Török Szilárd

NISZ IT biztonsági igazgató, NKE doktorandusz

Miért nem sikerül a magyar Anonymousna

nonymous a világban

chan.org

2003 őszén indult 4chan.org fotóalapú csevegő-oldal volt az inkubátoruk

Anonymous-ként lehetett hozzászólni, netes tréfák, átverések és hecckampányok verbuváltak itt „troll-hadsereget”

2003-tól EPIC FAIL (lefordítva: óriási pofára esés) és Guy Fawkes figura

V, mint vérbosszú című 2006-os sci-finek köszönhetik a maszkot, mint az összetartozás és anonimitás szimbólumát (filmben diktatúrát leverő forradalom kirobbantójaként jelent meg)

Miért november 5. a születésnapjuk? Angliában ekkor szokásos tűzijátékkal és bábuégetéssel emlékezni a legnevezetesebb balekra - 1605-ben anonim levél által bukott le.

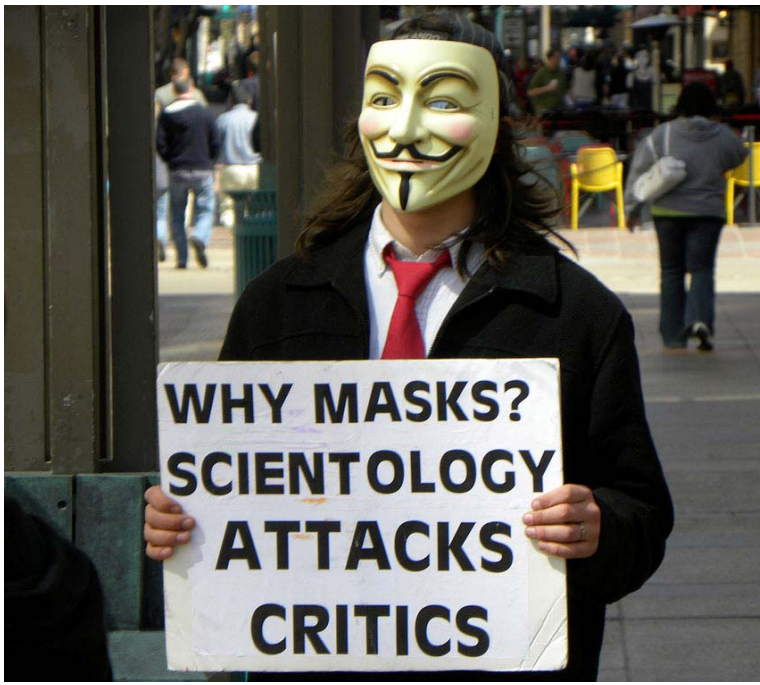
nonymous versus Szcientológia Egyház

2008-ban a Szcientológia egyház ellen kezdődött el a szerveződés

2008-tól elektronikus tiltakozás - internet támadásokat is felhasználásának

iért terjedt el a maszk 2008-tól?

cientológia egyház „belső rendőrsége” az egyház ellen rdult ex tagokat felkutatja, akár zsarolhatja…



„Fantasy uniforms were used to p and protest the uniform obsessed

ontosabb fogalmak

Hacker

Cracker

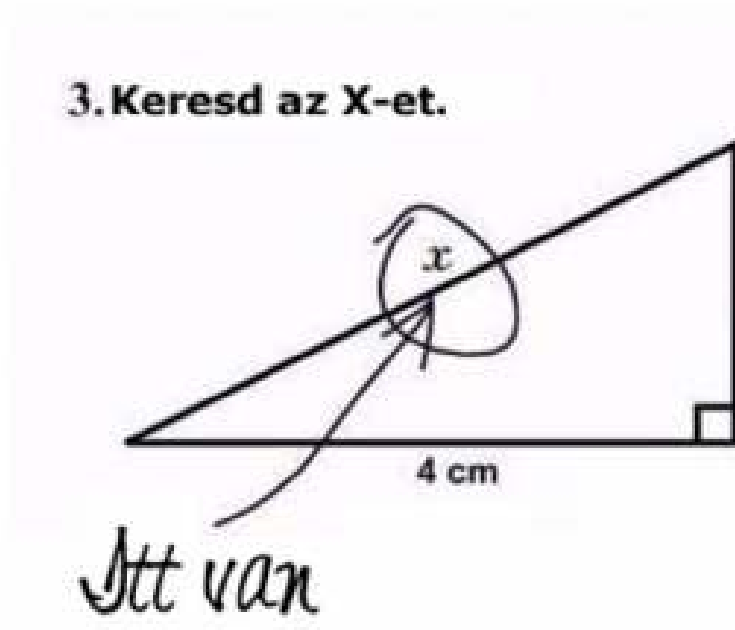
Legal Hack

Etikus Hack

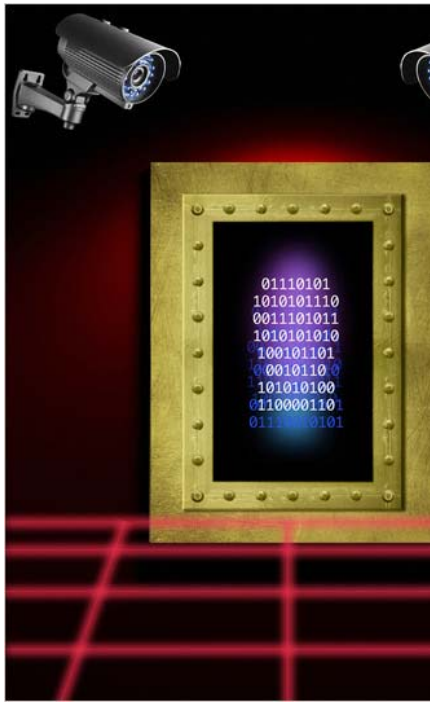
Penetration Test

Hacker aktivista - hacktivista

Anonymous és Lulz



zai kiber-történelem



3: szoftver feltörések, átalakítások és illegális solások

3-1997: internettel együtt megjelentek a betörési érletek. Jelentősebb hazai esetek: NASA, Soros pítvány / C3.hu, Kormányzati tűzfalrendszeren át harcok egyetemi hálózatokért, végtelen telefonkártyák és más piltrükkök

7: Cyber kultúra és harcosai a Telko ellen fordultak, fibb módszerek használata - vezetékes és Mobil hack: e" hívás/hangposta, világkártya, stb.

8: DLP/adatszivárgások kezdete, ATM és banki adások

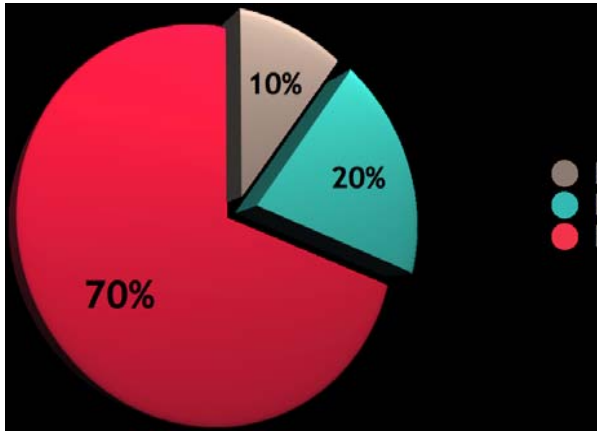
9: Magyarországon az első Legal Hacker szolgáltatás. ges cyber harcok: Index vs Internetto. Komolyabb kdoor-ok, trójaik nagy cégeknél, álbetörések

0-2002: Megjelentek az első komolyabb ipari nkedések IT segítséggel - synergon.hu, tőzsdei dszerek 1 óra alatt feltörhetők, legnagyobb hazai bank

azai tapasztalatok (anonimizálva)

- Banki rendszerek
- Egészségügy
- Fővárosi tulajdonú cégek
- SCADA
- Közlekedési rendszerek
- Országos nyilvántartás
- Digitális aláírás alapú biztosítói rendszer

...



OWASP TOP 10 alapú vizs
eredménye

éz dolga lehet az Anonymousnak?

ük meg a mobilparkolást!

szám (+36xxxxxxxxx):

Belépési kód: OK

WP

Belépési kód: ie12l OK

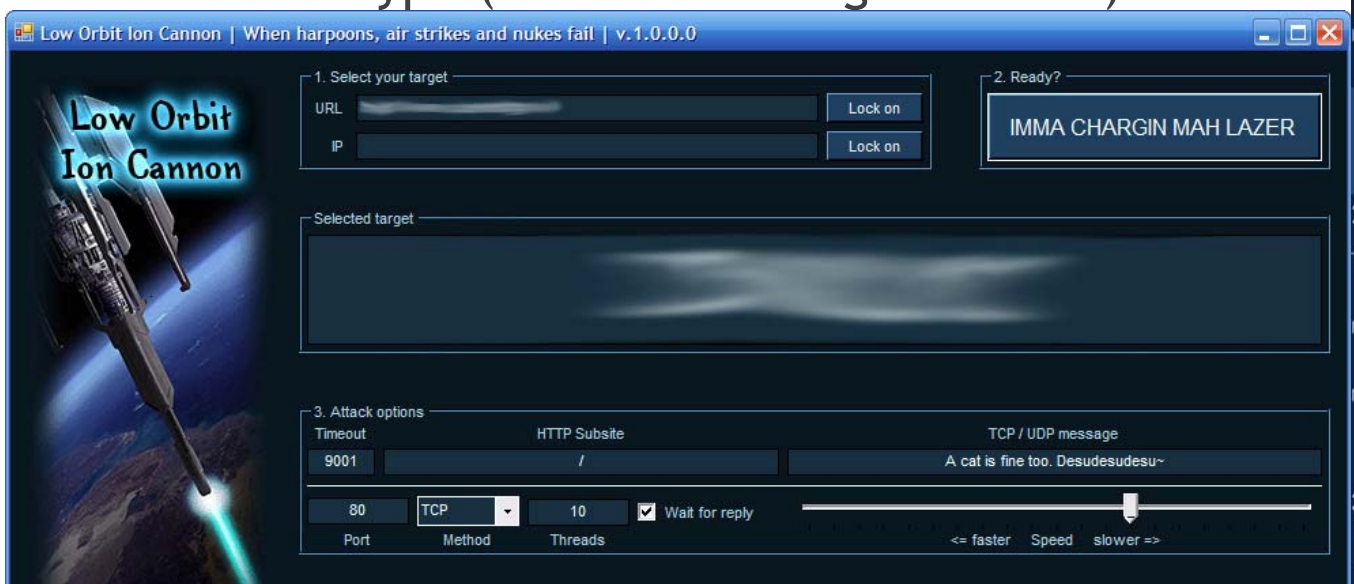
```
ml><title>SMS-szimuláció</title><link href="style.css" rel="stylesheet"
e="text/css"><script src="functions.js"></script><body marginwidth="8"
ginheight="0"> A belépési kódját elküldtük sms-ben. <br>
rm name="megerosites" id="megerosites" method="post">          Belépési kód:
 <input type="Password" name="kod" id="kod" class="text" maxlength="10">
      <input type="Hidden" name="mit" id="mit" value="1">        <input
e="Hidden" name="kod_generalt" id="kod_generalt" value="ie12l">      <input
e="Submit" name="mehet" id="mehet" value="OK" class="button"></form><br>
rm name="form_kilep" id="form_kilep" method="post">  <input type="Hidden"
ne="kilep" id="kilep" value="Kilépés" class="text">          <input type="Button"
ne="kilep_gomb" id="kilep_gomb" value="Kilépés" class="button" onclick="javascri
```

nonymous, Maszkok és az ACTA

agyar Anonymous tevékenységek

ső „tavaszi” hullám 2012.01 - 2012.04.

egjelenés felület:	Twitter, YouTube, Facebook
enyegetés publikálva:	PasteBin és YouTube ((2012.01.13 kezdettel)
zerveződés:	2011. decemberétől, ACTA tüntetésre készülve
valitás / késztetés:	7 / 5 (10-es skálán)
élpont kiválasztás:	spontán, 1-2 nappal előtte
tenzitás:	1-2 hetes intervallumok jellemzőek
él tech.felderítése:	nem ismert, esetenként nem jellemző a felderítés
ejtőzés:	álnevek, anon proxy
nline kommunikáció:	Skype (csak a zárt mag esetében)



agyar Anonymous tevékenységek

ső „tavaszi” hullám célpontjai

012.02.14: DDoS: hoffmanrozsa.hu, hamisitasellen.hu
kormany.hu (külföldi jelenléttel)
012.02.21. ügyfélkapu, MTVA, Artisjus (legtöbb résztvevő)
012.02.25. Deface: Ifjúsági KDNP (csak 1 Anon tag)
012.03.02. XSS: magyarorszag.hu
012.03.04. Deface: Alkotmány Bíróság (valószínű 1 személyes művelet)
012.03.16. DDoS: monsanto.hu (sikeres), kormany.hu
012.03.28 Deface: NRSZH, Leaking: PTF DB
012.03.30. Leak: zsaru.hu DB, Deface: Katolikus Püspöki Kar
DDoS: KEH.hu
012.04.20. *DDoS: szélsőjobb*
012.04.24. Jobbiktól adatokat kiloptak

agyar Anonymous tevékenységek

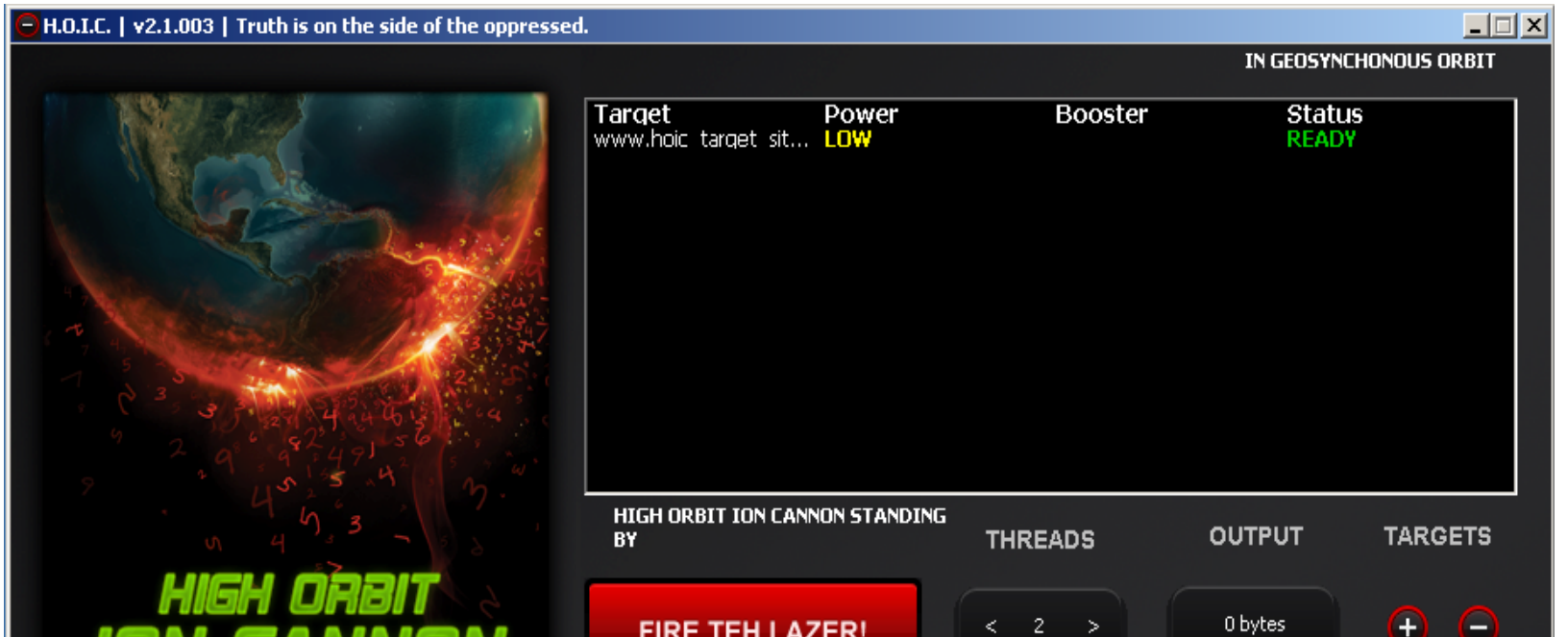
ásodik „őszi” hullám: 2012. augusztustól

egjelenés:	Facebook
enyegetés módjai:	PasteBin és YouTube ((2012.01.13 kezdettel)
zerveződés:	ACTA tüntetés előtt és azzal összhangban
valitás / késztetés:	4 / 7 (10-es skálán)
élpont kiválasztás:	szervezettebb (bár nincs összehangolt előkészület)
tenzitás:	2-3 naponta
ülföldi támogatás:	előfordul, főleg olasz Anonymous tagok
elderítésük:	fejlettebb (jóval hamarabb ismertek a célpontok)
elderítés eszközei:	nyíltforrás: nmap, havij, nessus; zárt: Acunetix WVS
nline kommunikáció:	Skype (csak a zárt mag esetében), IRC
ejtőzés:	álnevek, Open Proxy, VPN, TOR
ámadó eszközök:	L.O.I.C. (Orbit Ion Cannon + mobil verziója) UDP, TCP SYN és HTTP flood H.O.I.C. (High Orbit Ion Cannon, valódi alkalmazás szintű DoS eszköz, nehezebb tűzfalazni, Booster VB scriptekkel bővíthető) Sloworis/pyloris (HTTP Partial Request Attack)

agyar Anonymous tevékenységek

ásodik „őszi” hullám célpontjai

012.08.27. DDoS: Közgép
012.08.30. DDoS: monsanto.hu
012.09.20. DDoS: kormany.hu, TEK, Simicska
012.10.31. DDoS: monsanto.hu, kormany.hu
012.11.06. DDoS: MTVA, TEK, OTP (itt már erőtlenek lettek)



Kik az Anonymous tagjai?

Jellemzően 15-25 évesek fiatalok

övetkeztetések

ithout achievements any research good for nothing”

- Nem IT területen levő vezetők és döntéshozók jellemzően nincsenek tisztában a kibertámadás valódi kockázataival
- Felismerhetőek az azonosságok a haza Anonym tevékenységek között: előkészületben, módszerek kapcsolattartásban, kommunikációban
- magyar Anon sikertelennek tekinthető (kivéve A
- Hazai Anonymous nem összemérhető pl. az ame
- Ha egy képzett szakember beáll közéjük és nem elismerést szereznének, komoly meglepetést és fejtörést okozhatnak…
- Amennyiben hazánk ellen nemzetközi kiber tám kerülne sor (Anonymous által), vélhetően jóval kiszolgáltatottabb helyzetbe fogunk kerülni

KÖSZÖNÖM A FIGYELMET!

FACEBOOK/Ádám Novák(Anon) hozzászólása: „ha annyit tudnál mint mi anonok összetennéd a 2 kezed azért nem használunk extrémebb támadásokat mert nem akarjuk,hogy lesitteljenek vágod?”