Cyberbezpieczeństwo w pracy oraz w życiu prywatnym

EURid?

- EURid jest rejestrem europejskich domen internetowych .eu oraz .ею (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

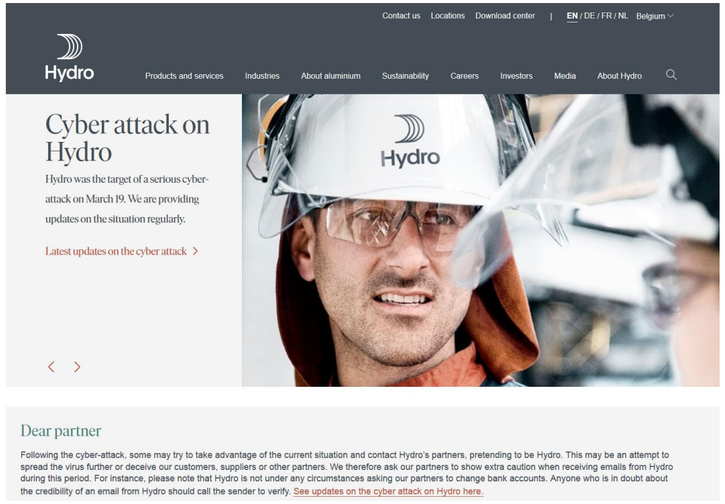
- Złośliwy program szyfrujący dostęp do naszego urządzenia bądź aplikacji (dla okupu)

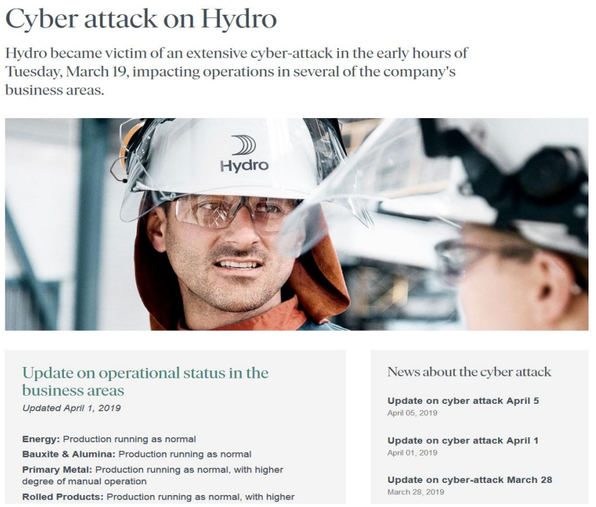
Ransomware – w szkołach

- 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

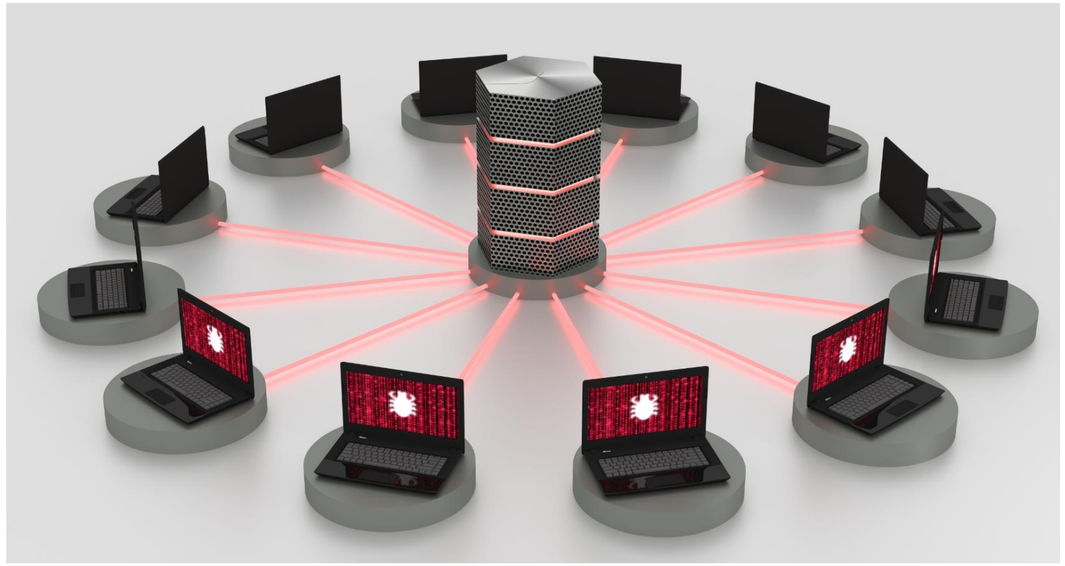
- Marzec 2019: atak na producenta aluminium Norsk Hydro zatrudniającego 35.000 pracowników w 40 krajach, w tym w Polsce. Firma przechodzi na ręczne sterowanie produkcją



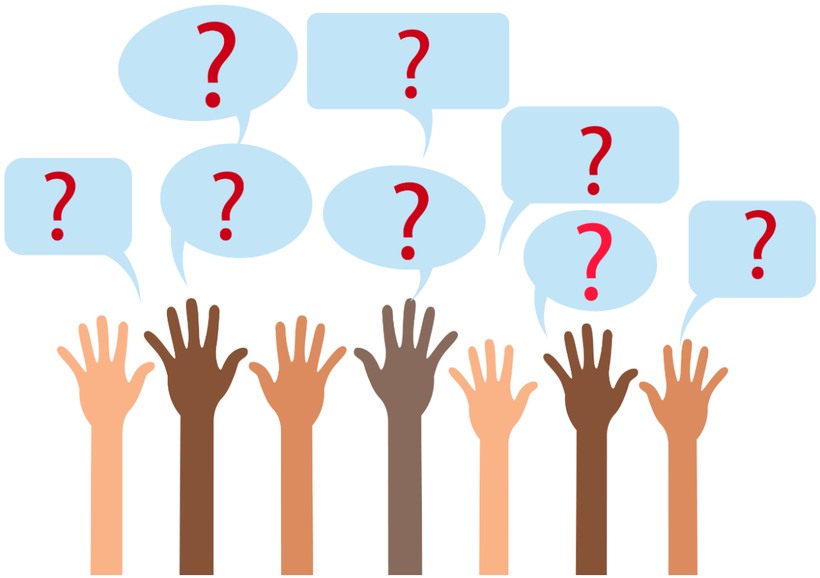


Ataki DDOS

- 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.

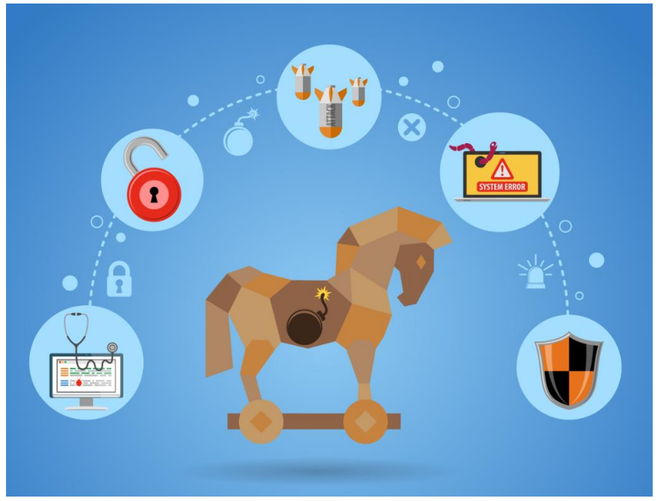
Phishing

- 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 *(podszywająca 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)

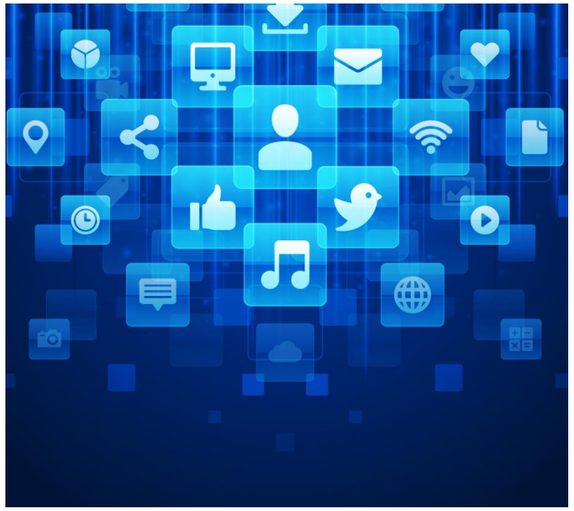
- W 2019 zwrot w kierunku przechwytywania informacji w chmurze

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%

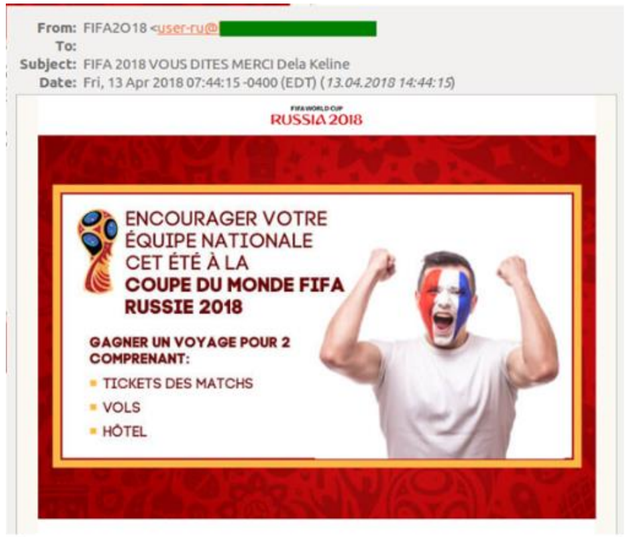
- Na drugim miejscu uplasował się ransomware a dalej naruszenia spowodowane przez hackerów (często wewnętrznych)

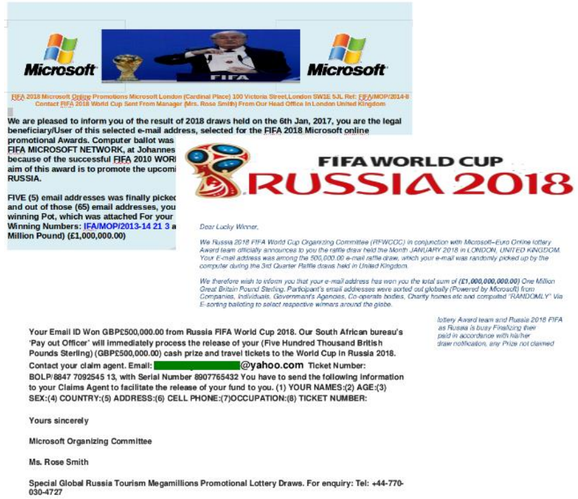
Phishing i media społecznościowe

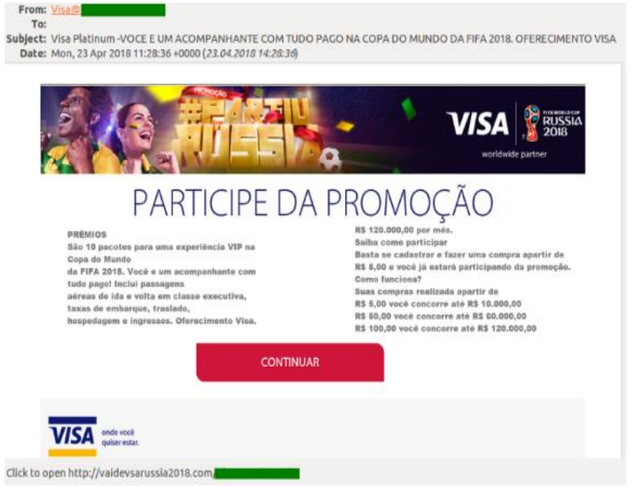


- Media społecznościowe kojarzą nam się z czasem wolnym, zabawą i znajomymi
- Najczęściej korzystamy z FB i Twittera przez telefon (linki są skrócone)

Phishing spersonalizowany







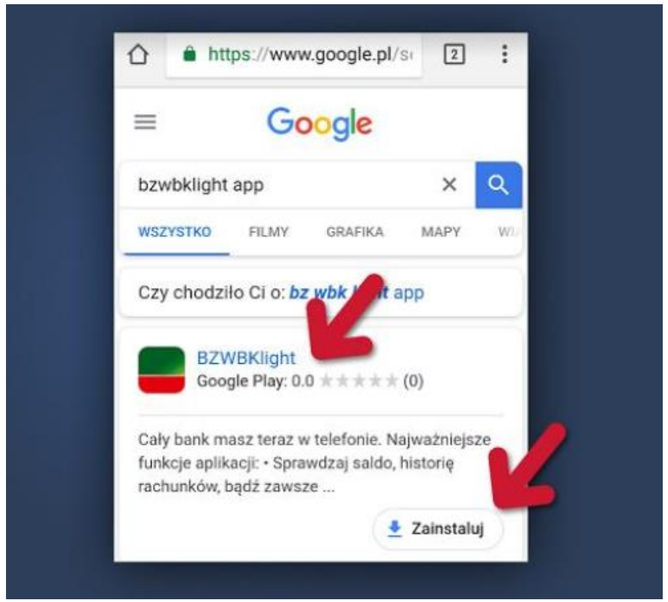
Ransomware: „pomyślna współpraca” z ofiarą warunkiem skutecznego ataku

Powered by EURid

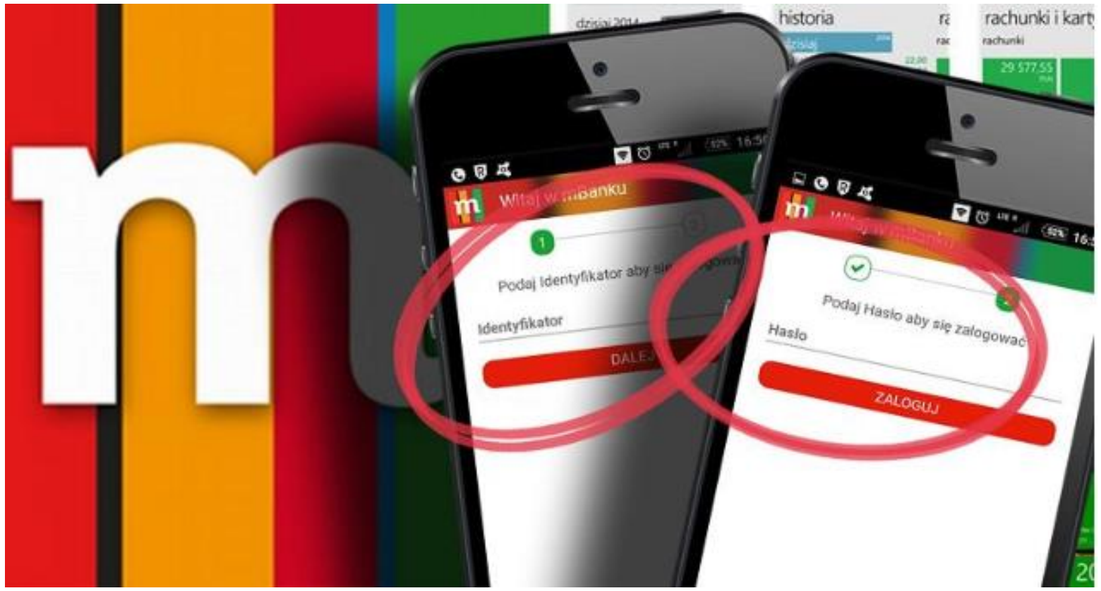
Wyciek danych (FB i komórki)

- 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…

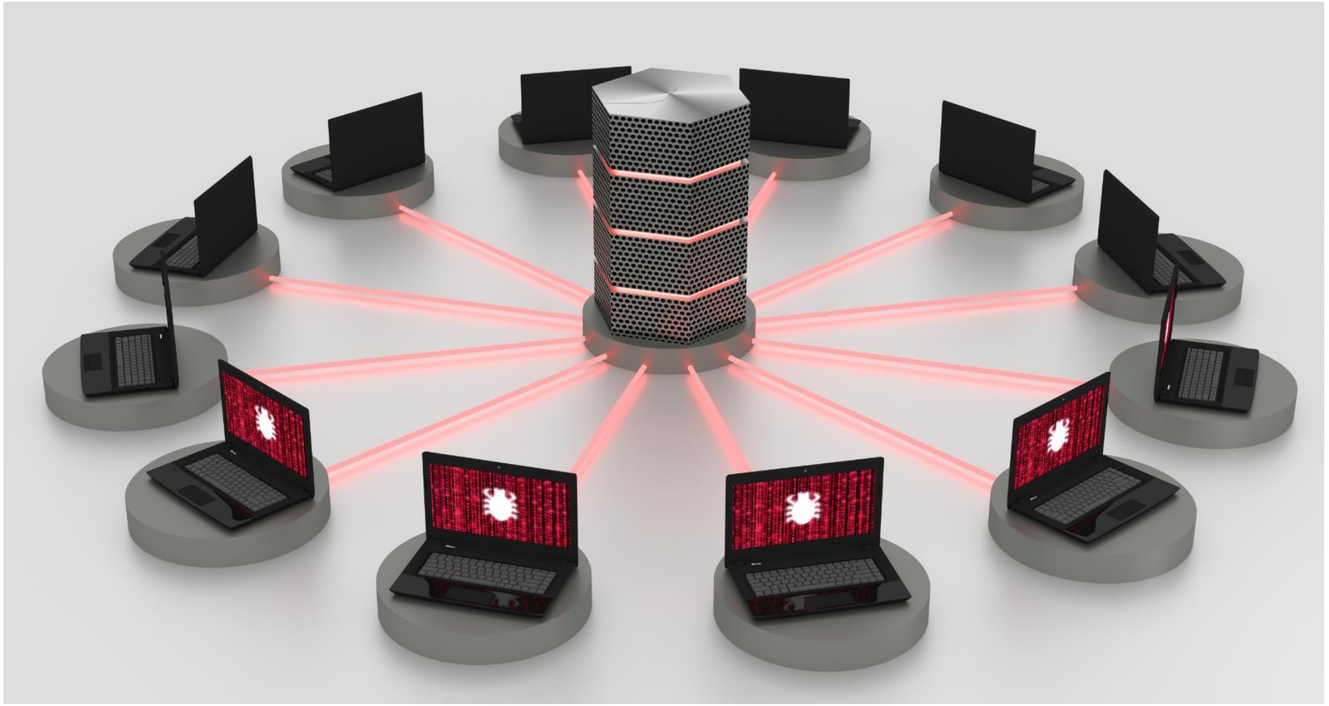


EURid a cyberbezpieczeństwo

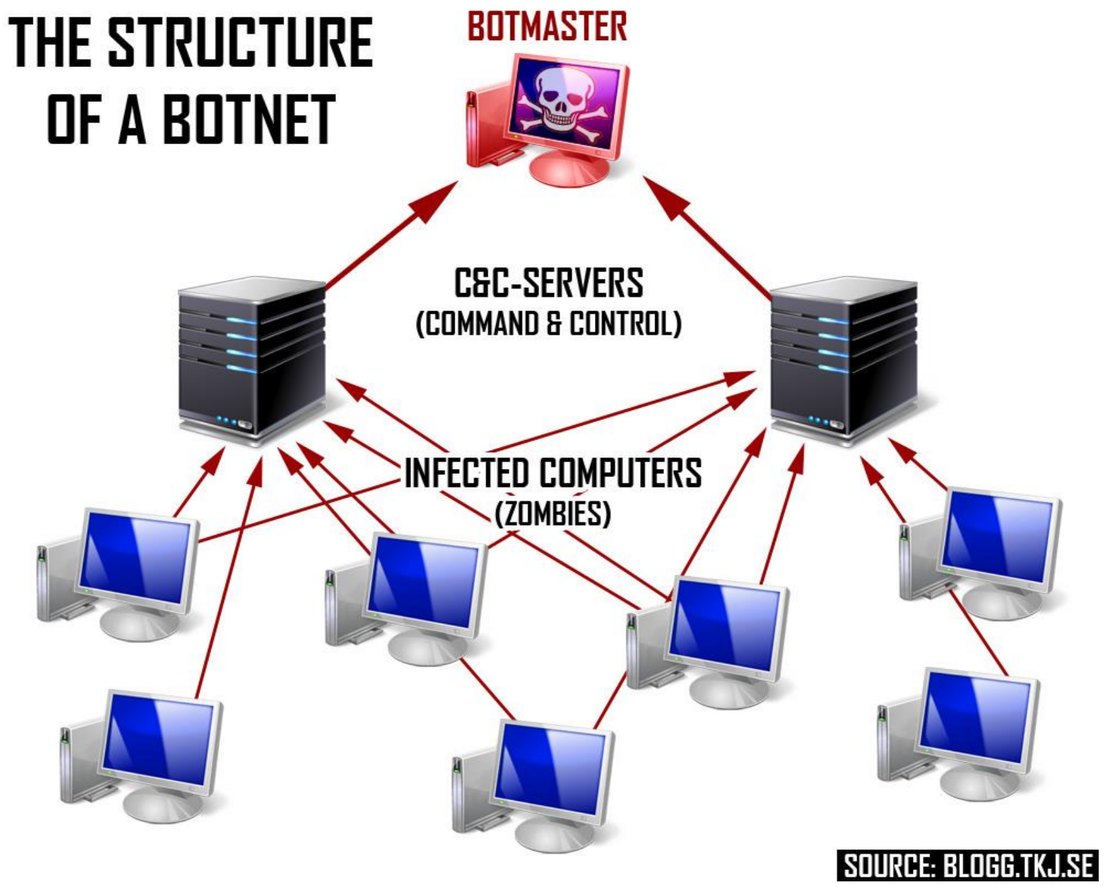
- Co jest głównym motorem skutecznego ataku cyberprzestępczego?

Botnet

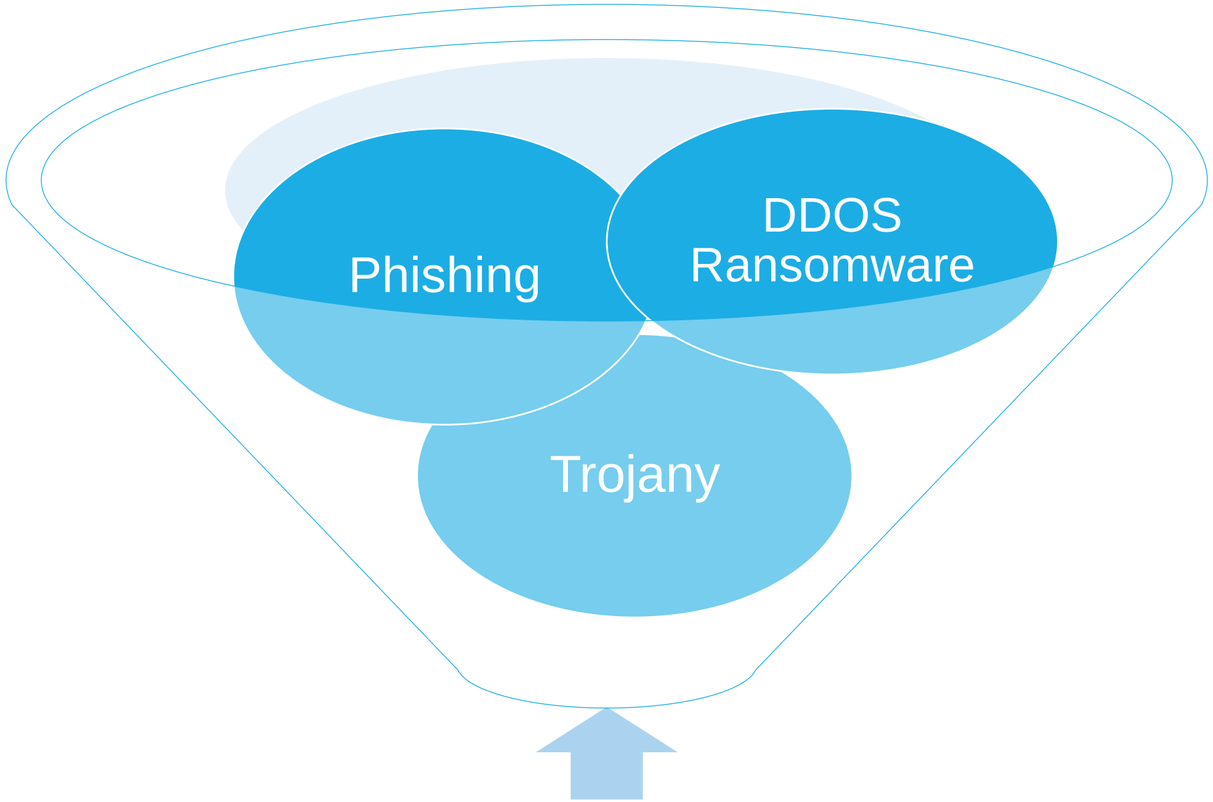
- Czyli baza infrastrukturalna dla działań cyberprzestępczych



Anatomia botnetu



Bez botów ani rusz…



strony www & sztuczki socjotechniczne

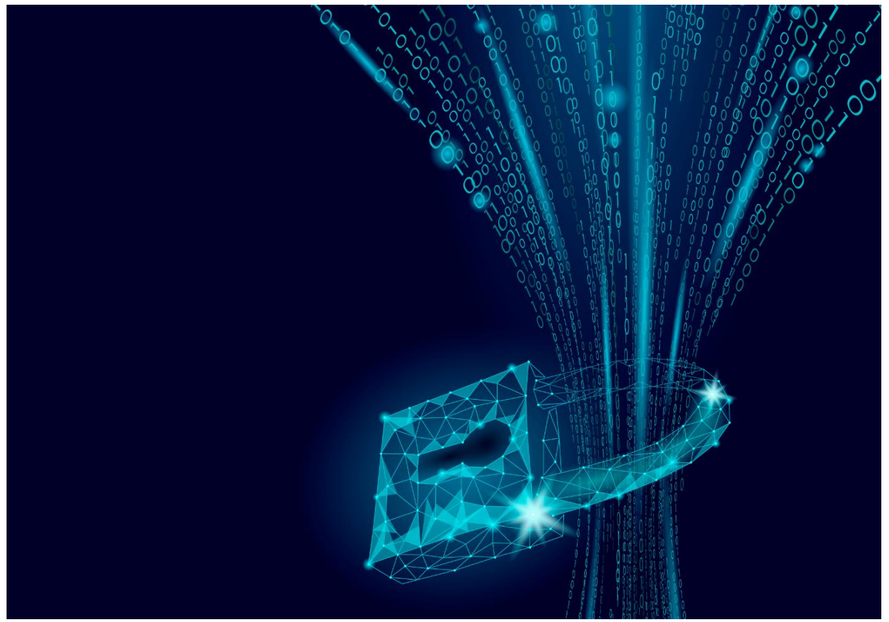
Kontrola danych rejestracyjnych abonentów

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 DNNSEC 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

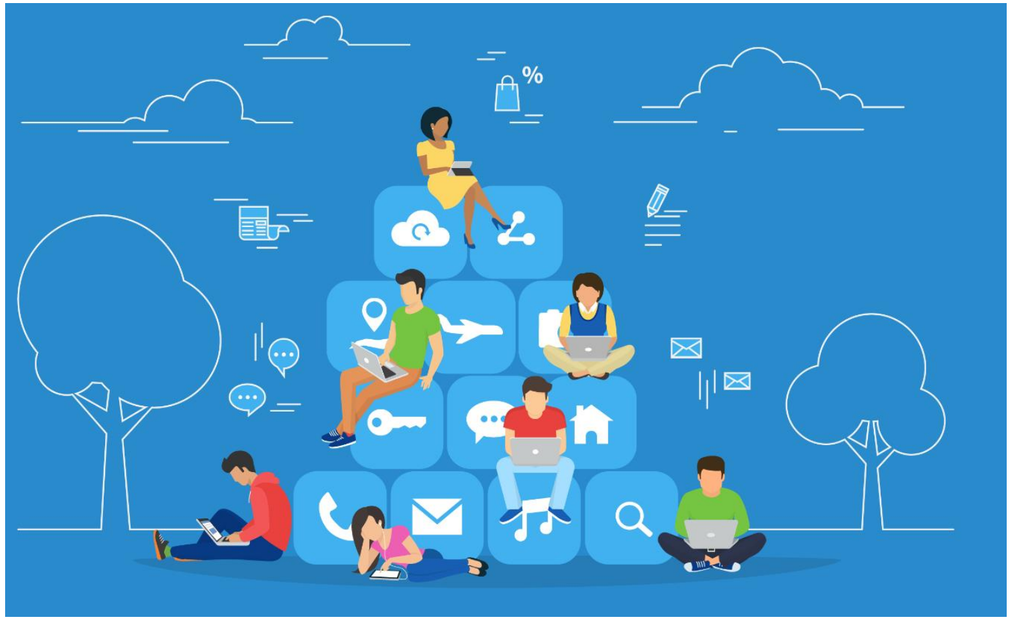
Usługa Blokady Nazwy Domeny

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

Profilaktyka cyberbezpieczeństwa

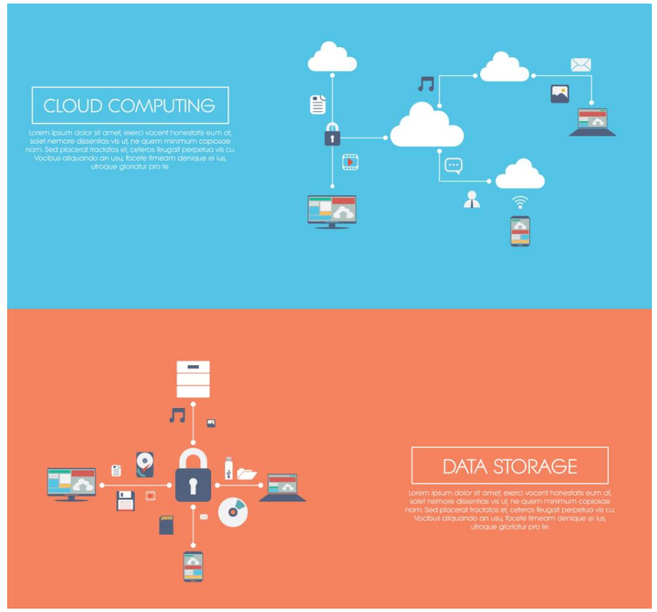
Połączenia bezprzewodowe (routery, Wi-Fi, itp.)

- 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
- ✓ Zaszyfrować 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

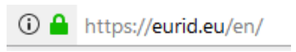
Klasyczne sztuczki socjotechniczne

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

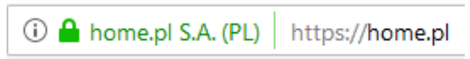
Zabezpiecznie SSL

- 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:*



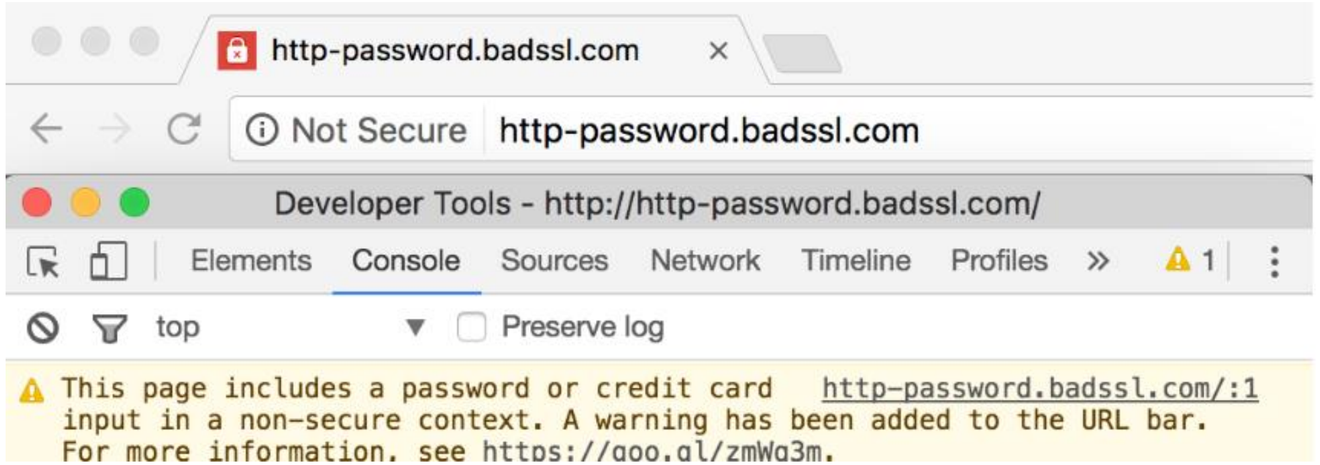
  - *wersja zaawansowana certyfikatu*



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

Powered by EURid

Powered by EURid