NÁDOR RENDSZERHÁZ

Információbiztonsági kihívások

Horváth Tamás & Dellei László

2010. 11. 23.

Miről lesz szó

- Bemutatkozás
- Aktualitások, veszélyek az IT biztonság területén
- Megoldások

- Elő bemutató – WIFI Hack

Nádor Rendszerház Kft.

MINŐSÉGI ESZKÖZÖK

PROFESSZIONÁLIS SZOLGÁLTATÁSOK

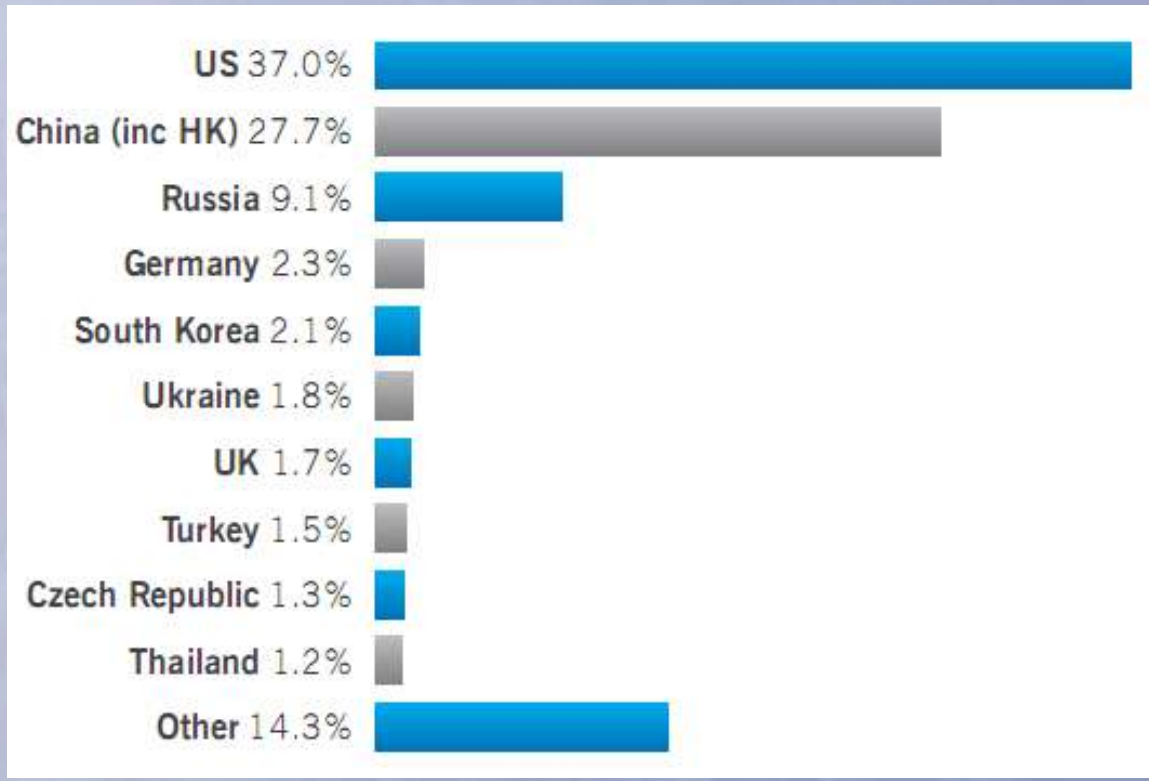
- Informatika
- IT Biztonság
- Távközlés
- Vonalkódtechnika és RFID
- Irodatechnika
- Szerviz szolgáltatások

…1992 óta

Múlt – 2008 veszélyforrások

Web fenyegetések

- Oldal törések, fertőzések (Euro 2008, Wimbledon)
- SQL Injection
- Search engines – kihasználható sérülékenységeket tartalmazó web oldalak keresésére írt program, kártékony kód elhelyezése a szerveren. Automatizált.
- Anonymizing proxy



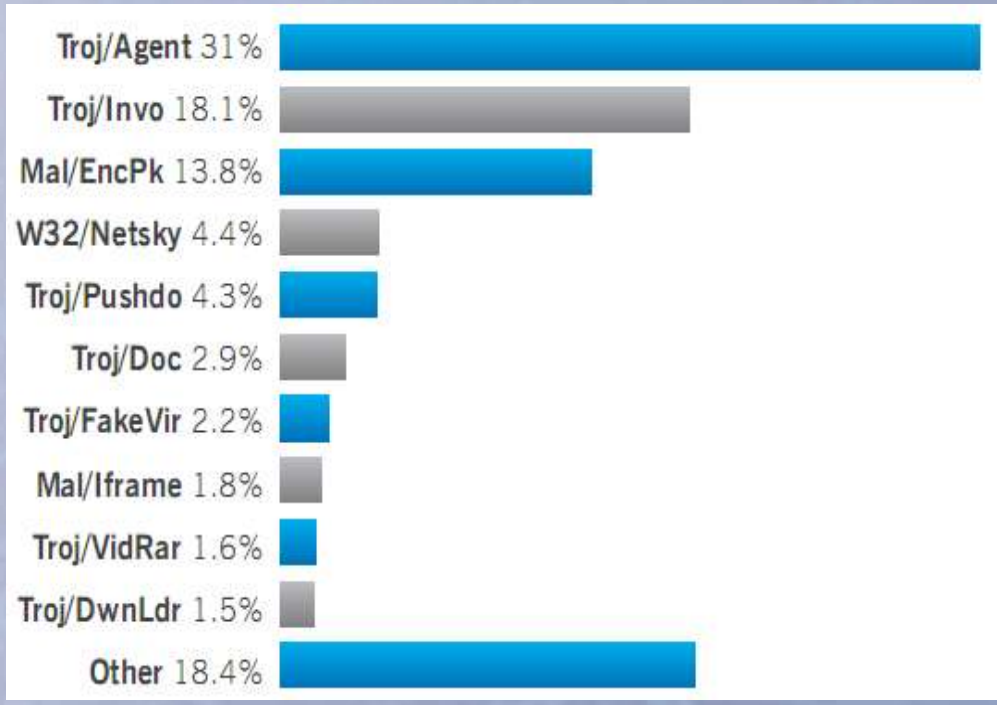
Múlt – 2008 veszélyforrások

Email fenyegetések

- csatolmányok növekedése
- kártékony linkek

Malware kódok

- Cél: azonosság lopás, pénzszerzés,
- kínai (backdoor, jelszó lopás online játékokon keresztül,), brazil (trójai, banki információk), orosz (botnet, backdoor, internetes bűnözés)
- Pop-up alkalmazások
- Ingyenes „anti-spyware" programok megjelenése
- Adobe PDF exploit-ok megjelenés



Múlt – 2008 veszélyforrások

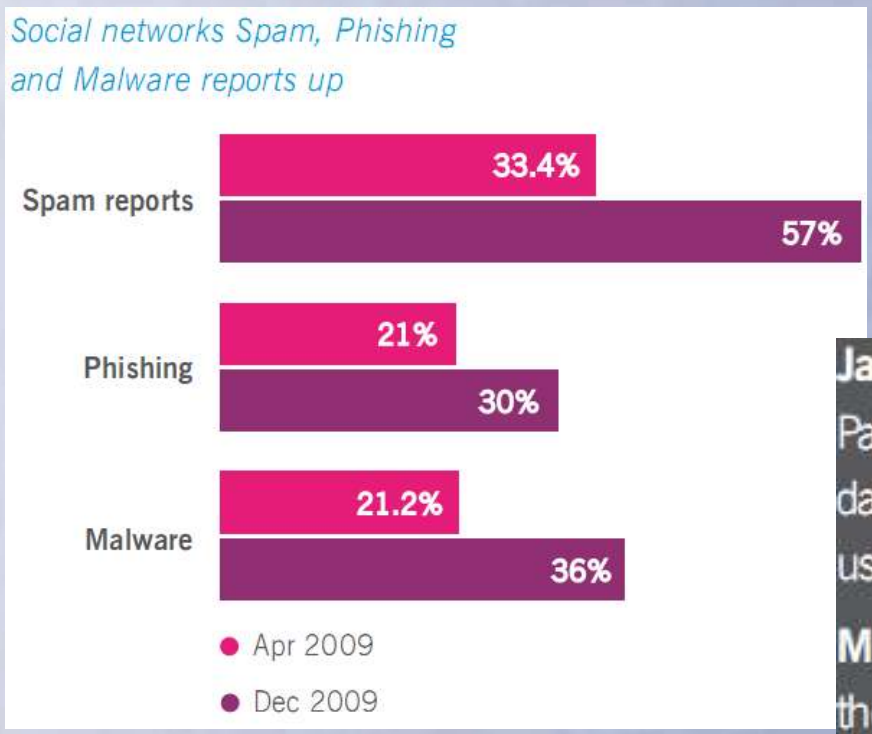
Spam-ek

- Levelek mellet megjelent a blog spam és a társasági oldalakon terjedő spam-ek

Operációs rendszerek

- Mac OS X kártékony kódok (backdoor)
- Mobil készülékek

Múlt – 2009 veszélyforrások



Társasági oldalak

- Céges blog bejegyzések,
- Spam-ek, malware-ek,
- Fertőzött web oldalak
- Adatlopás, teljesítmény csökkenés

Adatszivárgás

- Személyes adatok
- Felhasználók adatai
- Pénzügyi adatok

January 2009: Networks at Heartland Payment Systems are hacked, exposing data on 130,000,000 credit card users.[34]

May 2009: Secret information on the Joint Strike Fighter and President Obama's personal helicopter were leaked through P2P networks.

October 2009: Hard drives sent for repair are found to contain data on 76 million US Army veterans.

Múlt – 2009 veszélyforrások

Web oldalak sérülékenységei

- SQL injection
- Reklámok -> kártékony kód, oldal támadás és fertőzés (New York Times, Gizmodo)
- Nagykövetségi honlapok pl: Azerbajdzsán magyarországi nagykövetsége
- FTP login -> iFrame, PHP kód feltöltés

Spam-ek

- Újjáéledés történt, csatolmányokban kártékony kódok terjesztése
- 2 nagy botnet hálózat megszűnt, helyettük Webmail email címekről

	Total	Day	Hour
Blocked	10,337,837	4,198	678
Blocked: Virus	32,035	10	0
Rate Controlled	46,441	39	0
Quarantined	49,960	8	1
Allowed: Tagged	37,399	4	3
Allowed	939,685	95	8
Total Received	11,443,357	4,354	690

Múlt – 2009 veszélyforrások

Malware

- Web oldalak
- Hamis AV vagy Scareware
- Adobe PDF
- Conficker (MS08-067)
- Társasági hálózatok
- 50 000 új malware

Troj/Bredo 42.8%

Timeline of Mac malware 2009

Malware targeting Macs discovered during 2009 included:

January: The OSX/iWorkS family of Trojans, which posed as pirated copies of Apple's iWork [101] and Adobe's Photoshop CS4[102]

March: OSX/RSPlug-F, again posing as hacked/cracked files[103] using social engineering to get users to install it[104]

May: OSX/Tored, an email worm claiming to be building the first Mac OS X Botnet[105]

June: Trojans posing as ActiveX components required to view pornographic videos[106]

June: Links sent via Twitter leading to a supposed sex tape featuring TV star Leighton Meester, actually Trojan OSX/Jahlav-C[107]

July: OSX/Jahlav-C again, this time placed on sites created to take advantage of widespread rumors of a peephole video featuring ESPN TV reporter Erin Andrews[108]

August: OSX/Jahlav-C returns, disguised as an installer for MacCinema software[109]

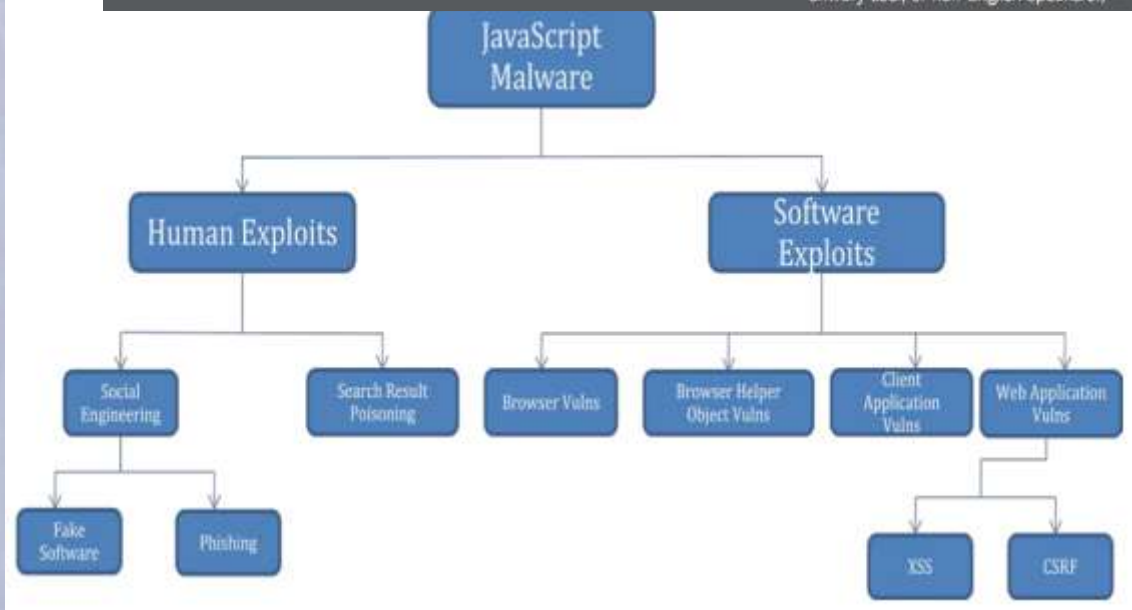
August: OSX/Jahlav-C once more, this time hooking on Twilight movie star Ashley Greene and posing as QuickTime updates[110]

November: OSX/LoseGame-A, a bizarre example of malware that posed as an old-fashioned Space Invaders game and openly deletes users' files (It is not exactly a Trojan as it is open about its intentions, but nevertheless is a hazard to the unwary user, or non-English speakers.)[111]

Operációs rendszerek

- Windows 7 : számos biztonsági újítás
- Mac – növekvő malware szám

SEO poisoning



Jelen – 2010 veszélyforrások

- **2010 január IPv6 protokollt használták a levelek terjesztésére**
- **Sebezhetőségek:**
  - Adobe termékek (PDF Reader, Flash)
  - Windows termékek (OS, Office, Internet Explorer)
  - Egyéb böngészők (Firefox, Opera)
  - Google termékek (Chrome OS, Wave, böngésző)
  - Mobiltelefon operációs rendszerek
- **Közösségi portálok: Twitter, Facebook**
- **Fájlcserélők**
- **Botnet hálózatok (Afrika)**

Jövő – 2011 veszélyforrások

- **Mobil fenyegetettségek egyre nőnek**
  - 2011-re minden elemzés kiemelt veszélyként említi
- **Különböző Kormányok által támogatott hacker támadások:**
  - Nem a pénzügyi haszonszerzés, hanem kritikus infrastruktúrák fölötti irányítás megszerzése a cél.
  - Például: Stuxnet
- **Belső dolgozó:** adatlopás, kiszivárogtatás
- **Man in the Browser attack:** az online alkalmazások terjedésével nő , site-to-client authentikációval lehet kivédeni

Jövő – 2011 veszélyforrások folyt.

- Közösségi portálok: Twitter, Facebook – 2011-ben is!
- Adatszivárgás
- Az adatbiztonság a ködbe megy…
- A biztonság üzleti folyamattá válik
- Az adatvédelmi előírások szigorodnak, konszolidálódnak

IT Security portfólió

- CenterTools (DriveLock), Sophos – adatvédelem
- Safenet (Aladdin) – felhasználó azonosítás
- Barracuda – spam, webszűrés, web védelem, levelezés archiválás
- Omnikey – kártyaolvasók
- Precise Biometrics – ujjlenyomat olvasók
- Watchguard, Juniper, Cisco, Zorp - tűzfalak
- Avira, McAfee, Symantec - vírusvédelem

IT Security Portfólió

Folyt.

- IBM ISS – sérülékenység vizsgáló eszköz, IPS
- Sophos, DriveLock – végponti védelem
- WatchGuard – UTM eszközök
- Barracuda - Phion – tűzfalak, VPN megoldások
- IBM Security megoldások (Tivoli)
- RSA – logelemzés
- Secuvoice - lehallgatás biztos mobilkommunikáció

Jelen – IT Security KSzF-ben

KSzF keretmegállapodás alapján elérhető gyártók és megoldásaik

- Sophos
- McAfee
- Barracuda
- WatchGuard
- CheckPoint
- Aladdin

SOPHOS

McAfee

BARRACUDA NETWORKS

WatchGuard

Check Point SOFTWARE TECHNOLOGIES LTD.

Aladdin SECURING THE GLOBAL VILLAGE

Válaszaink

- **IT Audit - helyzetkép felmérés, kockázatfelmérés**
- **Informatikai Biztonsági Menedzsment Rendszer (IBMR) kidolgozása, bevezetése, működtetése.**
  - (többek között a Szabályzati rend kidolgozásával)
- **Sérülékenység elemzés,** Ethical hacking
- **Adatszivárgás elleni védelem** – Sophos, McAfee, DriveLock
- **Naplóelemzés** – szolgáltatás és termék
- Social Engineering – IT Biztonsági tudatosság növelő oktatás

Válaszaink

- Szektor, Fájl szintű titkosítás, mobil adathordozók védelme, biztonságos fájl továbbítás, fájl szerveren tárolt adatok titkosítása. – Utimaco, DriveLock termékcsalád
- Spam, vírus – Barracuda Spamfilter
- Malware, Ad-aware – Aladdin eSafe, Barracuda Webfilter

Köszönjük a figyelmet!

Horváth Tamás
IT Biztonságtechnikai tanácsadó

Dellei László
IT Biztonságtechnikai tanácsadó

Nádor Rendszerház Kft
1141 Budapest, Öv utca 3.
Tel: 470-5000/174
Mobil: +36(20)991-1614
Fax:+36(1) 470-5011
http://www.nador.hu