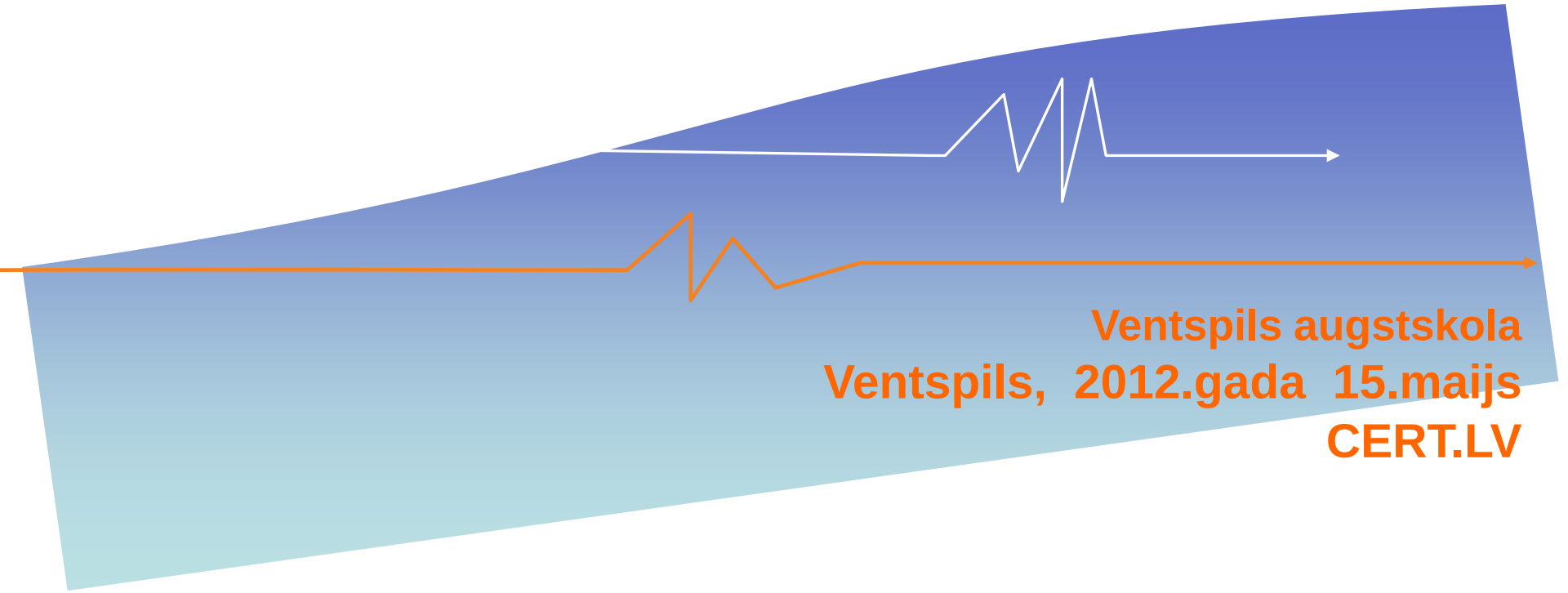
“IT drošības aktualitātes”

Gints Mālkalnietis, CERT.LV



Ventspils augstskola

Ventspils, 2012.gada 15.maijs

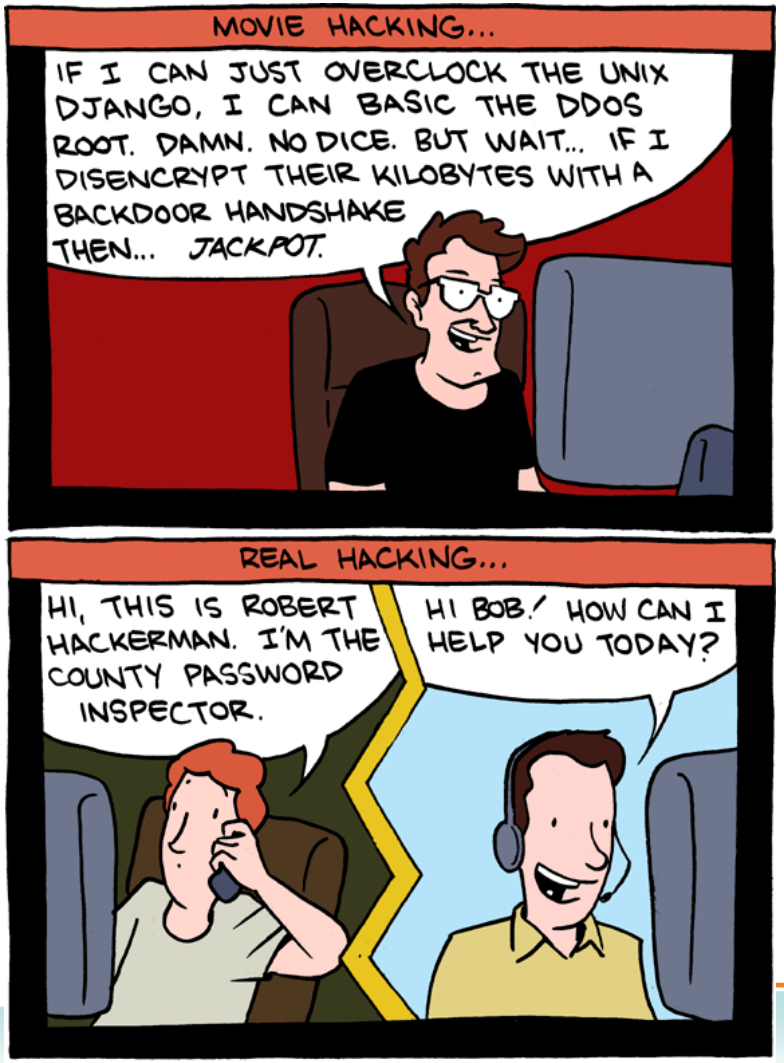
CERT.LV

Saturs

- Riski mūsdienu tehnoloģijās
- Nedaudz par datorvīrusiem
- Reāla uzbrukuma anatomija
- DOS/DDOS tendences
- Īsi par botnetiem
- Dažas noderīgas lapas

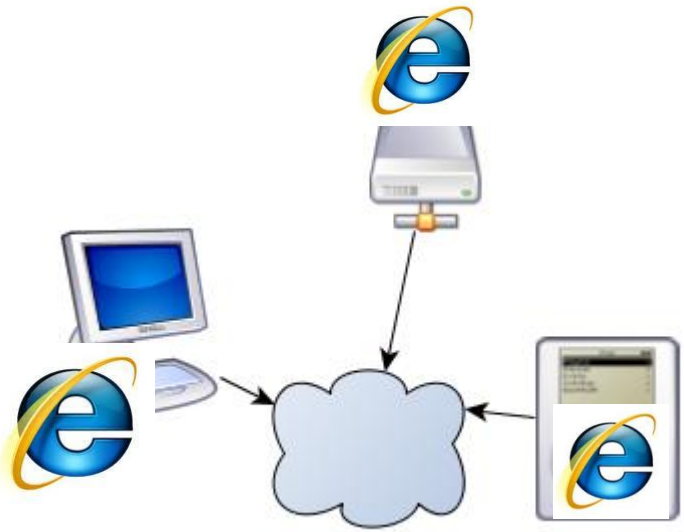
Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



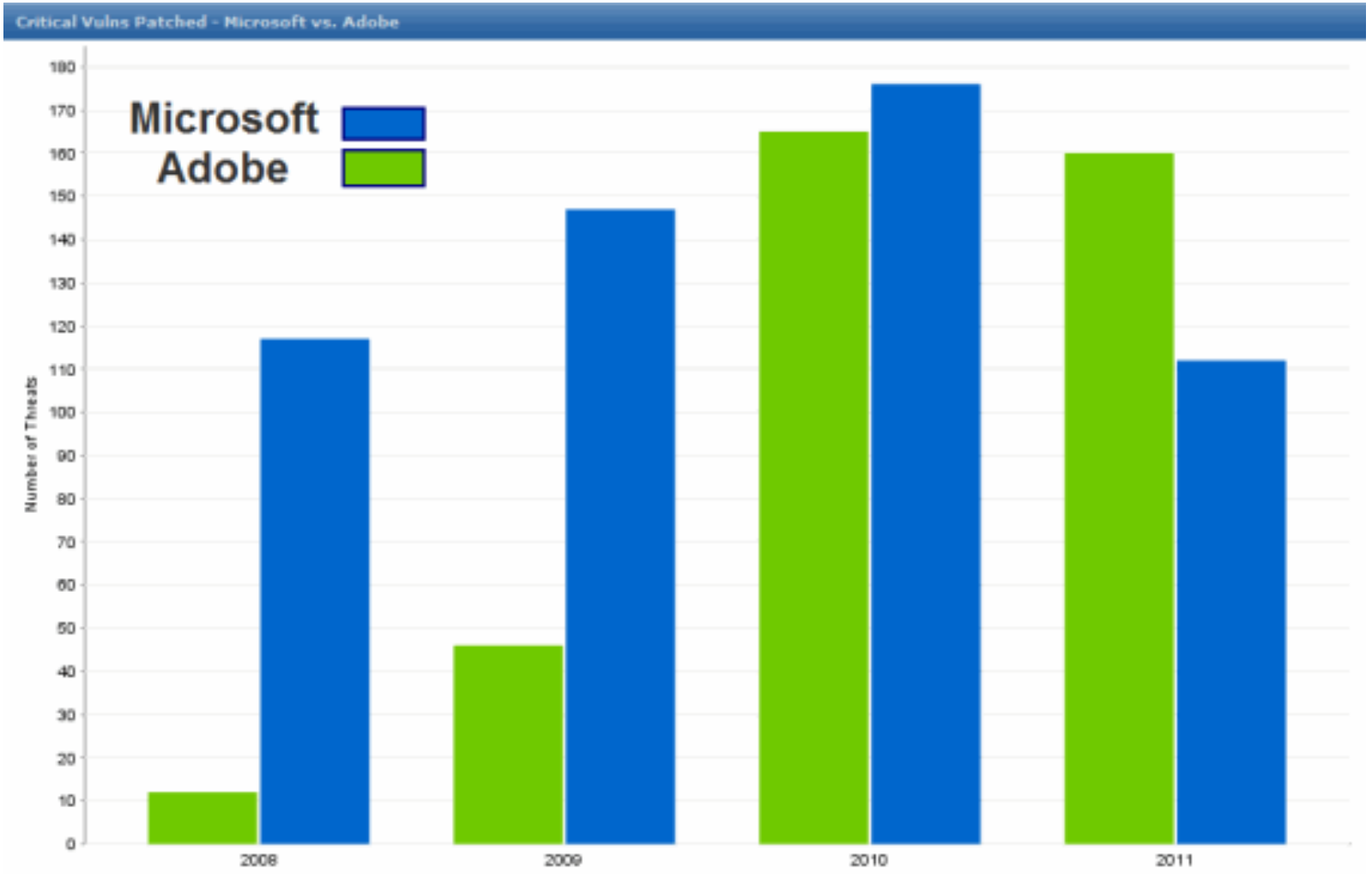
Interneta pārlūks = dators (OS + app.)

- 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


Critical Vulns Patched - Microsoft vs. Adobe
Microsoft
Adobe
Number of Threats
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
2008
2009
2010
2011

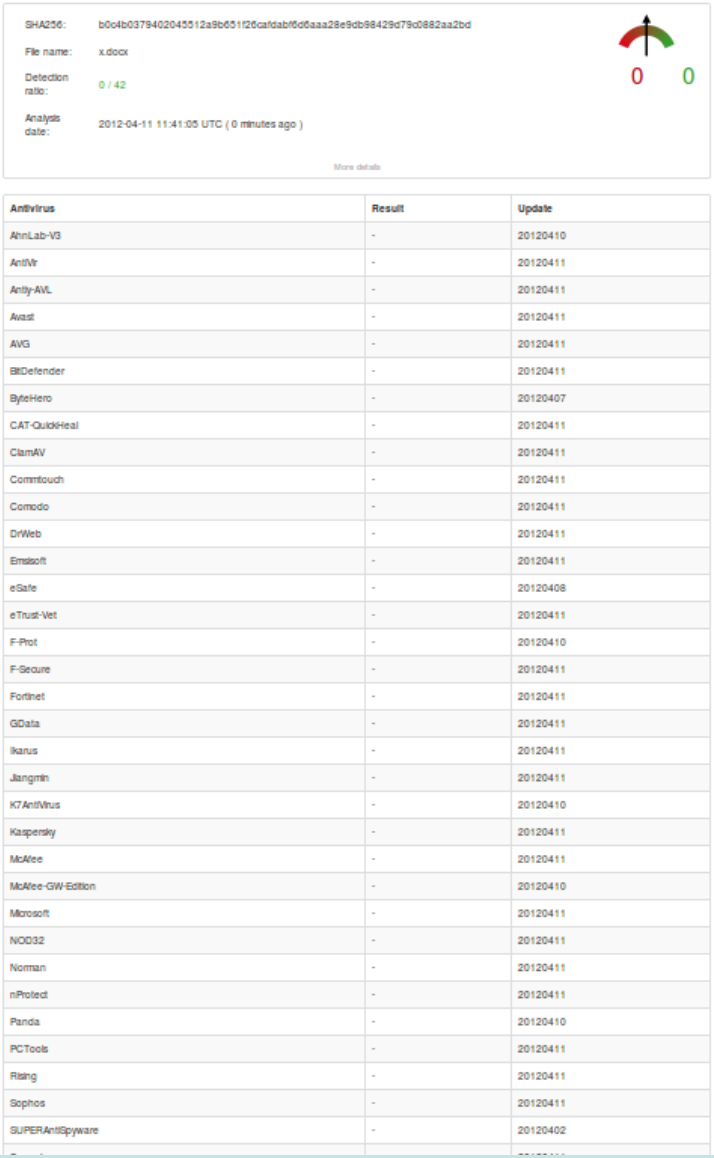
Datu “mākonis” – neglābj no vecām kļūdām!

•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 2a9b651f26cafdabf6d6aaa28e9db98429d79c0882aa2bd

File name: x.docx

Detection ratio: 0 / 42

Analysis date: 2012-04-11 11:41:05 UTC (0 minutes ago)

0 0

More details

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

Antvīrusu programmu efektivitātes pavairošana

1. Antivīrusu programma = pēdējais datora aizsardzības līmenis
2. Atvieglojiet tā darbu ar vispārēju datortīkla drošības uzstādījumu sakārtošanu!
3. Izmantojiet operētājsistēmas iespējas ierobežot nezināmu programmu izpildi
4. Atslēdziet automātisku programmu izpildi no noņemamjiem datu nesējiem
5. Izmantojiet centralizētu antivīrusu vadību

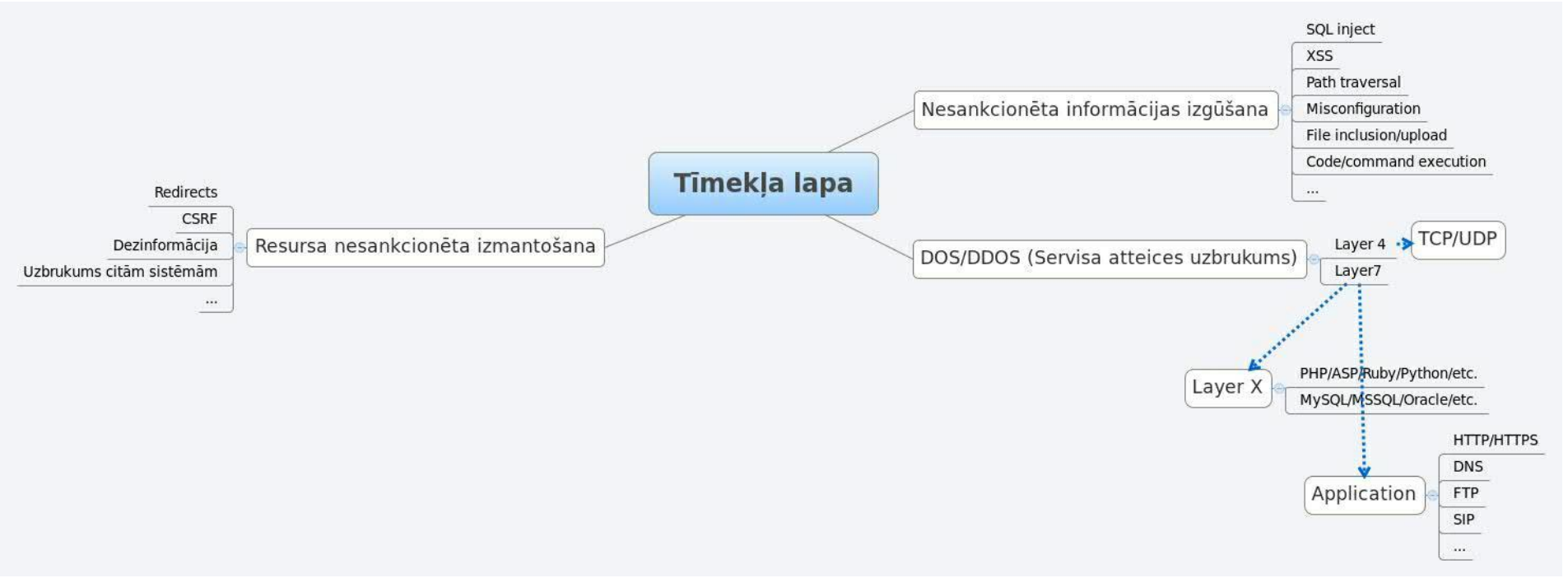
Kur slēpjas datorvīrusi?

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 izcelmes CD
   - ✓Navigācijas iekārtas (TomTom, Garmin utt.)
   - ✓Citas iekārtas ar iebūvētu datu krātuvi – GSM modēmi, mobilie telefoni, mūzikas atskaņotāji

Kur slēpjas datorvīrusi?

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

Reāla uzbrukuma anatomija



Uzbrukuma motivācija

- Nozagt informāciju
- Padarīt nepieejamu mērķa lapu
- Radīt neslavu
- Šantažēt
- ...

Uzbrukuma anatomija

1. Fāze - uzbrukumi tiešsaistes lapām

- Satura rediģēšanas sistēma pieejama no jebkuras IP adreses
- Administratora parole, lietotājvārds konfigurācijas failos/datu bāzē atklātā tekstā
- Nesekmīgo autentifikācijas mēģinājumu žurnalēšana datu bāzes tabulā

Uzbrukuma anatomija

Uzbrucēja metode = SQL injekcija

- Kāda parametra ievades dati netiek pienācīgi pārbaudīti
- Nesekmīgo autentifikācijas mēģinājumu žurnāls nonāk uzbrucēja rīcībā
- Ar SQL injekciju starpniecību ir izgūstami arī citi dati, taču sākotnēji tas uzbrucējam nav nepieciešams

Uzbrukuma anatomija

2. Fāze – deface

• Pēc drošības ielāpu ieviešanas uzbrucējs jebkurām metodēm cenšas padarīt web projektu nepieejamu

- dusmu izpausme?
- demonstrācija?
- mērķis?

Uzbrukuma anatomija

3. Fāze – DOS

- Slowloris/RSnake HTTP GET DOS
- HTTP range header DOS CVE-2011-3192
- GET DDOS izmantojot botnet
- Uzbrukumi pakalpojumu sniedzējam
- SQL BENCHMARK + MD5 pārslodzes radīšanai
- Uzbrukumi citiem web projektiem/serveriem upura tīklā ar mērķi realizēt uzbrukumu pakalpojuma sniedzēja resursiem no iekšienes

Nozieguma pēdu slēpšana

• Nelikumīgi iegūtā informācija parasti tiek publicēta ārvalstu bezmaksas resursos
• Darbības tiek veiktas no “anonīmiem” proxy servisu tīkliem, publiskiem WiFi tīkliem vai uzlauztām sistēmām
• Botnet lietošanai jābūt labai motivācijai un/vai līdzekļiem
–Uzbrukums vienai web lapai “izgaismo” botnet IP adreses
–Vai tas ir tā vērts?

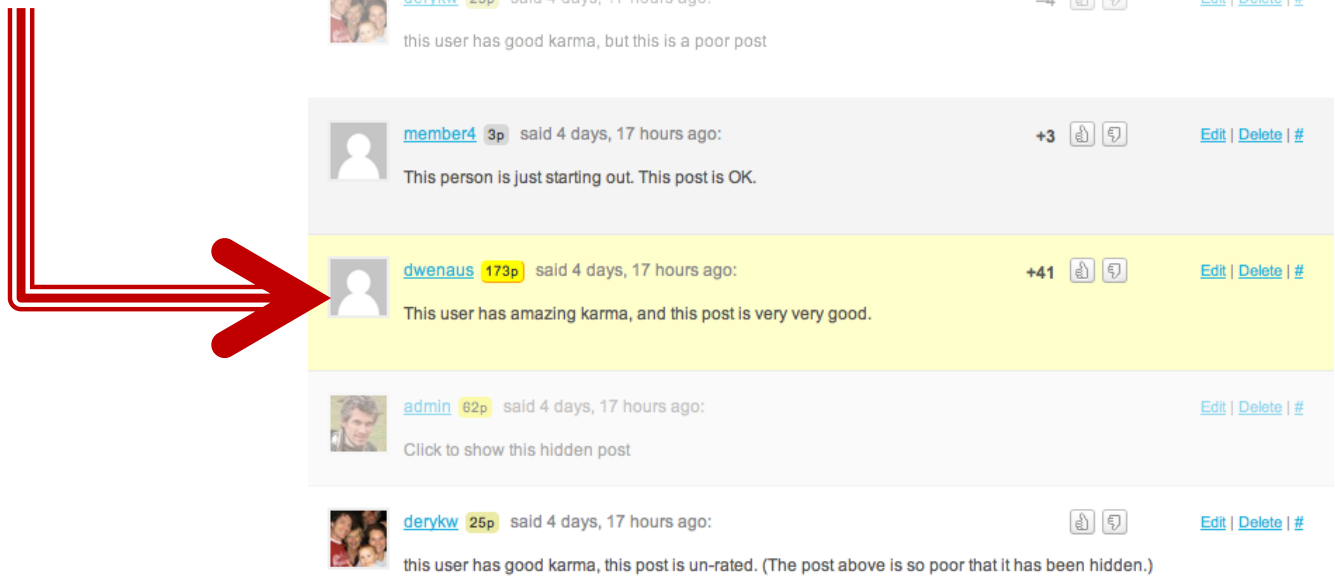
Nozieguma pēdu slēpšana

•Tiek lietoti redirect servisi - bit.ly, tinyurl.com, tiny9.com, etc.

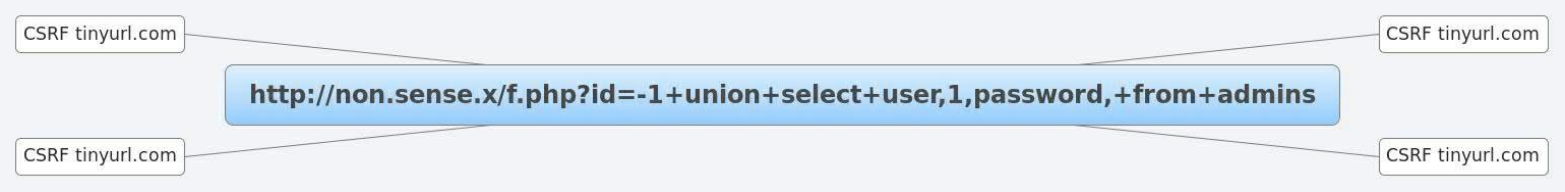
- Saites tiek noformētas kā uzbrukums vai identiskas pieprasījumiem, ko veicis uzbrucējs
- Publicētas dažādos publiskos resursos kā saites uz bildi vai citu saturu, kas tiek automātiski pieprasīts atverot lapu

Nozieguma pēdu slēpšana

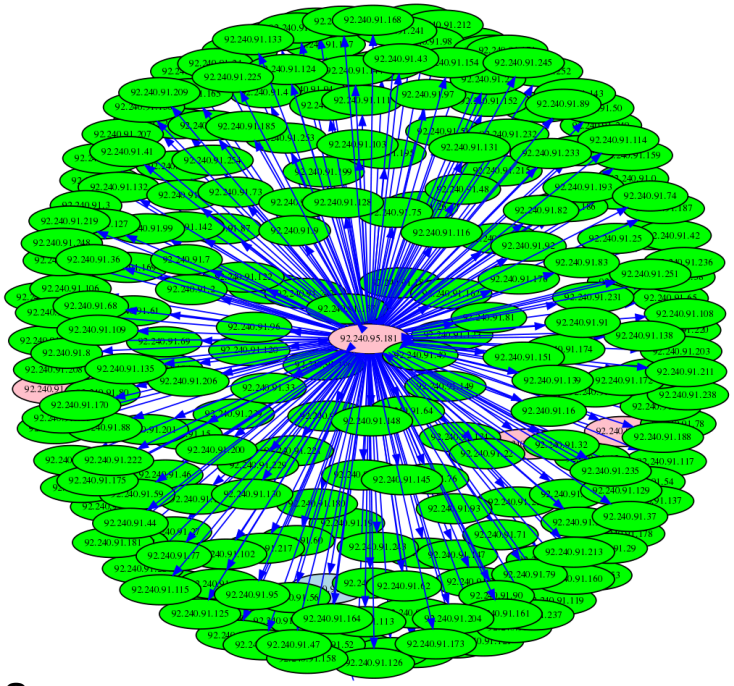
```
<img src='http://tinyurl.com/abcdf'
style='width:16px;
height:16px;' alt='[Face] ' />
```



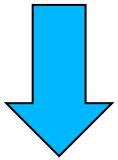
Nozieguma pēdu slēpšana



Rezultātā par uzbrucēju kļūst katrs CSRF tīmekļa lapas apmeklētājs, web meklētāji, ...



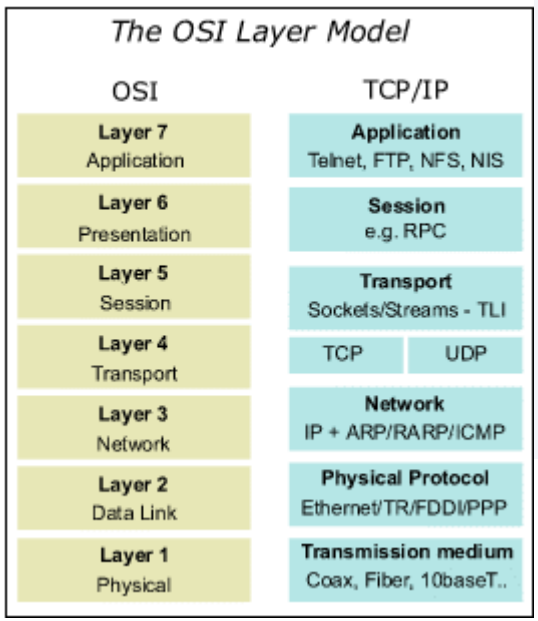
http://tinyurl.com/abcdf

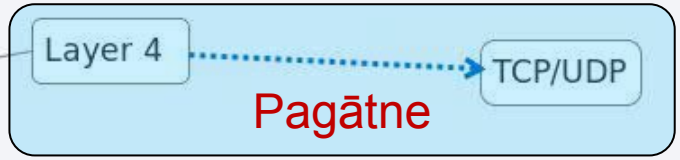


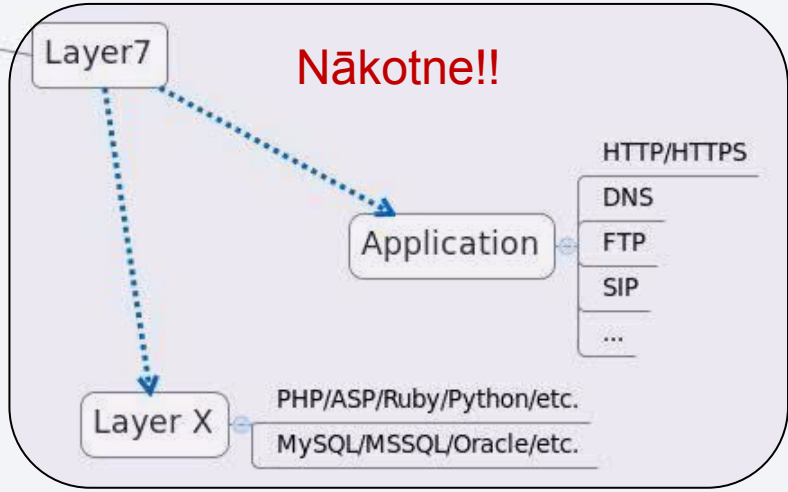
http://non.sense.x/f.php?id=-1+union+select+user,1,password,+from+admins

DOS/DDOS tendences

DOS/DDOS (Servisa atteices uzbrukums)







DOS/DDOS tendences

Layer 7?? = Application layer DOS

- Slowloris/RSnake HTTP GET DOS
- HTTP range header DOS CVE-2011-3192
- GET DDOS izmantojot botnet
- SIP/HTTP/HTTPS/DNS
- ASP/PHP/Ruby/Python...

Botnet

- Botnet = standarta lietotāja mājas/ofisa dators + uzlauztie serveri
- Lietotāja datori visbiežāk tiek inficēti apmeklējot kaitīgu kodu saturošas mājas lapas
- Tiek izmantotas internet pārlūkprogrammu un to papildinājumu ievainojamības
- Skaits nepārtraukti svārstās
- Tiek izmantoti application layer uzbrukumiem citām sistēmām, mēstuļu izsūtīšanai
- Var vākt dažādus lietotāja datus

Botnet

•Windows lietotāju ir vairāk, taču **maldīgs** ir uzskats, ka UNIX/Mac OS mašīnas ir pasargātas

CERT.LV pētīts botnet

- 38 :Darwin
- 161 :FreeBSD
- 378 :Linux
- 3 :SunOS

Neviena Windows mašīna!

Dažas noderīgas adreses

Failu antivīrusu pārbaude- http://www.virustotal.com/
Pārlūkprogrammas drošības pārbaude - https://browsercheck.qualys.com/
Kaspersku Virus Removal- http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
Bitdefender Rescue CD- http://kb.bitdefender.com/site/article/650/

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