz programów szpiegujących)
- W 2018 główną przynętą (1 na 4 wiadomości phishingowe) były rzekome produkty Microsoft
- W 2018 najwyższą klikalność dla wiadomości phishingowych miał „Brainfood” (ponad 1,6 kliknięcia)
- W 2019 zwrot w kierunku przechwytywania informacji w chmurze

# Najczęstsze typy kompromitacji w firmach



- Wrzesień 2019: jak podaje CERT (według [raportu AIG](#)) do najczęstszych kompromitacji systemowych w firmach dochodziło z powodu fałszywych e-maili biznesowych (BEC) – 23%
- Na drugim miejscu uplasował się ransomware a dalej naruszenia spowodowane przez hackerów (często wewnętrznych)

# Phishing i media społecznościowe



- Media społecznościowe kojarzą nam się z czasem wolnym, zabawą i znajomymi
- Najczęściej korzystamy z FB i Twittera przez telefon (linki są skrócone)



# Phishing personalizado

From: FIFA2018 <user-ru@>  
To:  
Subject: FIFA 2018 VOUS DITES MERCI Dela Keline  
Date: Fri, 13 Apr 2018 07:44:15 -0400 (EDT) (13.04.2018 14:44:15)

FIFA WORLD CUP  
RUSSIA 2018

ENCOURAGER VOTRE ÉQUIPE NATIONALE CET ÉTÉ À LA COUPE DU MONDE FIFA RUSSIE 2018



GAGNER UN VOYAGE POUR 2 COMPRENANT:

- TICKETS DES MATCHS
- VOLS
- HÔTEL

Microsoft Microsoft

FIFA 2018 Microsoft Online Promotions Microsoft London (Cardinal Place) 100 Victoria Street London SW1E 5JL, Ref: FFA/MOP/2014-9 Contact FIFA 2018 World Cup Staff From Manager (Mrs. Rosa Smith) From Our Head Office In London United Kingdom

We are pleased to inform you of the result of 2018 draws held on the 6th Jan, 2017, you are the legal beneficiary/User of this selected e-mail address, selected for the FIFA 2018 Microsoft online promotional Awards. Computer ballot was FIFA MICROSOFT NETWORK, at Johannesburg because of the successful FIFA 2010 WORLD aim of this award is to promote the upcoming RUSSIA.

FIVE (5) email addresses was finally picked and out of those (65) email addresses, you winning Pot, which was attached For your Winning Numbers: FFA/MOP/2013-14 21 3 a Million Pound (£1,000,000.00)

Dear Lucky Winner,

We Russia 2018 FIFA World Cup Organizing Committee (RFWCOC) in conjunction with Microsoft-Euro Online lottery Award team officially announces to you the raffle draw held the Month JANUARY 2018 in LONDON, UNITED KINGDOM Your e-mail address was among the 100,000,000 e-mail while draw which your e-mail was randomly picked up by the computer during the 3rd Quarter Raffle draw held in United Kingdom.

We therefore wish to inform you that your e-mail address has won you the total sum of (£1,000,000,000.00) One Million Great Britain Pound Sterling. Participant's email addresses were sorted out globally (Powered by Microsoft) from Companies, Individuals, Government's Agencies, Co-operative bodies, Charity homes etc and compiled "RANDOMLY" via E-scoring balloting to select respective winners around the globe.

Lottery Award team and Russia 2018 FIFA as Russia is busy finalizing their paid in accordance with his/her their notifications any Prize not claimed

Your Email ID Won GBP£500,000.00 from Russia FIFA World Cup 2018. Our South African bureau's 'Pay out Officer' will immediately process the release of your (Five Hundred Thousand British Pounds Sterling) (GBP£500,000.00) cash prize and travel tickets to the World Cup in Russia 2018. Contact your claim agent. Email: <user-ru@>@yahoo.com Ticket Number: BOLP 8647 7092545 13, with Serial Number 8907765432 You have to send the following information to your Claims Agent to facilitate the release of your fund to you. (1) YOUR NAMES:(2) AGE:(3) SEX:(4) COUNTRY:(5) ADDRESS:(6) CELL PHONE:(7)OCCUPATION:(8) TICKET NUMBER:

Yours sincerely  
Microsoft Organizing Committee  
Ms. Rosa Smith  
Special Global Russia Tourism Megamillions Promotional Lottery Draws. For enquiry: Tel: +44-770-030-4727

From: Visa@>  
To:  
Subject: Visa Platinum-VOCE E UM ACOMPANHANTE COM TUDO PAGO NA COPA DO MUNDO DA FIFA 2018. OFERCIMENTO VISA  
Date: Mon, 23 Apr 2018 11:28:36 +0000 (23.04.2018 14:28:36)

VISA  
RUSSIA 2018  
worldwide partner

PARTICIPE DA PROMOÇÃO

PRÊMIOS  
São 10 pacotes para uma experiência VIP na Copa do Mundo de FIFA 2018. Você e um acompanhante com tudo pago! Inclui passagens aéreas de ida e volta em classe executiva, taxas de embarque, traslado, hospedagem e ingressos. Oferecimento Visa.

RS 120.000,00 por mês.  
Saiba como participar  
Basta se cadastrar e fazer uma compra a partir de RS 5,00 e você já estará participando da promoção. Como funciona?  
Suas compras realizadas a partir de RS 5,00 você concorre até RS 10.000,00  
RS 50,00 você concorre até RS 60.000,00  
RS 100,00 você concorre até RS 120.000,00

CONTINUAR

VISA onde você quiser estar.

Click to open <http://vaivevsarussia2018.com>

# Ransomware: „pomyślna współpraca” z ofiarą warunkiem skutecznego ataku



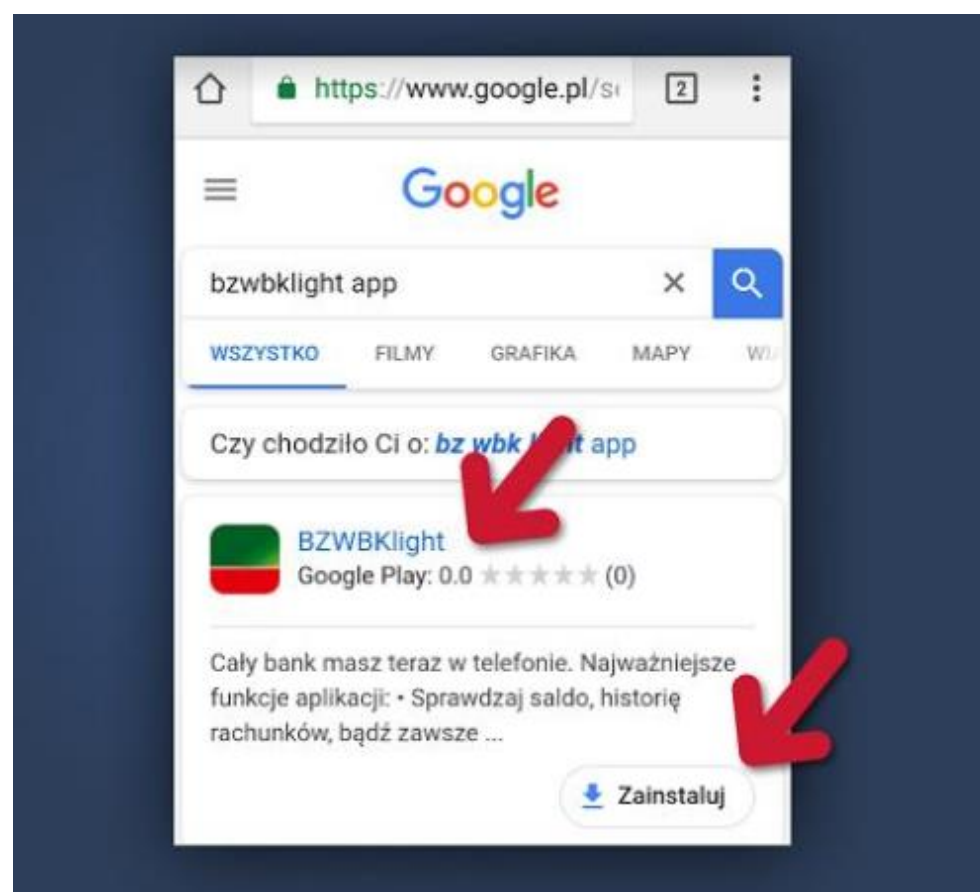


# Wyciek danych (FB i komórki)



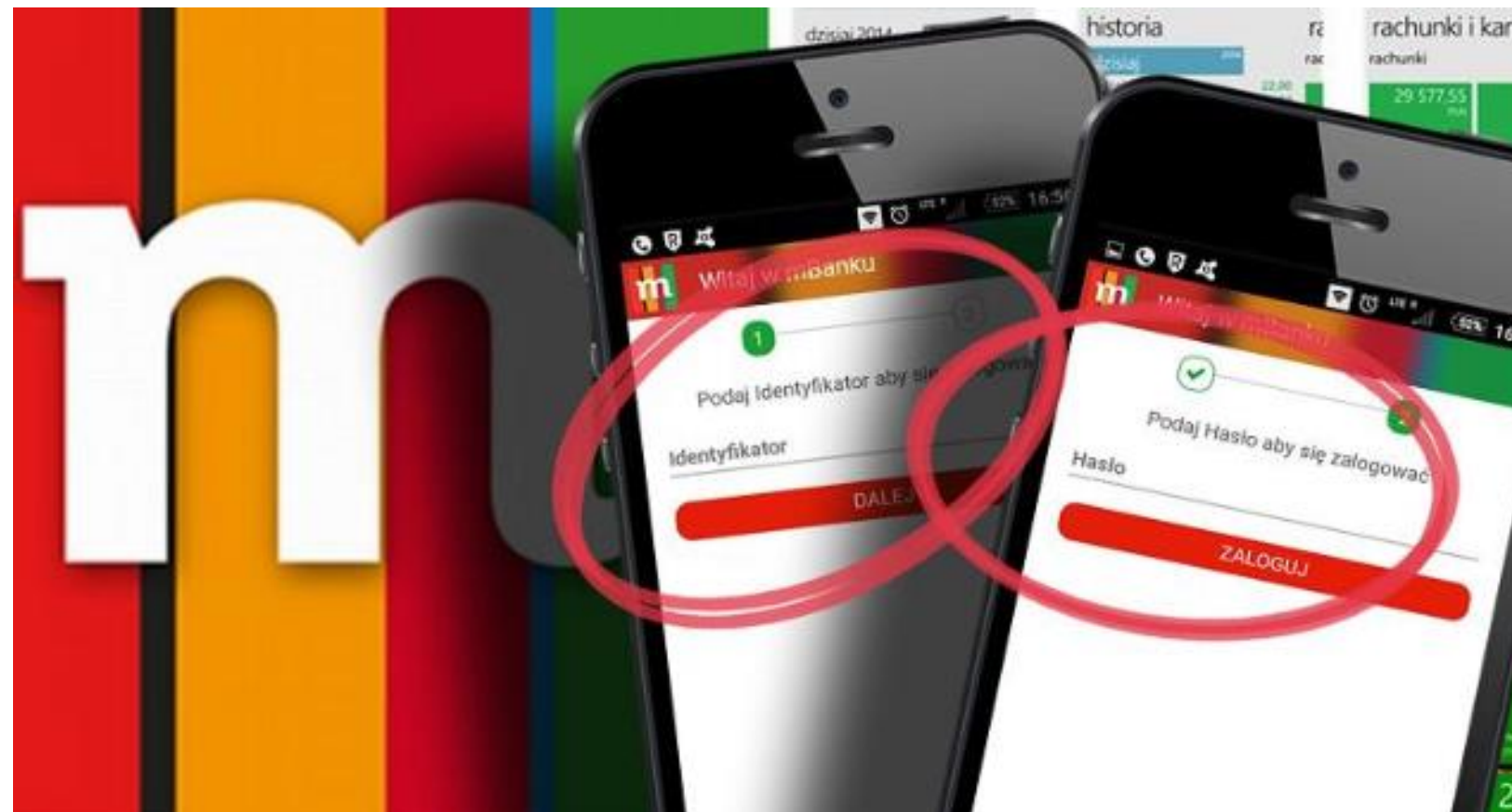
- Wrzesień 2019: [TechCrunch](#) zlokalizował bazę danych zawierającą 419 milionów numerów telefonów użytkowników z kontem na FB.
- serwer nie był chroniony hasłem i przechowywał rekordy z unikalnym identyfikatorem FB dla konkretnego użytkownika (+ numer telefonu powiązany z kontem).
- W niektórych przypadkach zapisy ujawniały także nazwę użytkownika, płeć i lokalizację według kraju.

# Trojany bankowe i urządzenia przenośne





# I znowu trojany...



# EURid a cyberbezpieczeństwo

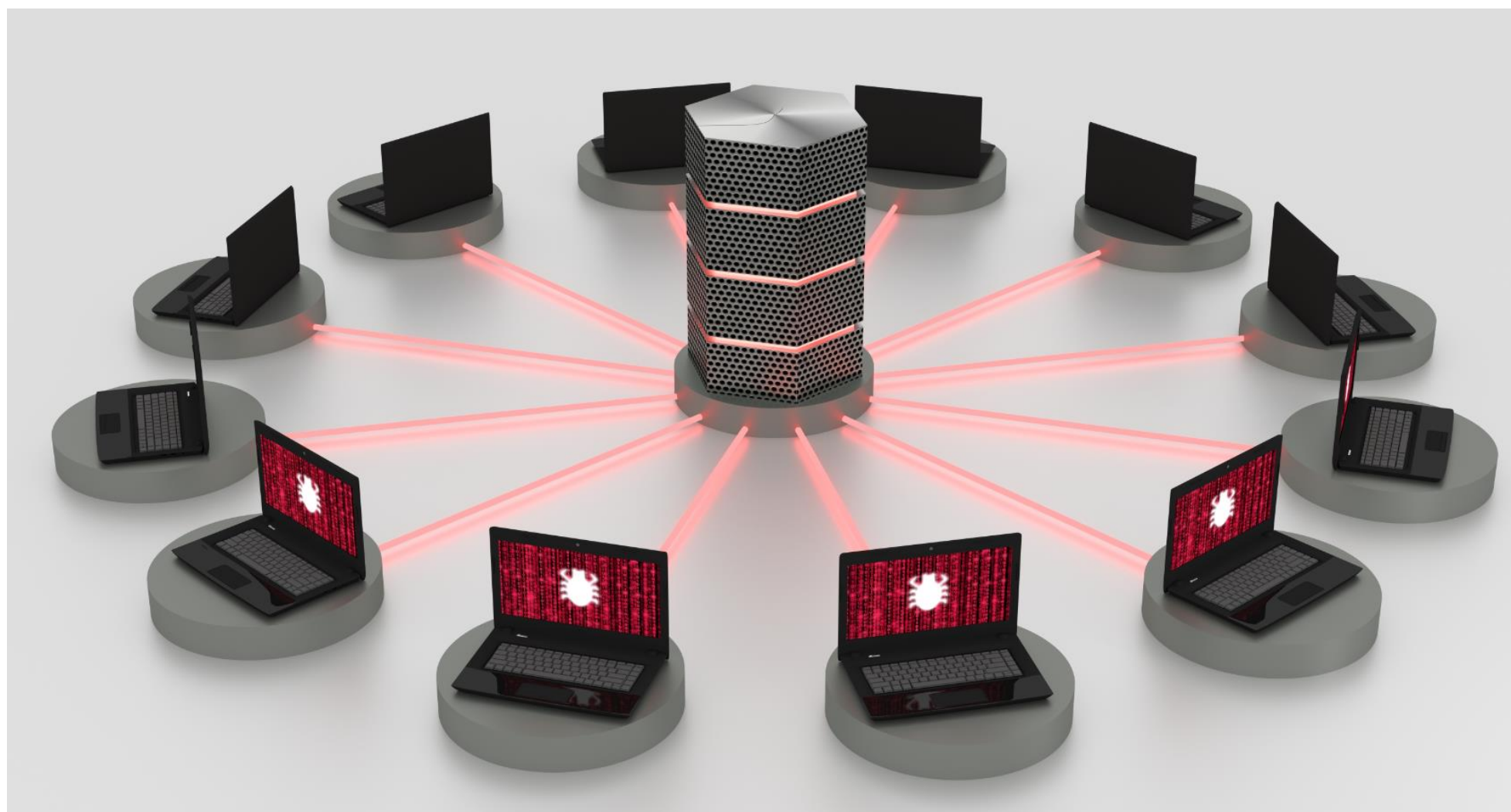


- 
- Co jest głównym motorem skutecznego ataku cyberprzestępczego?

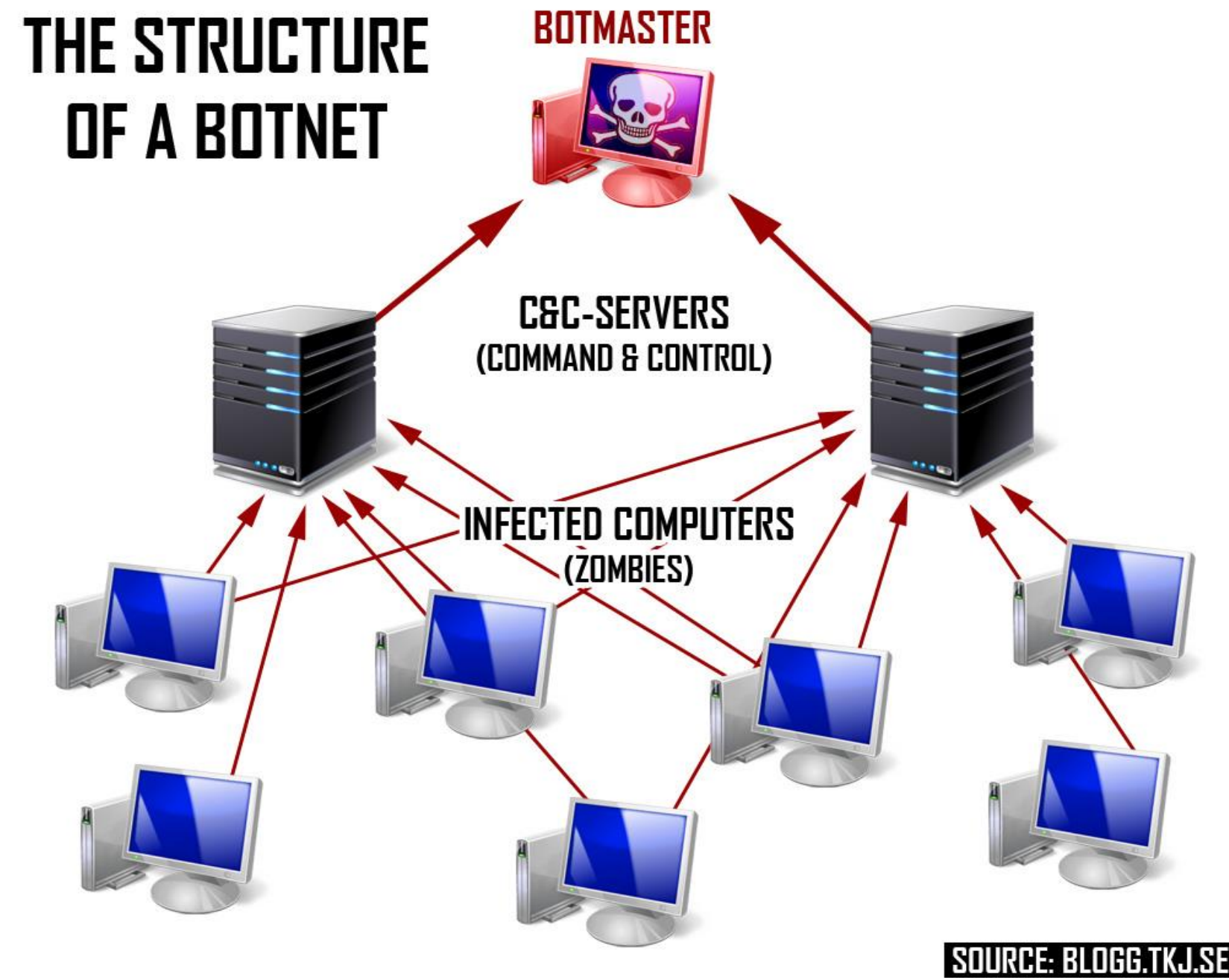


# Botnet

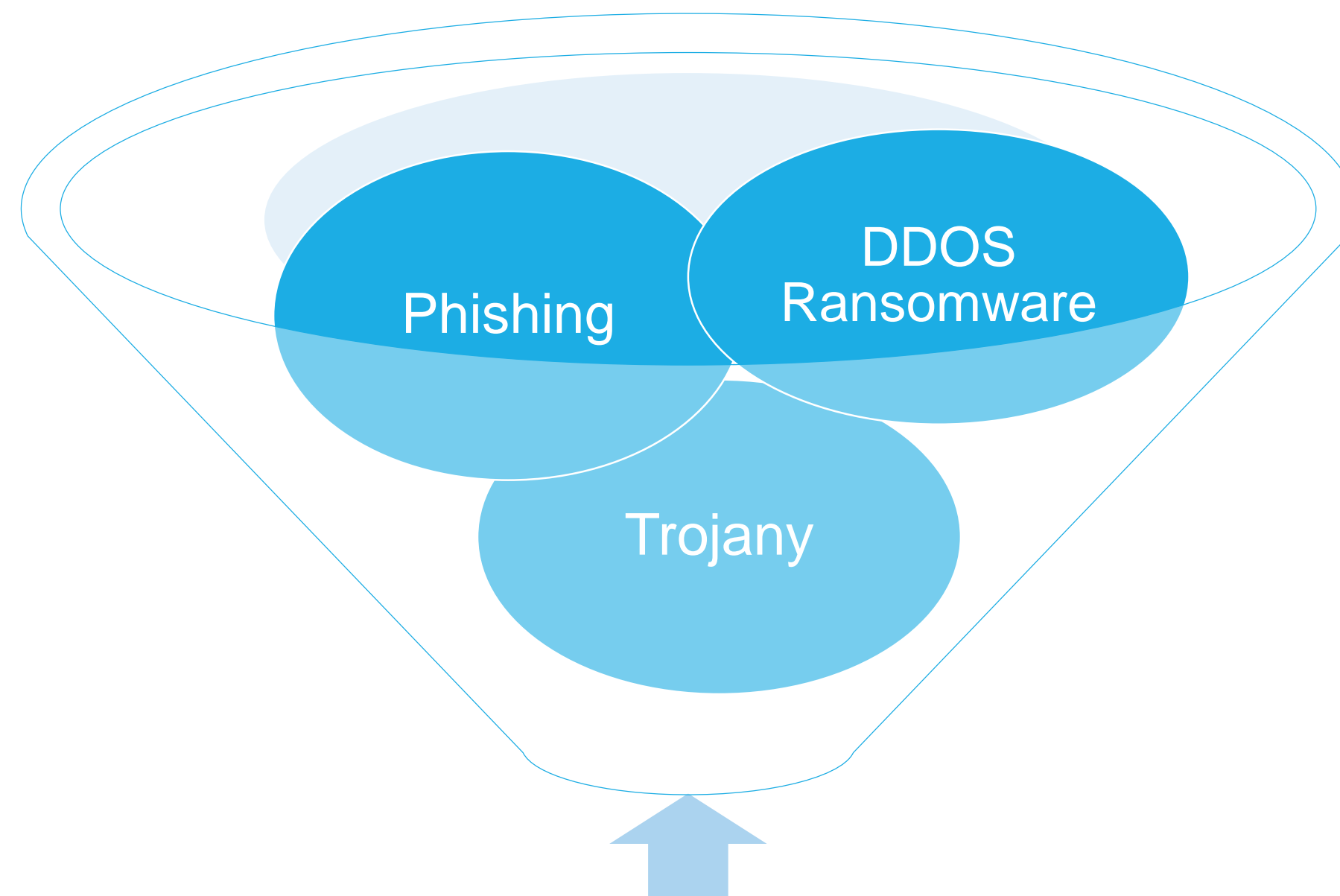
- Czyli baza infrastrukturalna dla działań cyberprzestępczych



# Anatomia botnetu



# Bez botów ani rusz...



strony www & sztuczki socjotechniczne



# Kontrola danych rejestracyjnych abonentów



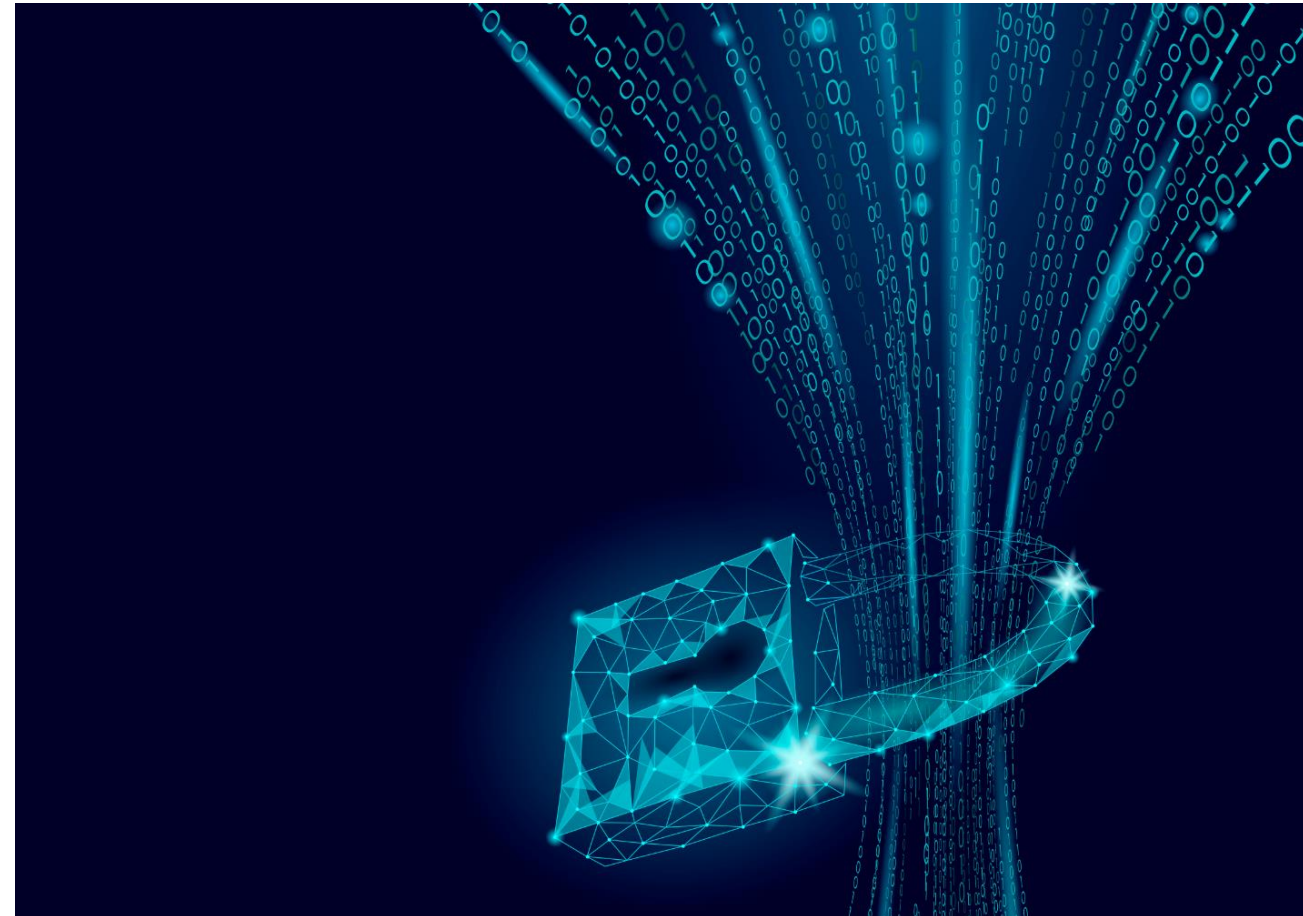
# Odroczona delegacja domen oraz system szybkiego wykrywania

- EURid przy współpracy z KU w Lowanium (najstarszy uniwersytet w Belgii) prowadził [badania](#) na temat możliwości wczesnego wykrywania rejestracji domen w celach przestępczych
- Badania były prowadzone przez okres 14 miesięcy i dotyczyły blisko 830 tys. nowo rejestrowanych domen; 2,5% z nich było oznaczonych do przodu jako potencjalnie złośliwe i znajdowały się na czarnej liście (prowadzonej przez wyspecjalizowane organizacje typu Spamhouse)
- Nasze badania pokazały, że dodatkowe 18,2% złośliwych domen nie trafia na czarną listę a proces rejestracji złośliwych domen jest tylko częściowo zautomatyzowany.
- Organizacje cyberprzestępcze działają w godzinach pracy, mają przerwy na wakacje, a ich „pracownikom” zdarzają się pomyłki (ludzki błąd) podczas rejestracji fałszywych domen.
- Dzięki zastosowanym algorytmom i AI (uczeniu maszynowemu) EURid planuje wprowadzić w połowie października odroczone (na mniej niż 4 dni) delegacje domen .eu oraz system dodatkowego screeningu domen po dokonanej rejestracji.



# Zabezpieczenie DNSSEC

- EURid wprowadził protokół DNSSEC już w 2010 r. jako jeden z pierwszych rejestrów



# Wspieramy DNSSEC

- EURid wspiera każdego rejestratora (poprzez system zniżek), który oferuje zabezpieczenie DNSSEC
- Prowadzimy profesjonalne szkolenia dla swoich partnerów
- Abonenci domen wybierając domeny z zabezpieczeniem DNSSEC także przyczyniają się do utrzymywania wyższego bezpieczeństwa wszystkich internautów

# Współpraca z EURidem

- EURid nie zawiesza domen .eu na podstawie treści publikowanej w witrynie. Zgłaszamy, co może być przestępstwem, współpracując z policją lub sądami.
- Od 2016 r. usprawniamy procesy i zwiększamy bezpieczeństwo domen oraz abonentów dzięki współpracy z następującymi organizacjami:
  - **EUROPOL** (wymiana informacji oraz wsparcie w przeciwdziałaniu; wspólne projekty – np. w grudniu 2017 konferencja nt. współpracy transgranicznej w zwalczaniu cyber przestępczości)
  - **EUIPO** (unijne znaki towarowe EUTM), od maja 2019 system powiadomień dla abonentów domen .eu

# Usługa Blokady Nazwy Domeny

- Usługa „Registry Lock” (Blokada Nazwy Domeny) dla nazw o szczególnej wartości



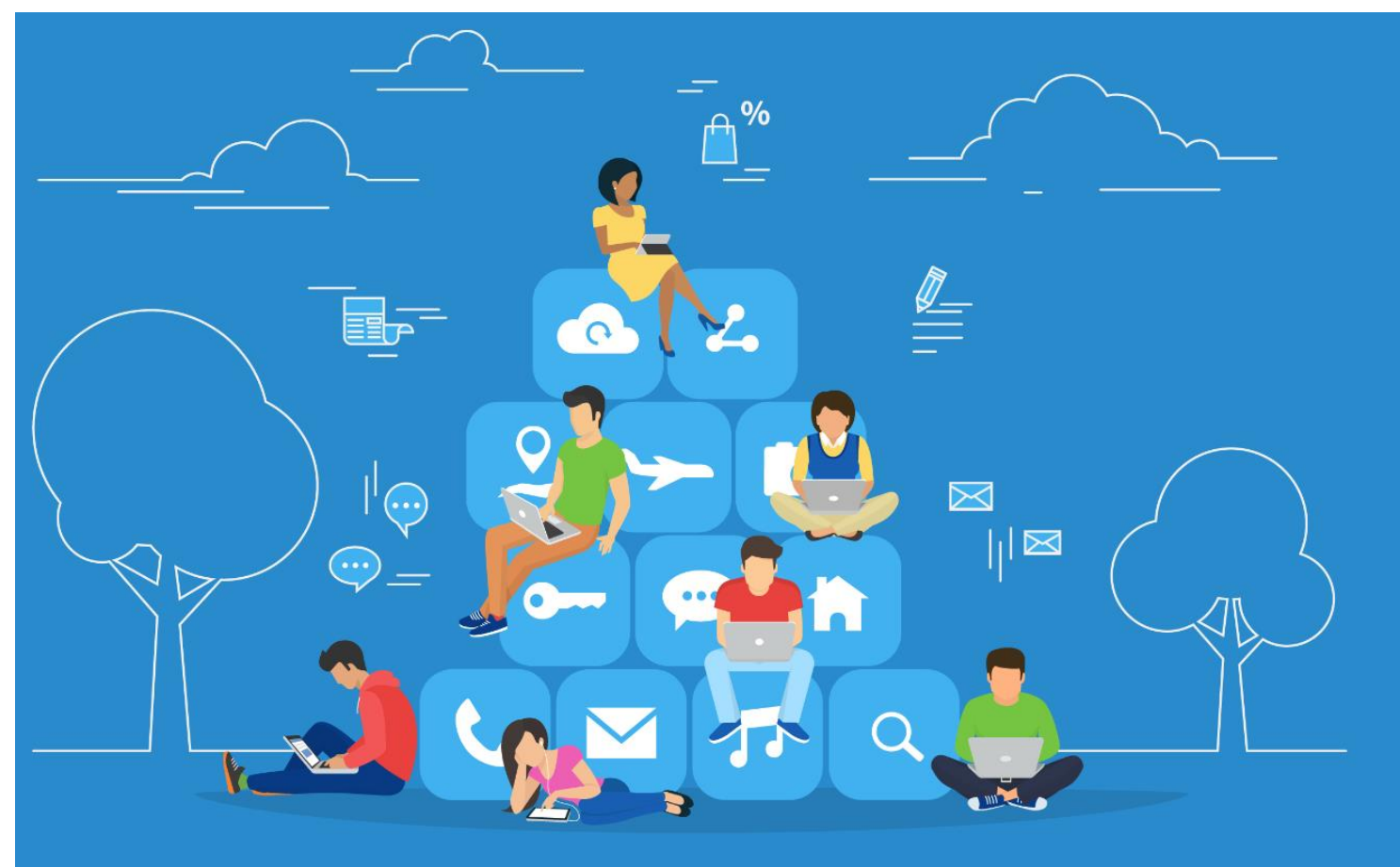
# Profilaktyka cyberbezpieczeństwa





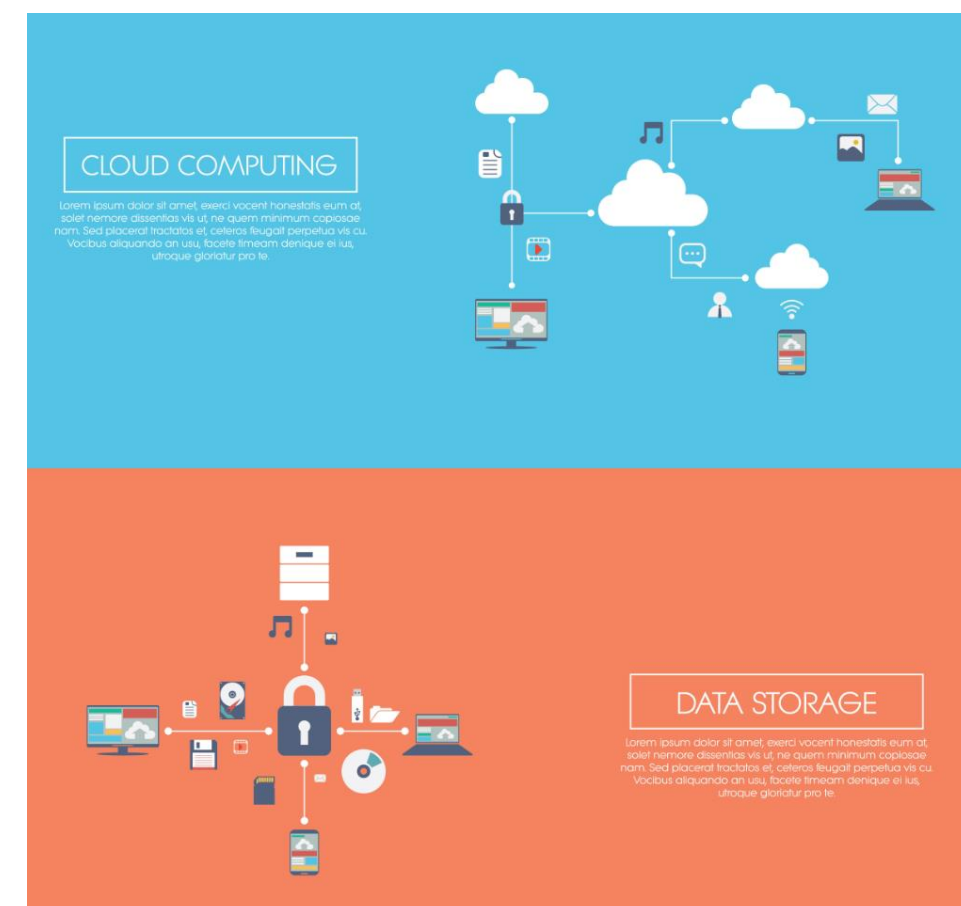
# Połączenia bezprzewodowe (routery, Wi-Fi, itp.)

- Najbezpieczniej z VPN



# Backup wszystkich zasobów

- Kopie zapasowe czyli backup:
  - W chmurze
  - Na zewnętrznym nośniku
- Szyfrowanie danych (w każdym przypadku)
- Szczegółowa umowa z usługodawcą



# Komórki oraz inne urządzenia przenośne

- ✓ Blokowanie ekranu (PIN/odcisk palca)
- ✓ Automatyczne wygaszanie ekranu
- ✓ Obszar aplikacji firmowych zamknięty w VPN i na osobny PIN
- ✓ Wyłączamy Wi-Fi oraz hotspot kiedy nie są bezpośrednio potrzebne
- ✓ Nie przeprowadzamy transakcji finansowych (ani żadnych gdzie musimy podawać poufne dane) w kawiarni
- ✓ Załączniki oraz linki – zastanawiamy się przed kliknięciem, sprawdzamy w komputerze, na dużym ekranie
- ✓ Zaszifrować obszar aplikacji firmowych w komórce silnym algorytmem (AES-256)
- ✓ Możliwość zdalnego blokowania i zarządzania urządzeniem/ ustawieniami
- ✓ Nie zezwalamy w Ustawieniach na instalacje z nieznanego źródła
- ✓ Nie wydajemy pozwolenia na przyjmowanie smsów przez aplikację
- ✓ Program antywirusowy.....oczywiście



# Klasyczne sztuczki socjotechniczne

- ✓ Załączniki niewiadomego pochodzenia
- ✓ Pamięć przenośna USB (pendrive)
- ✓ Spersonalizowane reklamy na FB/ Twitter
- ✓ Linki reklamowe (adres może być ładnie podobny, jednak różny od oryginalnego)
- ✓ Aplikacje „ułatwiające życie” (głównie cyberprzestępcom)
- ✓ Phishing – zbyt pięknie by prawdziwe
- ✓ Chwyty na „prezesa” – potrzeba jasnych procedur w firmie
- ✓ SMS-y, które może wysyłać każdy.. (za to np. z logo T-Mobile)



# Zabezpieczenie SSL

- Wszelkie dane przesyłane pomiędzy odwiedzającym strony a serwerem są szyfrowane, zatem niewidzialne dla osób trzecich
- Stronę zabezpieczoną poznamy po „https” oraz zielonej kłódce

- *wersja podstawowa certyfikatu:*

  <https://eurid.eu/en/>

- *wersja zaawansowana certyfikatu*

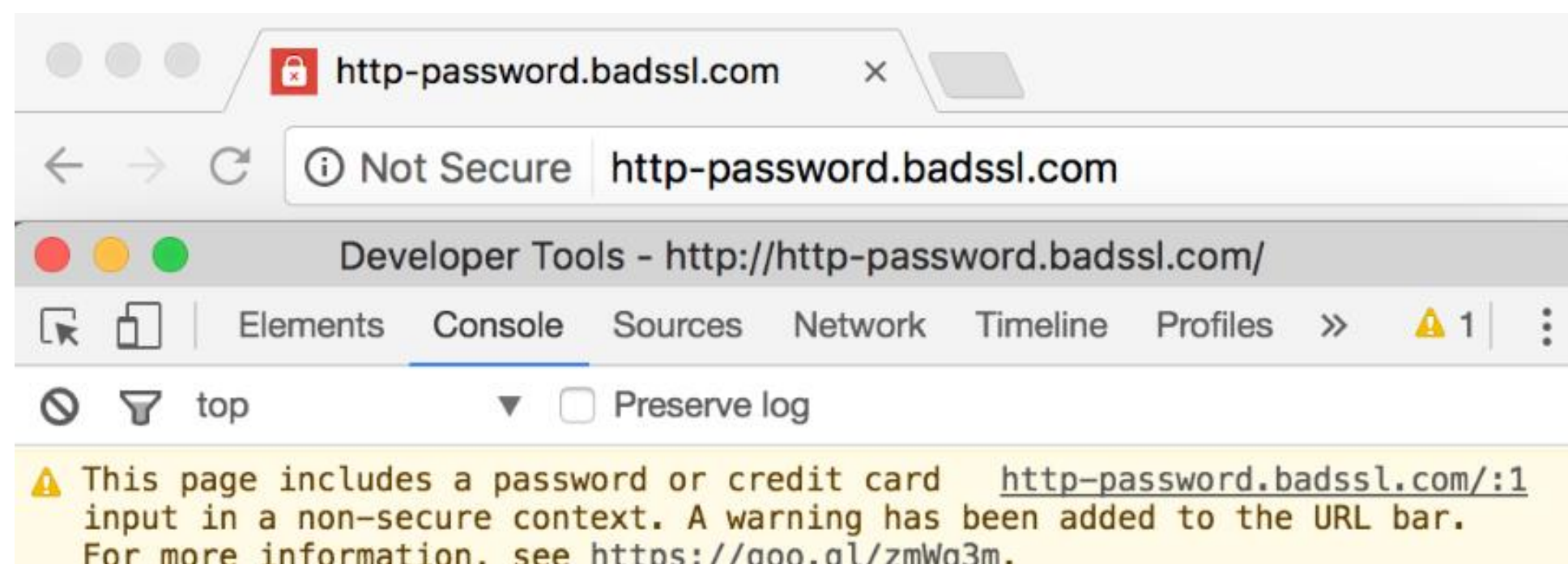
  [home.pl S.A. \(PL\) | https://home.pl](https://home.pl)

**Uwaga:** SSL oznacza jedynie, że komunikacja jest zaszyfrowana (a nie że strona jest w uczciwych rękach, patrz: Mistrzostwa Świata w Rosji)



# Ułatwienia w Google Chrome

- Google Chrome



# Przydatne linki

- <https://www.enisa.europa.eu/media/multimedia/material>  
(multimedialny materiał edukacyjny)
- <https://haveibeenpwned.com/>  
(tutaj można sprawdzić czy nasze konto pocztowe było zhakowane)
- <https://virustotal.com/>  
(skan wirusów według 50+ virusscanners)

# Pytania



# Dziękujemy!

Aneta Szczepankiewicz, [anetas@eurid.eu](mailto:anetas@eurid.eu)

...eu...eu

Powered by **EURid**

