# Probleem klaviatuuri ja tooli vahel? Või eikellegi laps?

TPK2012
Kaido Kikkas

# Nägin kord jaburat und...

- Kuri nõid tegi “Pinnnn!” ja kaotas ära kõik liikluspolitseinikud
- ...ja autokoolid ning ARKi takkapihta
- ...ja peaaegu kõik liiklusmärgid

- Pärast seda hakkas linnaliiklus nägema välja umbes nagu Internet

# Näide päriselust: Valdo Vänt

- Tore lihtne mees, pereisa, ametilt mehaanik
- Valdo säästab raha ning jõulude eel otsustab Ülemiste keskuses šopates perele uue arvuti osta – jube hea diil oli, printer-skanner anti kauba peale ja kõik tarkvara oli kohe kaasas
- Valdo pakib arvuti lahti, ühendab juhtmed seina, järgmisel päeval paneb patsiga poiss neti sisse
- Paar päeva on kõik kena (lapsed on eriti sillas)
- Siis hakkab arvuti aeglaseks kiskuma, krõbistab pidevalt kettaga ja ilmuvad mingid uued asjad

# Kus põhiline probleem oli?

- Valdo Vänt ajas asju
  - arvutimüüjaga
  - tarkvarategijatega (enamasti läbi arvutimüüja)
  - võrguteenuse pakkujaga
- Tema turvalisus ei huvitanud mitte kedagi
- Tulemus paistab näiteks siit: http://www.securelist.com/en/analysis

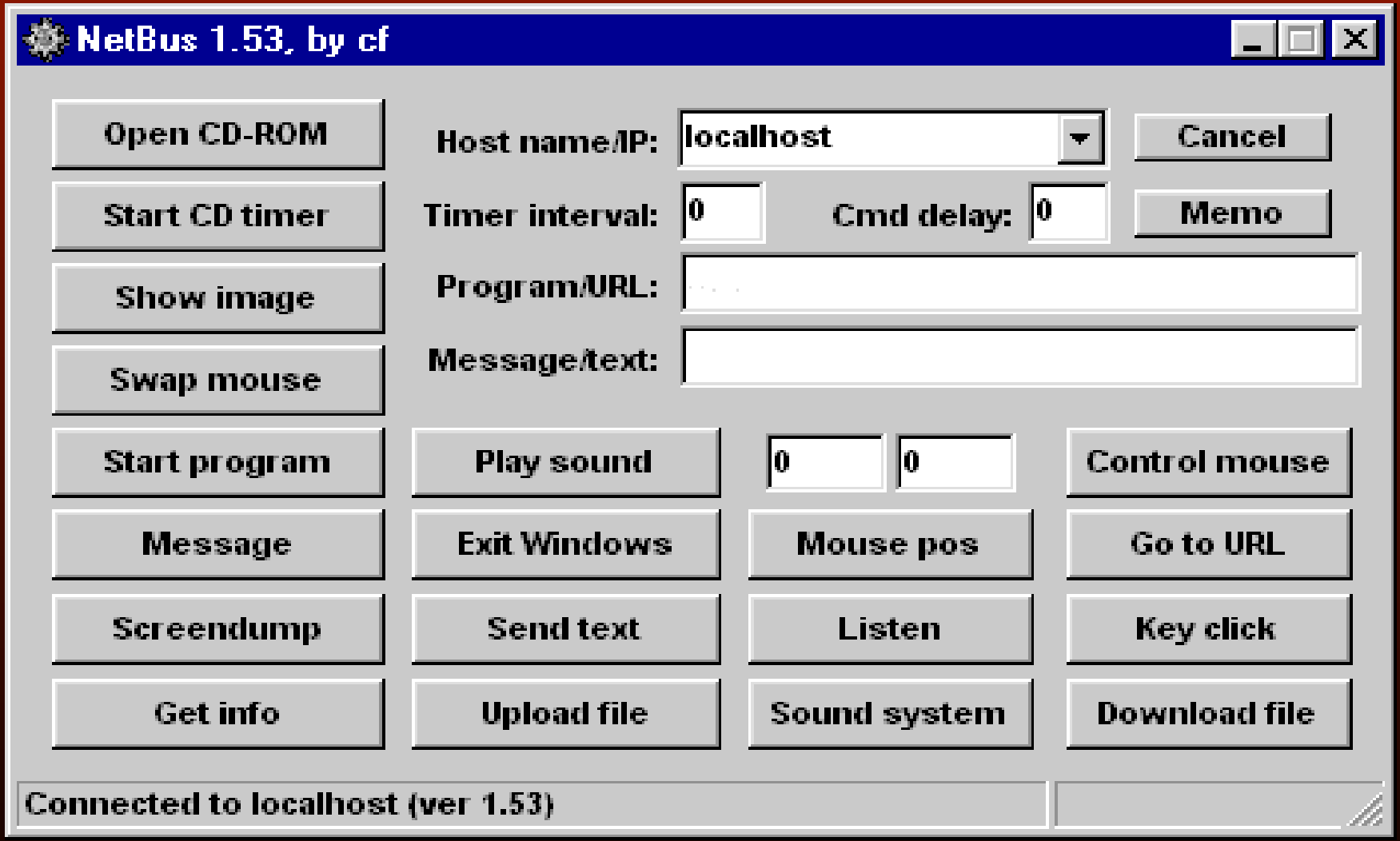
# Veel üks hea näide: Tiigrihüpe

- Palju räägitud ja promotud programm Eesti koolide varustamiseks arvutitega. Käis umbes nii:
  - Koolidele osteti arvutid. Algul ühe-, pärast klassikaupa. Kasutajate koolitamine ei huvitanud kedagi.
  - Siis sai keegi teada, et tarkvara oleks ka vaja. Osa osteti sisse, osa tehti kohapeal. Kasutajate koolitamine ei huvitanud kedagi.
  - Siis sai keegi teada, et ka võrku oleks vaja. Algul olid modemid, pärast püsiühendused. Kasutajate koolitamine ei huvitanud kedagi.
  - Siis hakati vaatama, et mis ikkagi toimub...

# Vanal ajal

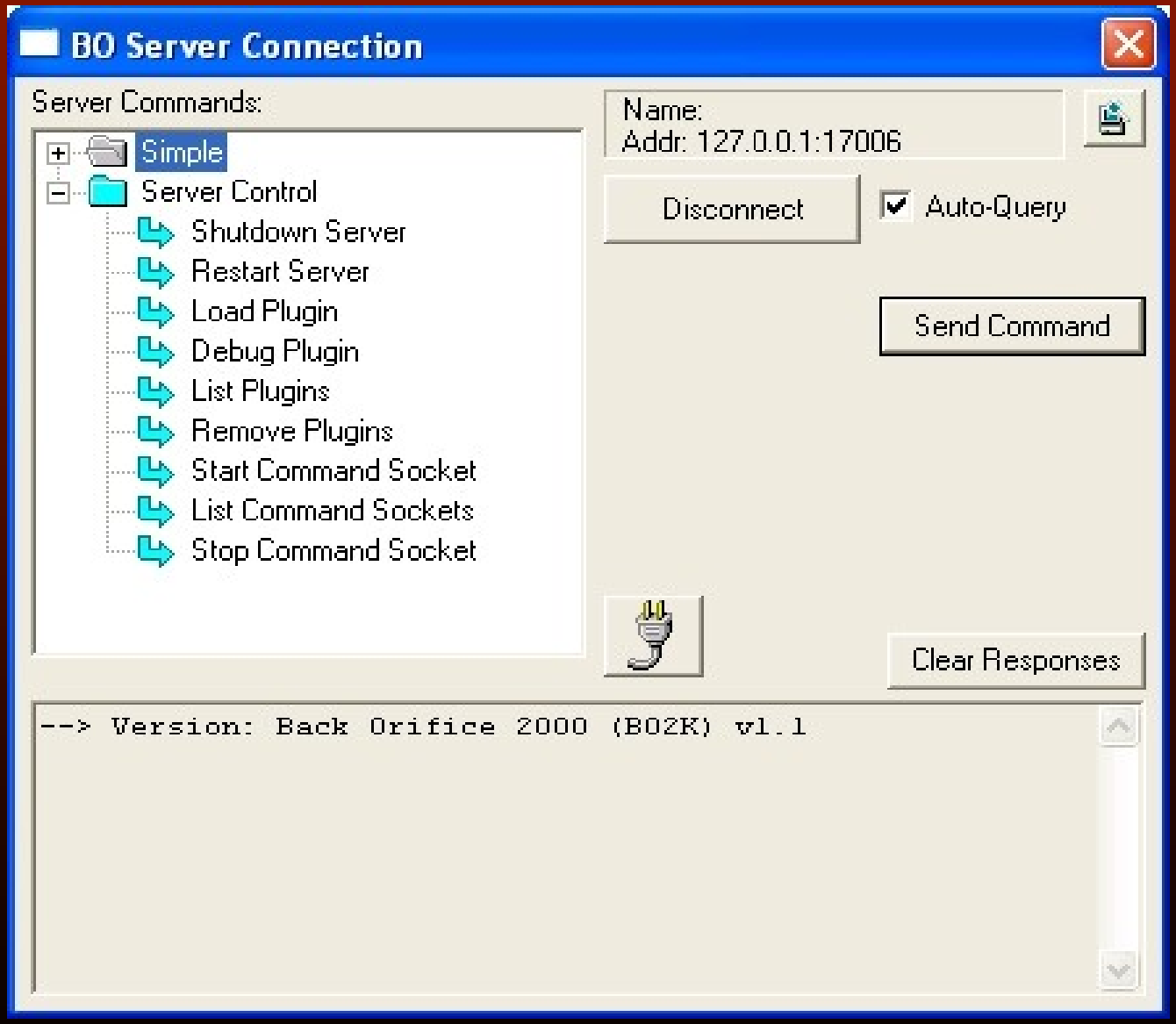
- ...oli arvutite kräkkimine
  - vähem pahatahtlik (vemp, mitte räige käkikeeramine)
  - väga harva seotud rahaga
  - omasuguste jõukatsumine
  - oskusi nõudev asi
  - üsna väikese seltskonna eralõbu

# Sajandivahetus: Netbus....

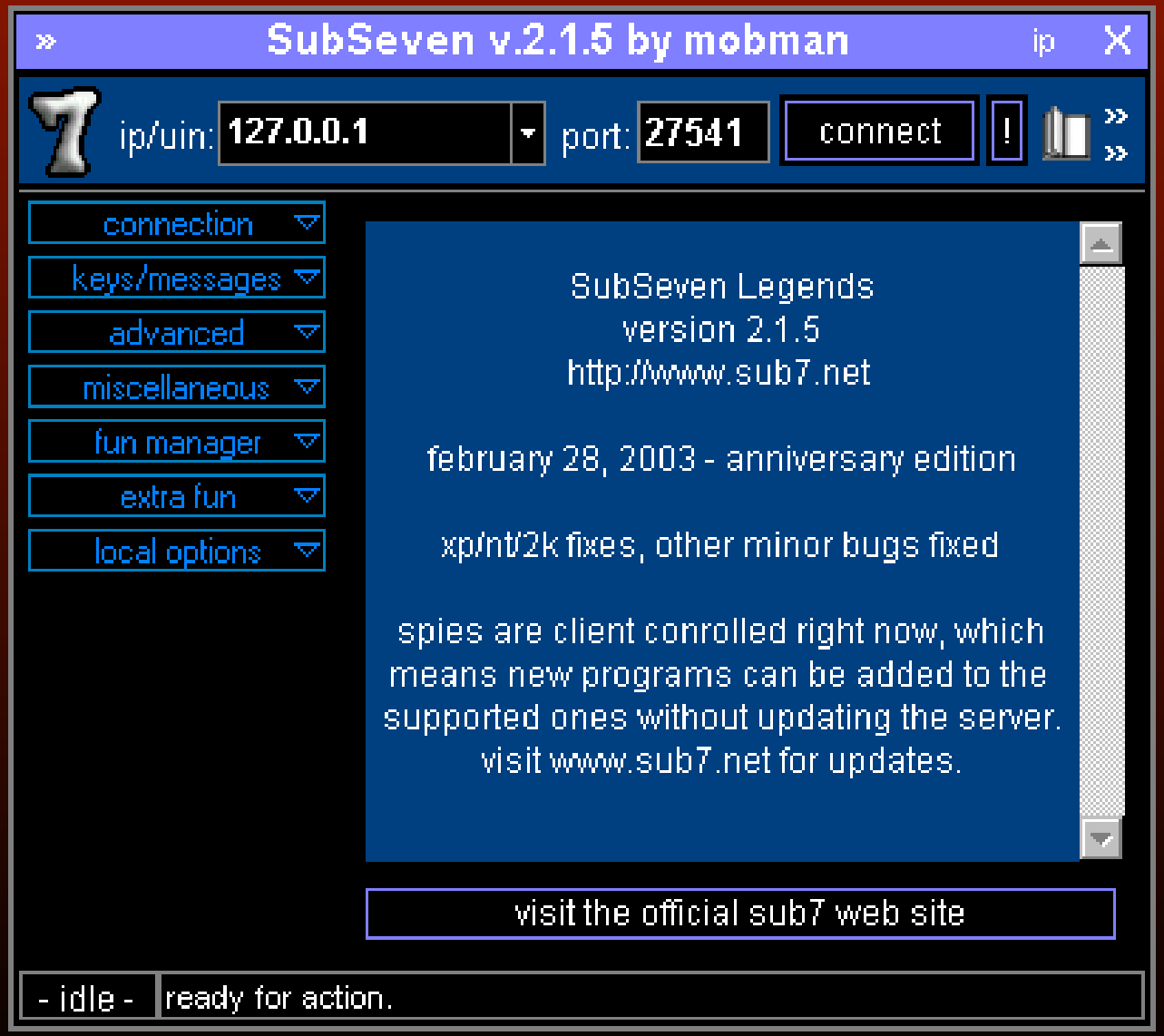



Vt ka Magnus Erikssoni juhtumit – näiteks siit:
http://radsoft.net/rants/20041128,00.shtml

# Back Orifice 2000....



# Sub7


SubSeven v.2.1.5 by mobman
ip
ip/uin: 127.0.0.1
port: 27541
connect
connection
keys/messages
advanced
miscellaneous
fun manager
extra fun
local options
SubSeven Legends
version 2.1.5
http://www.sub7.net
february 28, 2003 - anniversary edition
xp/nt/2k fixes, other minor bugs fixed
spies are client conrolled right now, which means new programs can be added to the supported ones without updating the server.
visit www.sub7.net for updates.
visit the official sub7 web site
- idle -
ready for action.

# Eesmärk muutub

- Tänapäeva sõjas on kasulikum vastast vigastada kui tappa – jääb teistele koormaks!
- Niisamuti ei kohta täna enam vana aja viirusi, mis vormindasid kõvaketta päästmatult üle
- Tänane põhieesmärk – ohvri masin peab jääma tööle (vahel isegi lapitakse sel turvaaugud ära!) ja täitma ründaja anta-vaid ülesandeid (põhitööna – kui aega üle jääb, võib ka endist omanikku teenindada)

# Massifaktor

- Iga kurja geeniuse kohta on olemas suur hulk skriptijuntsusid (ingl k. *script kiddie*), kel
  - pole erilisi oskusi ega teadmisi
  - pole elu
  - see-eest on roppumoodi vaba aega
- KÕIGE OHTLIKUM TEGELANE MAA-MUNAL ON HÄSTIVARUSTATUD LOLL

# Valel ajal vales kohas?

- Valdo Vänt kui isik ei huvitanud tegelikult mitte kedagi
- Huvitas sobivalt kaitsmata arvuti
- “Ära võta isiklikult!” (kaks lasku pähe)
- Skriptijuntsu tüüpiline taktika on kammida mingit võrgusegmenti, otsides mingit kindlat turvaauku ja rünnates siis leitud sihtmärke mingi valmisvahendi abil (tihti oma lõbuks, üha enam on aga nad mõne suurema jõu teenistuses – N: Russian Business Network)

# “No ja siis...?”

- Üsna tavapärane reaktsioon – “mina pole tähtis nina, kes see ikka minu arvutit torkima tuleb....”
- “Ja kui tuleb, keda see minu arvuti pahavara kotib?”
- MIND!
- Sest sinu arvuti ühineb tuhandete teiste samasugustega mõnes botnetis – JA MINA VÕIN JUBA SELLEGA PIHTA SAADA

# Botnet?

- Maakeeles ka robotvõrk; suur hulk võrku-pidi kaaperdatud ja sealtkaudu kellegi kurikaela keskse juhtimise all olevaid tavaarvuteid. Hästitoimiva robotvõrgu arvutusvõimsus on võrreldav superarvuti omaga! Rent: paarsada dollarit ööpäevas (http://blog.damballa.com/?p=330)
- Peamised kasutusalad:
  - rämpsposti ja petuskeemide levitamine
  - DDOS-rünnakud – viimasel aastakümnel väga levinud väljapressimisskeemide osana
  - poliitilised ründed ja infosõda (üha enam)

# Ettepanek, millest ei saa keelduda

- Uut laadi organiseeritud kuritegevus, mille ohvriteks on Lääne-Euroopa IT-võhikud, kelle äri aga sõltub võrguühendusest
- „Makske meile 5000 naela või olete kaks nädalat ilma võrguta!“
- Ei ole tühi ähvardus - botnetid on reaalsus
- „Mõistliku“ summa korral kutsub maksma
- Näe, loll maksis – küsime kuu aja pärast rohkem!

# Mida annab teha sinu arvutiga

- Hoida oma pornokollektsiooni – mõningat sorti porno on vägagi plahvatusohtlik
- Ladustada illegaalset tarkvara – BSA hakkab põrkama ja koledaid hääli tegema
- Tekitada kommunikatsioonikanal – näiteks IRC-kanal varastatud krediitkaartidega äritsemiseks
- Saata hulgaliselt nahaalkirju
- Rünnata kedagi (otse või vahelülide kaudu)
- Netipanka kasutada (sinu arvega)

# Veel üks mure: kolmest kaks

- Lihtne, soodne, turvaline – vali neist kaks!
- Tüüpiline arusaam:
  - Windows PC: (üsna) soodne, lihtne
  - Mac: lihtne ja (üsna) turvaline
  - Linux PC: soodne ja turvaline
- Pole päris tõsi, kuid arusaama on raske muuta
- Võrdlus autoralliga: vana Ladaga sõitev Sebastien Loeb tippklassi Citroëni roolis istuva Valdo Vända vastu - oskused loevad eelkõige, aga loeb ka platvorm

# Märkus õunainimestele

- Siiani on Apple'i kasutajaid pahavara eest kaitsnud väike turuosa ja intelligentsete kasutajate küllaltki suur osakaal. Mõlemad tegurid kipuvad tänapäeval üha enam muutuma (sama kehtib teatud määral ka Linuxite, eriti Ubuntu ja Minti suhtes)
- OS X on “põhja” poolest turvalisem kui Windows – aga lolli kasutajat see ei aita
- Apple ilmutab selget soovi saada uueks Tumedaks Jõuks Microsofti asemel. Suletuses ja salatsemises (ka turvaküsimustes) ollakse mõnes aspektis juba Microsoftist ees

# Lootusetu....?

- Nii hull ka ei ole
- Enamik lihtsaid ründevahendeid eeldab uuendamata ja/või muidu lohakil süsteeme
- Võrdlus korteriuksega: kuitahes hea Abloy lukk ei peata siseneda soovivat K-komandot, kuid hoiab tõenäoliselt eemal järgmise doosi jaoks raha vajava selli
- 100% turvalisust pole olemas – ent on olemas võimalus tõsta see mõistlike kulutustega mõistlikule tasemele

# *Password, password,* hakka pähe!

- Kehvad salasõnad („kala“ jt) - „Windowsi-põlvkonna“ ohtlikemaid haigusi
- Parool kui „tüütu ja mõttetu“ nähtus => jätkub ka W2000, XP, Vista ja 7 juures
- Sage „lahendus“ - kasutame adminirežiimis!
- Miski pole uus... Bob Metcalfe'i 1973. aasta RFC *The Stockings Were Hung by the Chimney with Care*, teemaks kehvad paroolid

# Mis kinni ei jää...

- Vähemalt 12 märki (tänapäeval üha enam ka mitmest sõnast koosnev paroolifraas)
- Nii suur- kui väiketähed, numbrid ja (kus lubatud) ka erisümbolid
- Ei oma otsest tähendust üheski levinud keeles (väga eksootiline keel on ehk OK)
- Soovitavalt mingi peidetud võtmega. N:
  - Le5ta.07.K4La : lemmiktoit + auto väljalaskeaasta
  - 5e6a+,5uMmA! : lemmikraamat „Pipi Pikksukk“

# *Quod licet Jovi non licet bovi*

- Sageli on koduarvutil mitu kasutajat. Näiteks selline perekond:
  - Isa – ülikooli ehitusmehaanika õppejõud
  - Ema – keskkooli eesti keele ja kirjanduse õpetaja
  - Vanem poeg – tudeng, programmeerija
  - Noorem poeg – 13-a hiphoppar, pinna-pealne arvutihuviline (kõva mängur)
  - Pisitütar – 4-a lasteaialaps
- Kuidas vältida olukorda, kus ühe pereliik-me eksimus kahjustab ka kõiki teisi?
- Kasu on kodusest selgest reeglistikust

# CERT soovitab

- Päris hea lugemine (2006, aga tänini asjalik):http://www.cert.org/tech_tips/home_networks.html
- Kodus töötades konsulteeri töökoha IT-turvaga
- Kasuta antiviirust
- Kasuta tulemüüri
- Ära näpi tundmatuid meilimanuseid
- Ära kasuta tundmatust allikast pärit tarkvara
- Lülita välja faililaiendite peitmine

# ...

- Uuenda regulaarselt kogu tarkvara (sh OS)
- Kui arvutit ei kasutata, lülita see välja või katkesta võrguühendus
- Kui võimalik, lülita Java, Javascript ja ActiveX välja
- Lülita välja e-postitarkvara skriptikasutus
- Tee regulaarselt tähtsatest andmetest varukoopia
- Loo arvutile varu-käivitusketas

# Õppida, õppida, õppida...

- Paljudes valdkondades on tänapäeval kasulikum jätta erialased jätta proffide hooleks (maja ehitamine, auto remont)
- Kehtis ka arvutiasjanduses – kuni võrgunduse massilise levikuni
- Tänane võrgukasutaja peaks tegelikult teadma arvutist rohkemgi kui eelmine põlvkond – või suutma need teadmised „sisse osta“

# Mida peaks oskama?

- Tunne oma arvutit (tähtsamate osade margid)
- Tea, mis tarkvara Su arvutis on
- Oska kettal orienteeruda
- Oska süsteemi regulaarselt uuendada (enamikul juhtudel üsna lihtne)
- Orienteeru tähtsamates abiprogrammides (antiviirused, nuhkvaraeemaldajad jms)
- Ole uudishimulik ja õpivõimeline

# Pahad Asjad

- Kasutada arvutit pidevalt administraatorina
- Valida parooliks lihtsaid sõnu
- Jätta süsteem uuendamata
- Ronida võrgus sinna, kuhu pole vaja
- Toppida oma meiliaadressi igale poole
- Näppida võõrastelt tulnud meilide manusefaile
- Paigaldada  tundmatust allikast pärit tarkvara (eriti Windowsil, aga ka muudes süsteemides)

# Õppejõu soovitused

- Vaheta välja Outlook ja IE (kasuta midagi muud). Väga mitmed riskid vähenevad
- Paigalda MS Office'i  kõrvale (kui mitte asemele) LibreOffice ja kasuta MSO-t vaid juhtudel, kui LO hätta jääb. Office'i pahavara oht väheneb kordades
- Tasuks kaaluda süsteemi väljavahetamist - Maci ja Linuxi puhul on probleem suurusjärgu võrra väiksem (ehkki kaugeltki mitte null). Windows 7 on eelmistega võrreldes vaid väike samm edasi (http://www.computerworld.com/s/article/9216654/Windows_7_s_malware_infection_rate_climbs_XP_s_falls?taxonomyId=17)

# Veel paar värvilist riskifaktorit

- Flash
- Silverlight
- ActiveX
- Acrobat & Co

- Õpetlik näide ActiveX kohta: http://www.koreatimes.co.kr/www/news/biz/2009/09/123_52401.html

# Veebilehitseja

- Tasub kasutada vahendeid, mis reguleerivad erineva võrgusisu kasutamist:
  - Reklaamipüüdja (N: AdAware)
  - Skriptikontroller (N: NoScript)
- Eriti tasub kasutada viimast – püsivalt lubada tasub skripte vaid seal, kus tõesti teame, et ohtu pole. Mujal aga proovida esmalt ilma skriptideta ja kui siis ei tööta, lubada seansipõhiselt

# Kokkuvõtteks

- Seis on üsna sant (aga mitte lootusetu)
- Suurim probleem istub arvuti taga
- Enda masina kaitsmine tähendab selle masina võrra väiksemaid botnette
- KAITSE ENNAST JA ÕPETA TEISI

# “Tahtsime parimat, välja tuli nagu alati”