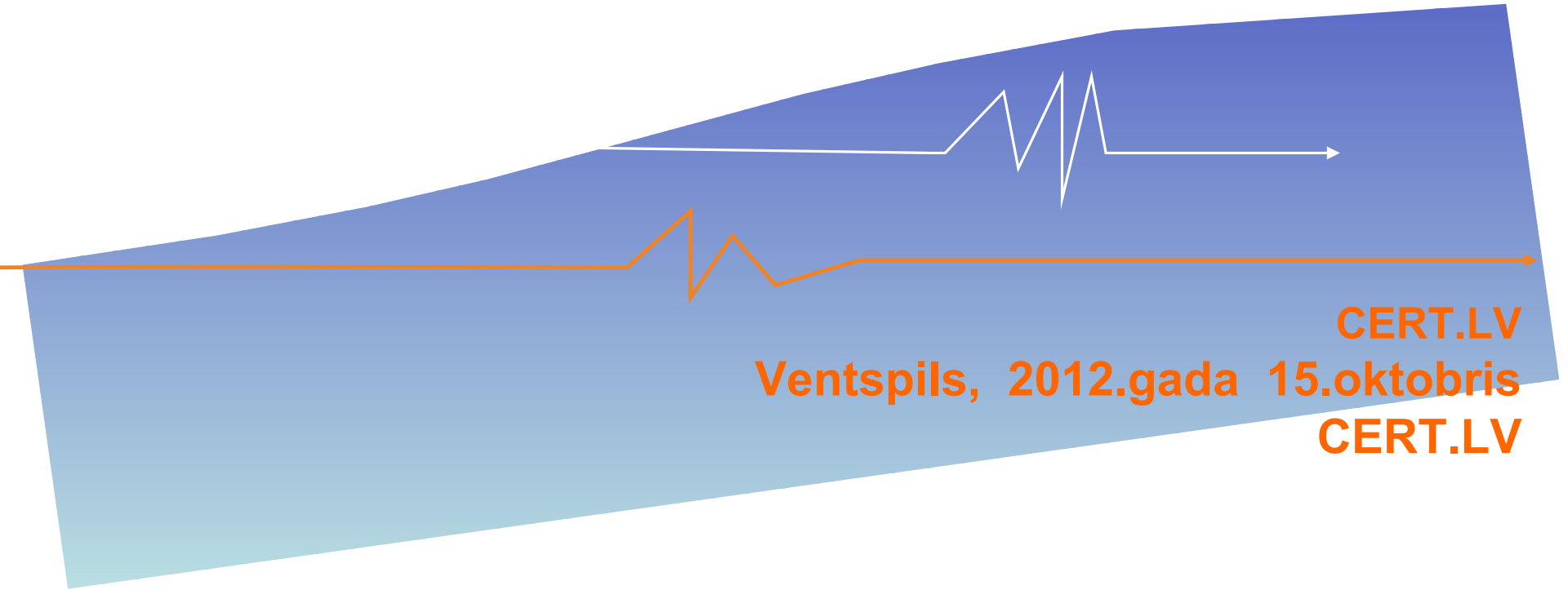
“Iekārtu (arī datoru :) drošība”

Gints Mālkalnietis, CERT.LV



CERT.LV

Ventspils, 2012.gada 15.oktobris

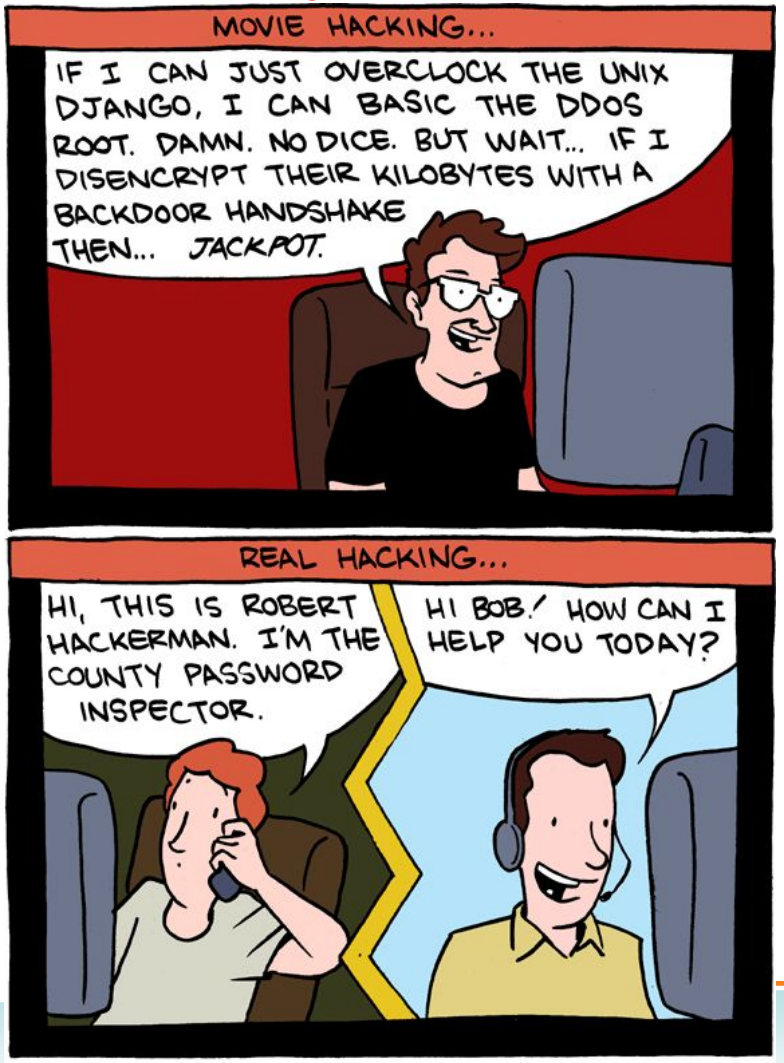
CERT.LV

Saturs

- Riski mūsdienu tehnikai
- Riski mūsdienu tehnikai
- Dažas noderīgas lapas

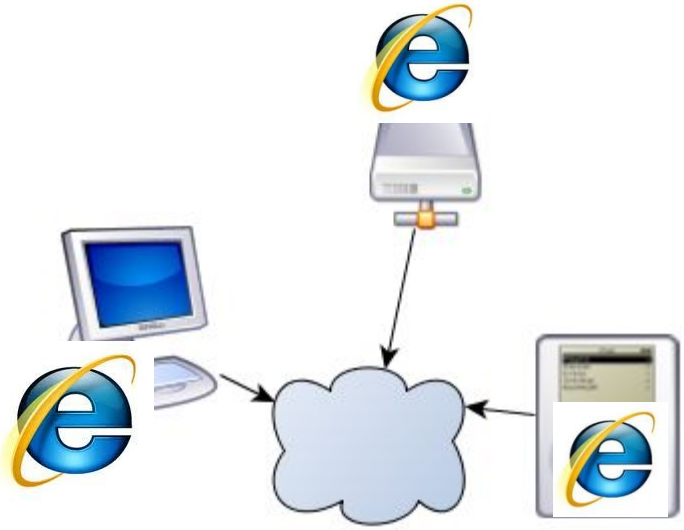
Riski mūsdienu tehnoloģijās

- Neviens drošības risinājums nav 100% drošs!



Interneta pārlūks = dators (OS + app.)

- Interneta pārlūks = pilnvērtīgs dators
- Veiksmīgs uzbrukums pārlūkam – pilnīga kontrole pār lietotāja datiem
- Dažādas ierīces – viena ievainojamība



Jebkurš dators = serveris

- Veiktspēja >kā 5 gadus vecam serverim
- Vienmēr – pievienots internetam
- Parasti – ar novecojušām, nelabotām programmām
- Dažreiz – ar pārāk lielām lietotāja pilnvarām veikt tajā izmaiņas

Datu “mākonis” – neglābj no vecām kļūdām!

• 2009 – Vairāk kā 300 dokumentu par TWITTER biznesa plāniem tika nozagti no Google Apps. Iemesls – vāja parole.
• 2010 – Izveidota programma WiFi paroļu uzlauzšanai, izmantojot Amazon E2 Cloud
• 2011 – Amazon E2 Cloud tiek izmantot uzbrukumā Sony PSN
• 2011 – Dropbox kļūdas pēc uz vairākām stundām atslēdz autentifikācijas pārbaudi = iespējams lejuplādēt jebkuru failu

Antivīrusu programmas – ne tik drošas kā solīts!

- Efektivitāte pret jauniem vīrusiem - 10-20%
- Nav laicīgi atjaunotas
- Traucē un bremzē ikdienas darbus
- Nereaģē uz ārējo “spiegošanas” aparatūru

virustotal

SHA256: b0c4b037940204551 2a9b651f26afdabf6d6aaa28e9db98429d79c0882aa2bd
File name: x.docx
Detection ratio: 0 / 42
Analysis date: 2012-04-11 11:41:05 UTC (0 minutes ago)
More details

0 0

Antivirus	Result	Update
AhnLab-V3	-	20120410
AntiVir	-	20120411
Antiy-AVL	-	20120411
Avast	-	20120411
AVG	-	20120411
BitDefender	-	20120411
ByteHero	-	20120407
CAT-QuickHeal	-	20120411
ClamAV	-	20120411
Commtouch	-	20120411
Comodo	-	20120411
DrWeb	-	20120411
Emsisoft	-	20120411
eSafe	-	20120408
eTrust-Vet	-	20120411
F-Prot	-	20120410
F-Secure	-	20120411
Fortinet	-	20120411
GData	-	20120411
Ikarus	-	20120411
Jiangmin	-	20120411
K7AntiVirus	-	20120410
Kaspersky	-	20120411
McAfee	-	20120411
McAfee-GW-Edition	-	20120410
Microsoft	-	20120411
NOD32	-	20120411
Norman	-	20120411
nProtect	-	20120411
Panda	-	20120410
PCTools	-	20120411
Rising	-	20120411
Sophos	-	20120411
SUPERAntiSpyware	-	20120402

SHA256: b0c4b037940204551 2a9b

File name: x.docx

Detection ratio: 0 / 42

Analysis date: 2012-04-11 11:41:05 UTC

- Programmēšanas laiks < 30 minūtes
- Profesionāli kaitīgā koda veidotāji izmanto automatizētus rīkus sava koda slēpšanai
- “Svaiga” datorvīrusa variācija katru dienu

Kur slēpjas datorvīrusi? (1)

1. Ļaundabīgu kodu saturošas interneta vietnes
   - ✓Izveidotas apzināti
   - ✓Apmeklētāji tiek pievilināti caur SEO
   - ✓Saites forumos, komentāros, Twitter
2. Uzlauztas labdabīgas interneta vietnes
   - ✓ SQL injekcijas
   - ✓Novecojušas satura vadības sistēmas
   - ✓Kļūdas lapas kodā
   - ✓Kļūdas reklāmas plūsmu sistēmās
3. Noņemamie datu nesēji:
   - ✓USB zibatmiņa
   - ✓Nezināms izcelsmes CD
   - ✓Navigācijas iekārtas (TomTom, Garmin utt.)
   - ✓Citas iekārtas ar iebūvētu datu krātuvi – GSM modemi, mobilie telefoni, mūzikas atskaņotāji

Kur slēpjas datorvīrusi? (2)

4. E-pastā saņemti dokumenti un saites
5. Tīkla iekārtas
6. Biroja tehnika
   - ✓ Printeri – satur operētājsistēmu Windows 2000 vai Linux speciālas versijas
   - ✓ “Smart TV” – gandrīz pilnvērtīgs dators ar Linux OS
   - ✓ Dažādas specializētas mēriekārtas, medicīnas aparatūra

MIPS 200 Mhz CPU, 256 MB RAM, 9GB HDD, IRIX 6.3 OS

1.4GHz Quad Core CPU, 1GB RAM, 64 GB flešatmiņa, Android 4.0 OS

Dzīvesvietu un e-pasta adreses, telefoni
Finansiāla informācija
Pieejas dati pakalpojumiem, citām ierīcēm
Fotogrāfijas, filmas, mūzika

Mobilais telefons ir jūsu dators
Mobilais telefons ir jūsu naudas maks
Drošības kods ir nepieciešams
Nesankcionēta pieeja ir iespējama attālināti

Google Play

App Store

OVI Store


AVG
Anti-Virus


lookout
MOBILE SECURITY


avast!

Paldies!!!

Gints Mālkalnietis
E-pasts: gints@cert.lv
Tīmekļa vietne: http://www.cert.lv
Portāla Esi drošs tīmekļa vietne: http://www.esidross.lv
CERT.LV Twitter vietne: http://twitter.com/certlv