Współczesna scena IT security

Leszek Tasiemski

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Kim jestem

- 10 lat doświadczenia
- Principal Security Consultant w nSense Polska
- Specjalność
  - web aplikacje
  - aplikacje mobilne
  - protokoły sieciowe
  - IPv6
- Researcher
- Zadeklarowany Whitehat
- Absolwent PUT i PUE
- Członek ISSA / ISSA Polska

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Cel wykładu

- **Uwrażliwić**
  - **zagrożeń jest bardzo dużo**
- **Uspokoić**
  - **większość z nas nie jest atrakcyjnym celem**
  - **ale automaty nie wybierają - botnety**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Koszty cyberprzestępczości

Źródło: Norton (2011)

Cele ataków / motywacja

- Kradzież pieniędzy / wyłudzenia – zorganizowane grupy
- Szpiegostwo polityczne i przemysłowe
- Terroryzm / sabotaż
- Kradzież tożsamości
- Rozsyłanie SPAM
- „Hacktivism”
- Zabawa

Ygnacio Valley Road in Concord ->

Skala

- **Case: Estońska grupa przestępcza**
  - Operacja „Ghost Click” (FBI, Estońska Policja i inni)
  - 14M $
  - DNS-rerouting
  - Reklamy (!!!)

- **Case: „Trident Tribunal”**
  - Scareware
  - Ukraina, Niemcy, Litwa, Cypr (centrala w Kijowie)
  - 72M $

Skala malware

„Every minute, 232 computers are infected by malware."

Źródło: RSA
(http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

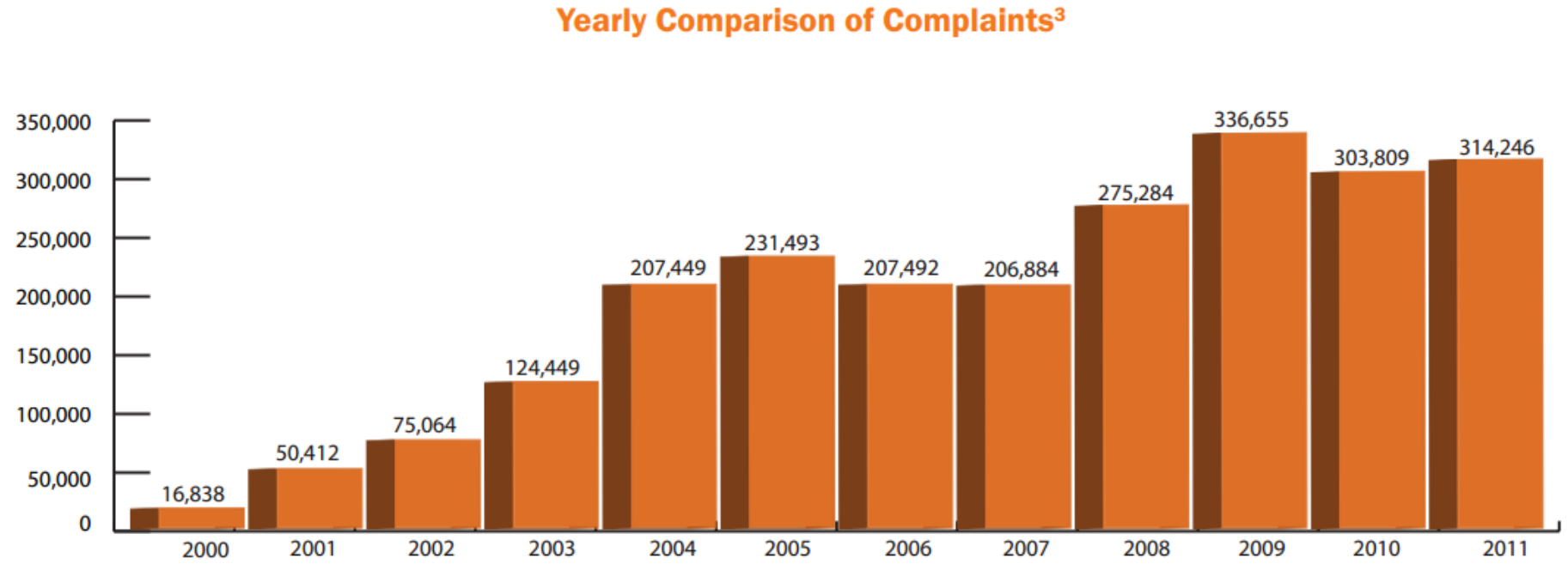
Cennik malware

- Zeus -> 10.000 $
  - Potem cena spadła do 600 $
- SpyEye -> 4.000 $
  - Potem … 2 za 380 $ (custom recompile)
- Handel podatnościami
  - Disclosure

Źródło: RSA (http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zgłoszenia (źródło IC3, FBI)



[1]Methodology of evaluating loss amounts: FBI IC3 Unit staff reviewed for validity all complaints that reported a loss of more than $100,000. Analysts also converted losses reported in foreign currencies to dollars. The final amounts of all reported losses above $100,000 for which the complaint information did not support the loss amount were excluded from the statistics.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Kto jest celem?

Ataki dedykowane

- **Banki**
- **Instytucje finansowe, ubezpieczeniowe**
- **Bazy danych medycznych**
- **Duże portale**
- **Kraje (i ich instalacje SCADA)**
- **Osoby publiczne**

Ataki automatyczne

- **Małe e-commerce, mało znaczące serwery**
- **Osoby indywidualne**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Kto jest celem?

Czasami przestępcy nie mają pojęcia na co się włamali…

Hakerzy nie są nieomylni ☺

- Case: Georbot Botnet (390 komputerów, szpiegostwo)
- Gruzja (Gregorian CERT)

Źródło: http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf

Ryzyko

- **Modelowanie**
- **Analiza**

Modelowanie ryzyka

STRIDE (Microsoft™)

- **S**poofing (Authentication)
- **T**ampering (Integrity)
- **R**epudiation (Non-repudiation)
- **I**nformation disclosure (Confidentiality)
- **D**enial of Service (Availability)
- **E**levation of privilege (Authorization)

Odpowiadamy na pytanie: Przed czym się chcemy zabezpieczyć?

Modelowanie ryzyka

Podejścia do modelowania

- Z perspektywy hakera
  - Atakujący chce przejąć konto administratora na serwerze
- Z perspektywy oprogramowania
  - Analizujemy model systemu i rozważamy ryzyka dla poszczególnych komponentów
- Z perspektywy zasobów
  - Baza danych medycznych

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Analiza ryzyka

$$\text{RYZYKO} = \frac{\text{Potencjał luki}}{\text{Trudność ataku}}$$

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Analiza ryzyka

DREAD (Microsoft™)

- **Da**mage
- **R**eliability
- **E**xploitability
- **A**ffected users
- **D**iscoverability

Numeryczne wartości, np. 3 wysokie ryzyko, 2 średnie, 1 niskie, 0 żadne – na podstawie indywidualnych wartości, możemy ocenić dane ryzyko całościowo i ilościowo

Np. **Severity = f(Da, R, A)**

CVSS

- **Common Vulnerability Scoring System (v2)**
  - Base score
  - Environmental score – umieśćmy podatność w kontekście
  - Temporal score – na jakim etapie jest proces związany z tą luką?
- **Wektor przeliczany jest na wartość liczbową**
  - **0.0 -> 10.0**
- **Wartość liczbowa, może być przekształcona w poziom ryzyka**
  - **0.0 <= Niskie ryzyko < 4.0**
  - **4.0 <= Średnie ryzyko < 7.0**
  - **7.0 <= Wysokie ryzyko <= 10.0**

http://nvd.nist.gov/cvss.cfm?calculator&version=2

CVSS - przykład

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2969

The SSL/TLS server implementation in OpenSSL 0.9.7 before 0.9.7h and 0.9.8 before 0.9.8a, when using the SSL_OP_MSIE_SSLV2_RSA_PADDING option, disables a verification step that is required for preventing protocol version rollback attacks, which allows remote attackers to force a client and server to use a weaker protocol than needed via a man-in-the-middle attack.

CVSS - przykład

Impact

CVSS Severity (version 2.0 incomplete approximation):

CVSS v2 Base Score: 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:P/A:N) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized modification

Przyczyny problemów

- **W jaki sposób dochodzi do włamania?**

Błędy w oprogramowaniu

- Systemy operacyjne
  - Aktualizacje SĄ WAŻNE
- Usługi sieciowe
  - Aktualizacje SĄ WAŻNE
- Dedykowane oprogramowanie (!!!)
  - Architektura
  - Komponenty / frameworki
  - Logika biznesowa
  - „Can we fix it with SSL?” ☺

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Cloud

- Buzz-word, ale…

- Gdzie są dane?
- Kto ma dostęp?
- Jak wygląda replikacja?
- Jak wygląda izolacja?
- Co się dzieje z danymi po skasowaniu VM?
- Panele administracyjne
- Aktualizacje VM

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

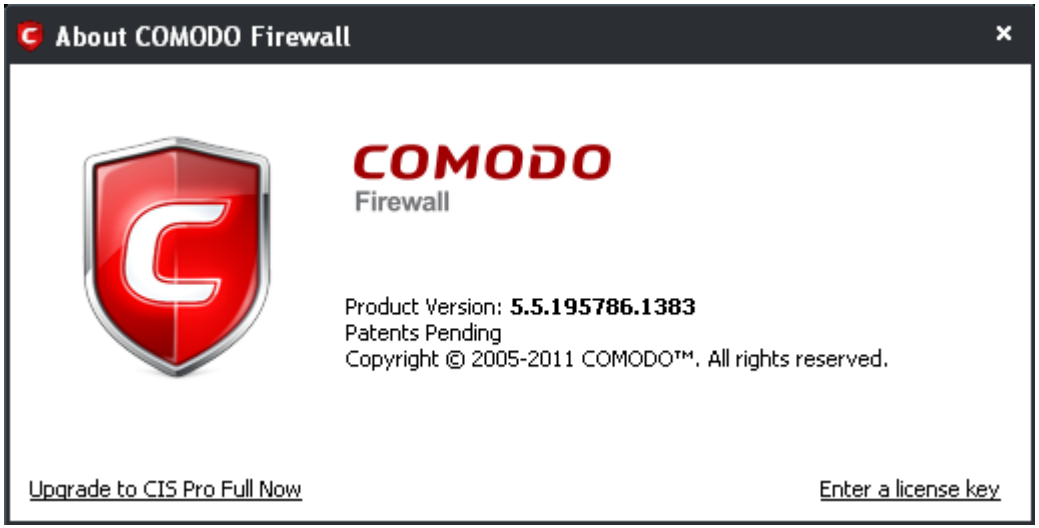
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Konfiguracja

- **Domyślne ustawienia**
  - Co raz częściej są bezpieczne
  - Ale admini je zmieniają na mniej bezpieczne…
- **Wyłączanie zabezpieczeń, żeby coś zadziałało (!!!)**
  - Również na poziomie oprogramowania
- **Urządzenia sieciowe**
  - IPv6

Konfiguracja - przykład

- **Domyślny „Safe Mode”**



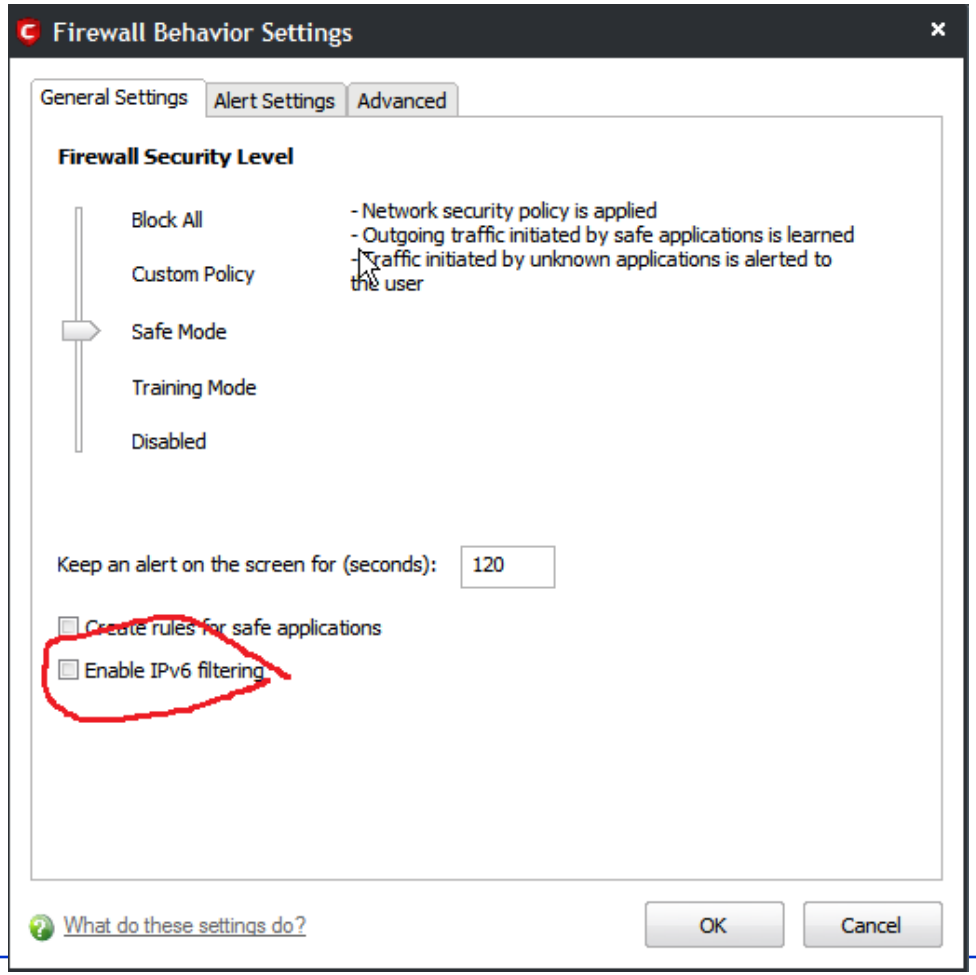
Konfiguracja - przykład

```
pingwin@holmes:~$ nmap -PN 10.50.1.2
Starting Nmap 5.00 ( http://nmap.org ) at 2011-07-29
   18:50 CEST
All 1000 scanned ports on 10.50.1.2 are filtered
```

Konfiguracja - przykład

```
pingwin@holmes:~$ nmap -6
   fe80::29e3:a36e:8470:4311%eth0
Starting Nmap 5.00 ( http://nmap.org ) at 2011-07-29
   18:50 CEST
Interesting ports on fe80::29e3:a36e:8470:4311:
   Not shown: 992 closed ports
   PORT      STATE SERVICE
   135/tcp   open  msrpc
   445/tcp   open  microsoft-ds
   3389/tcp  open  ms-term-serv
   49152/tcp open  unknown
   49153/tcp open  unknown
   49154/tcp open  unknown
   49156/tcp open  unknown
   49157/tcp open  unknown
```

Konfiguracja - przykład



Programowanie – Cykl życia

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Programowanie

- **Programiści działają pod presją**
  - Czas
  - Funkcjonalność
  - …
  - …
  - Bezpieczeństwo
- **Programiści wyważają otwarte drzwi**
- **I sami „wyłączają alarmy”**

Programowanie

Uczmy się od najlepszych:

JOINT STRIKE FIGHTER AIR VEHICLE
C++ CODING STANDARDS

by LockheedMartin

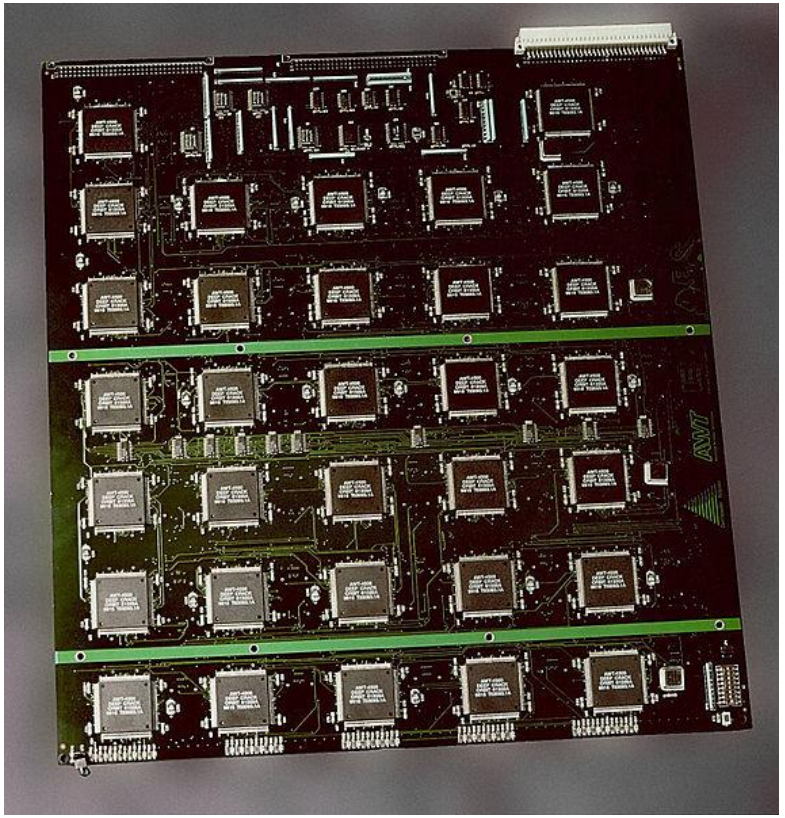
„Approved for public release; distribution is unlimited.”

Programowanie

- Często planowane są jedynie testy funkcjonalne
  - Testy obciążenia?
  - Testy bezpieczeństwa?

Programowanie - szyfrowanie

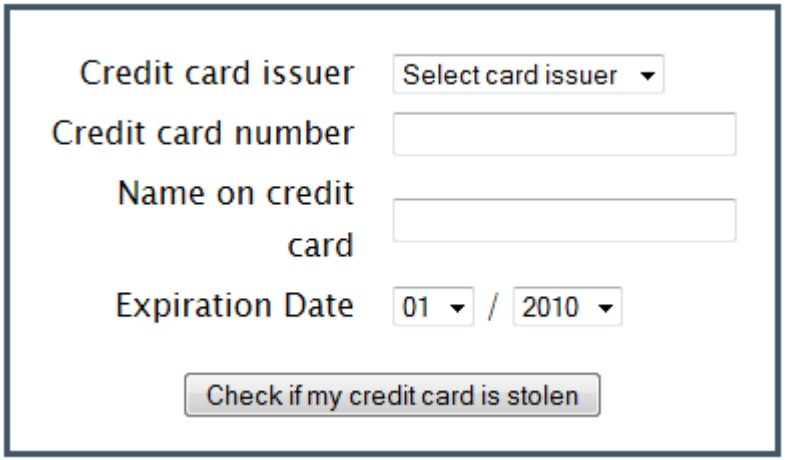
- Często używane bez zrozumienia
- Case: DES (56bit)

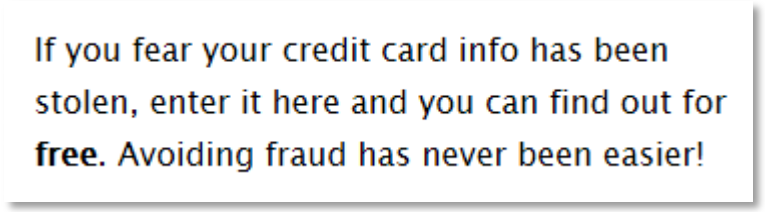


- DES cracker
- Deep Crack chips

Czynnik ludzki

Problem często znajduje się między krzesłem a klawiaturą.



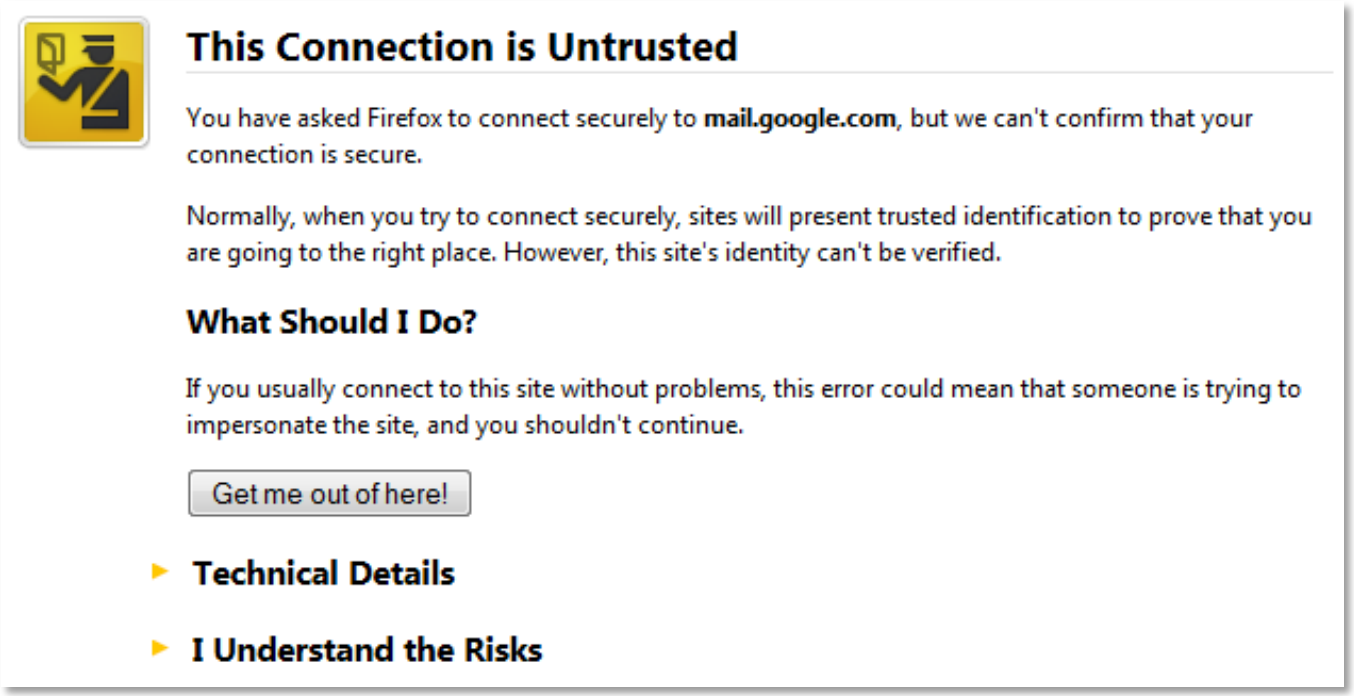


http://ismycreditcardstolen.com/

➲ przykładowa strona edukacyjna (to raczej nie są oszuści)

Czynnik ludzki

- **SSL/TLS man in the middle attack**

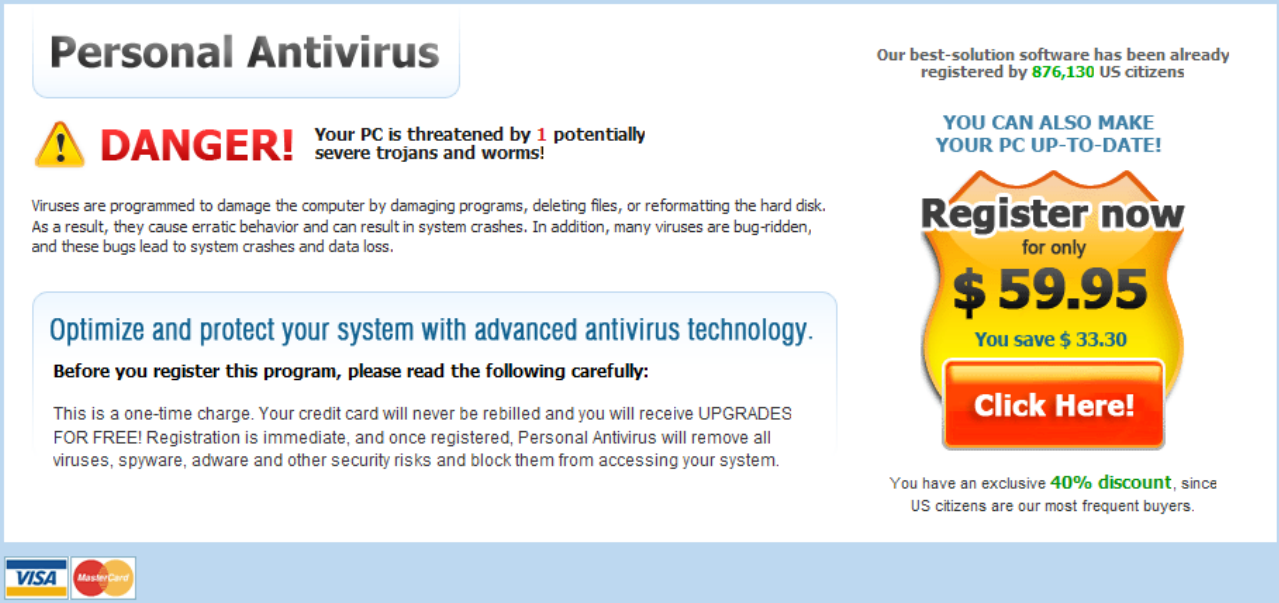


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Scareware



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

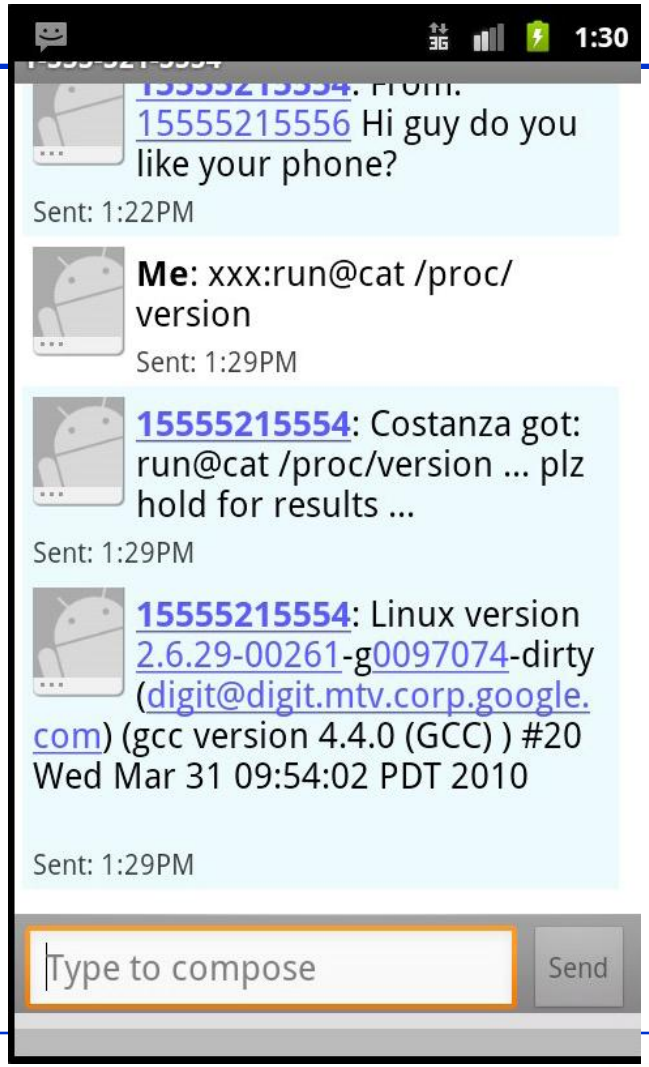
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Aplikacje mobilne

Platformy

- iOS (Apple™)
- Android (Google™)
- Windows (Microsoft™)

Smartfony to już w pełni funkcjonalne komputery.



Źródło: Bas Alberts & Massimiliano Oldani Immunity Inc.

Juice jacking

Źródło: http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Testowanie

- **W jaki sposób przeprowadzamy testy?**

Etyka i prawo

- **Zawsze, bezwzględnie, wszelkie testy bezpieczeństwa należy przeprowadzać za zgodą i wiedzą administratora testowanego systemu.**
- **Inaczej…**

- **To bardzo ważne, cześć administratorów nie ma poczucia humoru!**

Metodologie

- Pentest vs. Security assessment
- Black box vs. Gray box vs. White box

Wykrywanie podatności

- **Discovery** – odkrywanie hostów, usług i zasobów
- **Exploration** – wykrywanie podatności
- **Exploitation** – wykorzystywanie podatności
- **Reporting** – raportowanie wykonanej pracy
- **Mitigation** – łatanie i poprawianie systemów
- **Retest** – sprawdzanie efektywności wprowadzonych poprawek

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Discovery

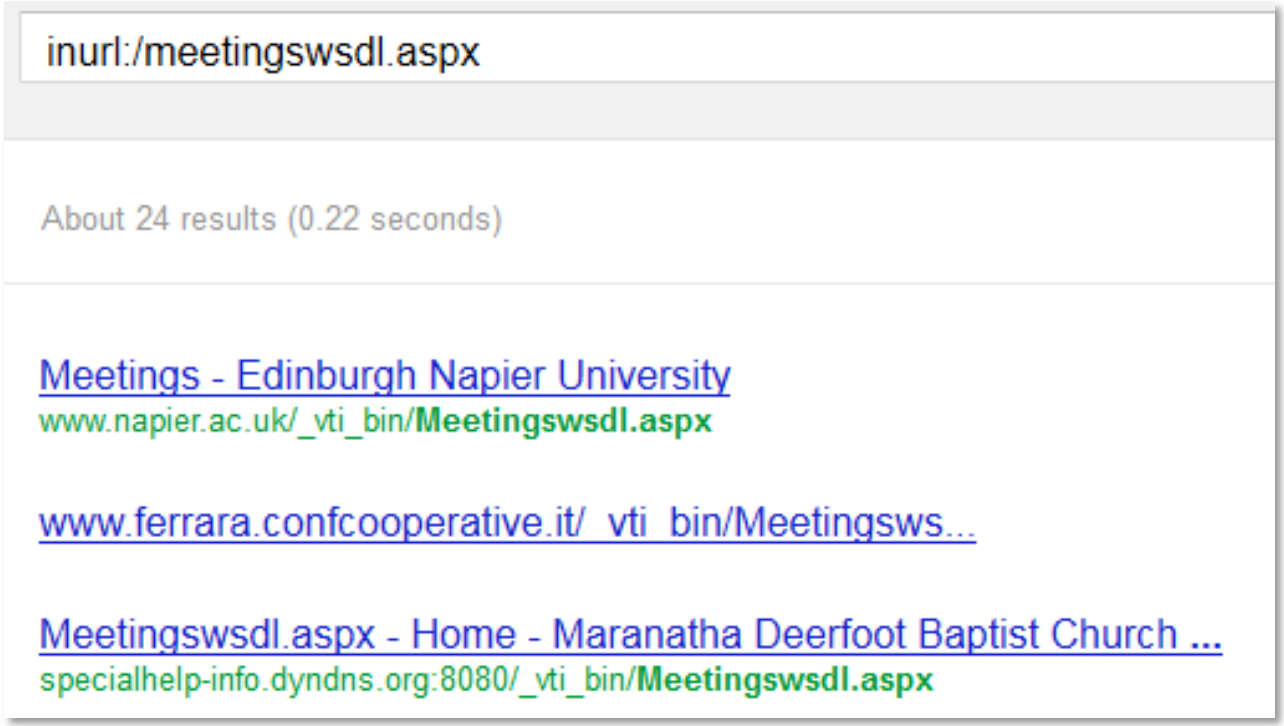
- **Skanowanie sieci**
  - IPv6
  - Port scanner
  - Wifi scanner
- **Wykrywanie usług, domen, hostów wirtualnych**
- **W ramach aplikacji, wykrywanie ukrytych zasobów**
  - Bruteforcing
- **Mapowanie zależności między organizacjami, zasobami i modułami**

Discovery

- Google™ and others are your friend!

inurl - przykład

- Microsoft™ Sharepoint – niegroźny przykład



Exploration

- **Wyszukujemy podatności, które można zaatakować**
  - **Skanery** (web aplikacji, systemowe, specjalistyczne)
  - **Manualne testy**
  - **Brute-forcery**
  - **Sniffing** – podsłuchiwanie ruchu
  - **Spoofing** – podszywanie się (pod innego hosta)
  - **Fuzzing** – generowanie modyfikacji na wejściu systemu

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Exploitation

- Używamy gotowych exploit'ów
- Piszemy sami narzędzia do symulacji ataku
- Łamiemy zgromadzone password hashes
- Próbujemy ataków DoS

- Warsztat jest nieograniczony, a w tej pracy najważniejsza jest kreatywność

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

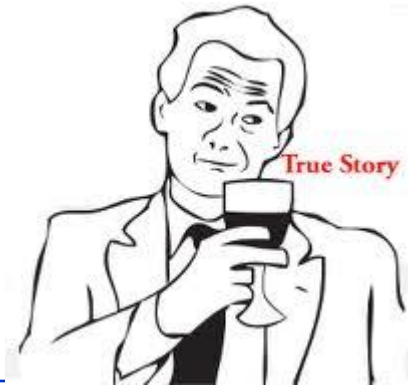
Case #1 (WordPress)

Aplikacja webowa

1. Instalacja WordPress... nieaktualna
2. Moduł XMLRPC zawiera znany SQL injection
3. Dostęp do bazy danych -> pobrałem hasze haseł (bez soli)
4. Mamy w biurze potężną maszynę do łamania haseł, ale...
5. Googled it first ☺ -> hasło administratora to: 5am5un6

Główna przyczyna (PHP):

- $max_results = $args[4]; <- część zapytania SQL
- $max_results = (int) $args[4]; <- rozwiązanie!



Case #2 (Sklep internetowy)

Sklep internetowy (duuuży)

1. PHP
2. Funkcjonalność weryfikacji człowieka (CAPTCHA) – wymagał podania równania spełniającego podaną zależność
3. Wpisana wartość jest przekazywana do PHP dla oceny bez żadnej walidacji, można było wykonać dowolny kod!
4. ... odnalazłem i pobrałem plik konfiguracyjny DB ☺
5. DB odsłonięta <- jeszcze łatwiej – wystarczy się połączyć ulubionym klientem MySQL
6. Uzyskałem dostęp do, między innymi,

   pełnych danych 40k klientów

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Incident Response

- **Najważniejsze to wykryć incydent**
  - Szkolenie i podnoszenie świadomości
- **… i odpowiednio zareagować**
  - Każda większa organizacja powinna mieć plan działania
- **Incident Response vs. Forensics**

„Nie mieliśmy nigdy incydentu bezpieczeństwa."

vs.

„Nie macie świadomości, czy mieliście kiedyś incydent…"

Podsumowanie

- Zagrożeń jest dużo i będzie ich coraz więcej
- Najważniejsza jest świadomość
- Używajmy dobrze sprawdzonych mechanizmów
- Żaden system nie jest bezpieczny raz na zawsze
- Analiza i modelowanie ryzyka są ważne
- Bezpieczeństwo IT to proces
- Wiedza hakerska jest niebezpieczna – ETYKA!

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Kolejny wykład

- **Bardziej szczegółowo o bezpieczeństwie:**
  - **Aplikacji internetowych**
  - **Aplikacji i platform mobilnych**

- **27/11/2012**

Źródło: Nitesh Dhanjani
Blackhat Barcelona 2011

Pytania

?