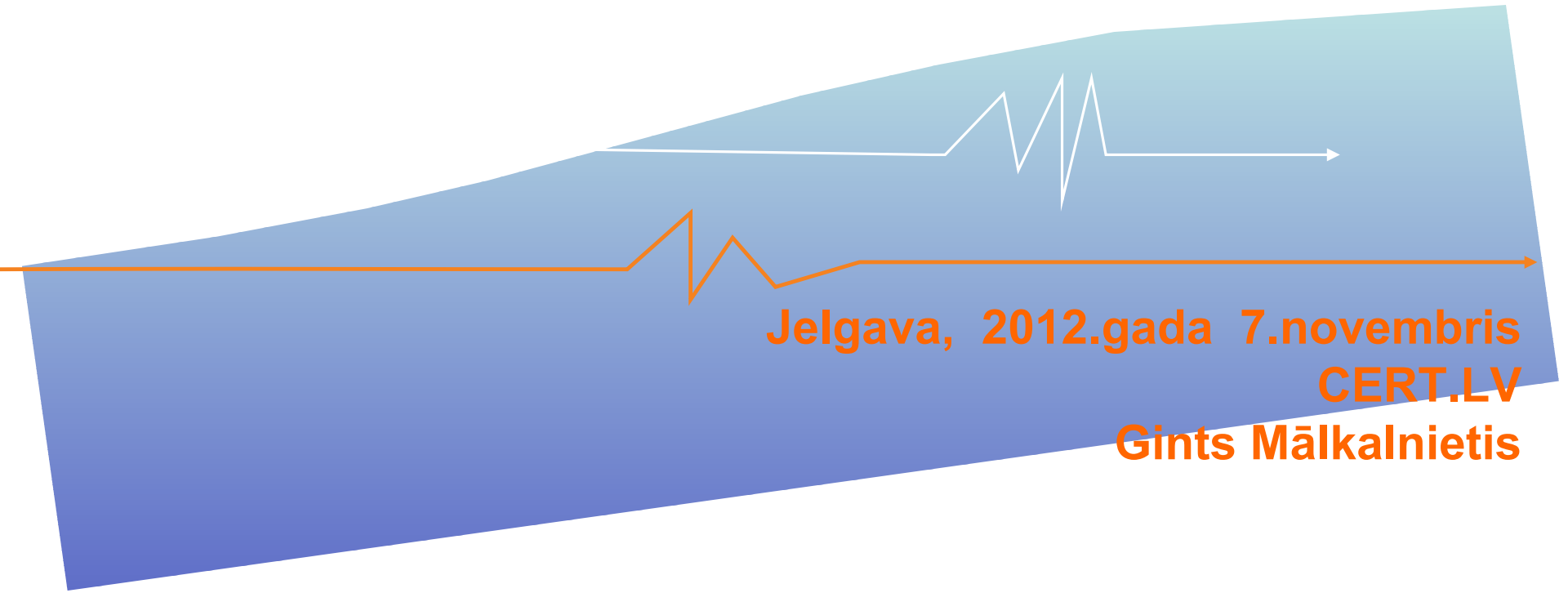
Cīņa ar robotu tīkliem un citām infekcijām



Jelgava, 2012.gada 7.novembris

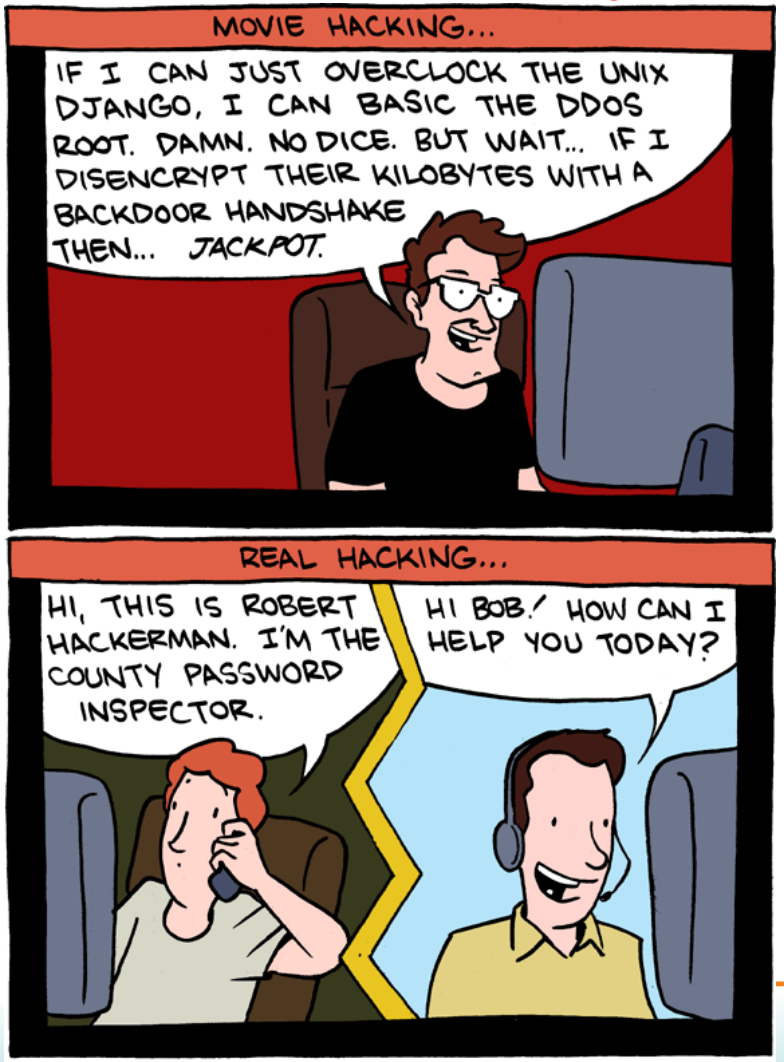
CERT.LV
Gints Mālkalnietis

Saturs

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

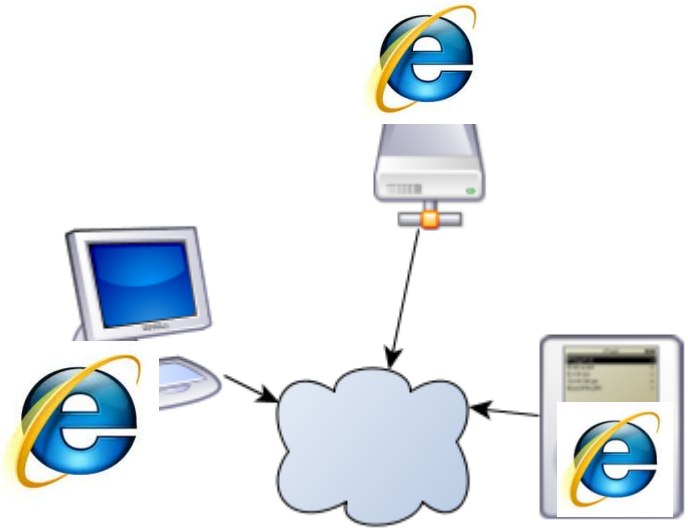
Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



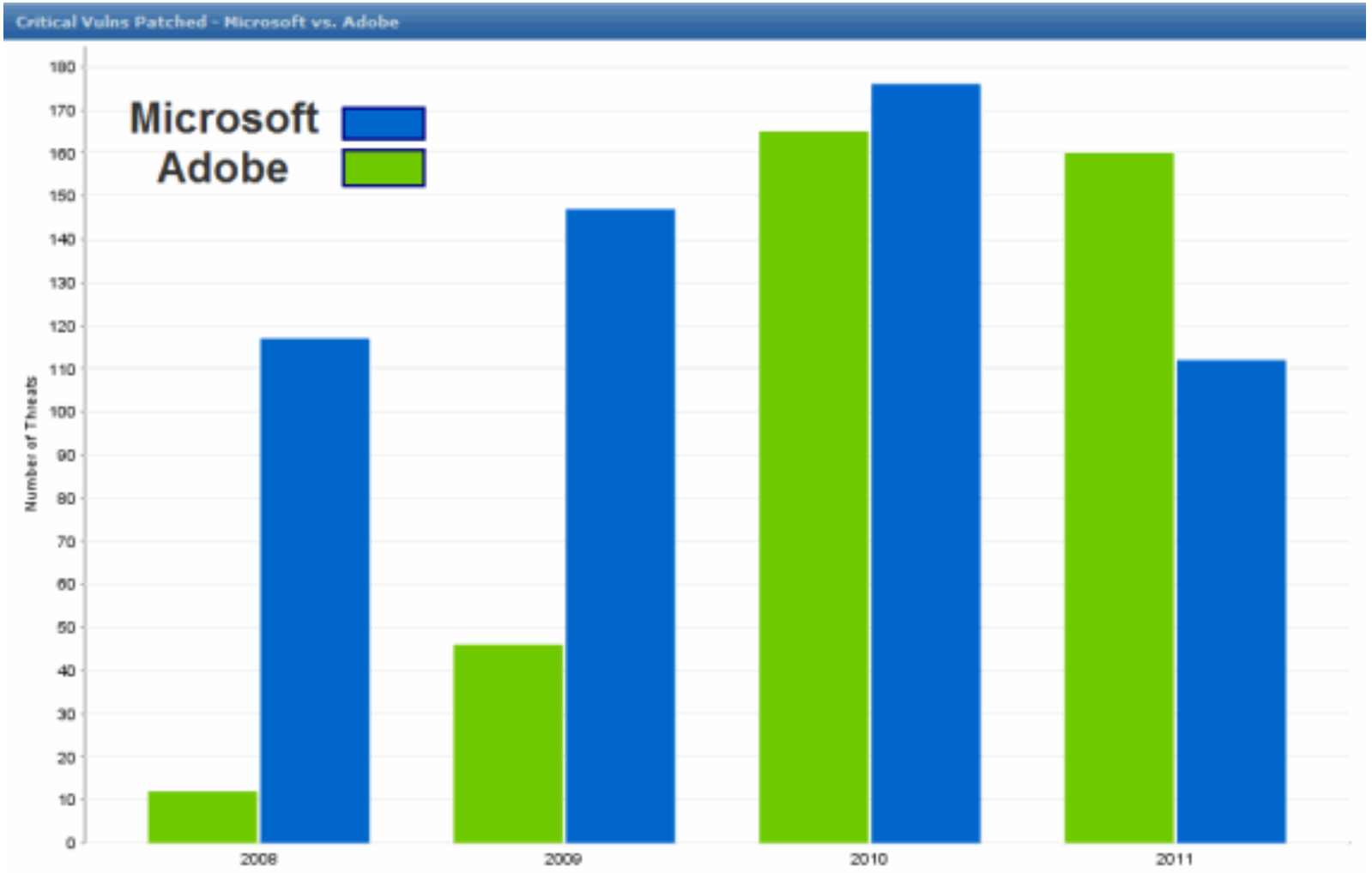
Interneta pārlūks = dators (OS + app.)

- 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

Uzbrucēju mērķauditorija

1. Sociālo tīklu lietotāji
   - %{HTTP_REFERER} ^(tweet|twit|linkedin|instagram|facebook\.|myspace\.|bebo\.)
   - %{HTTP_REFERER} ^(hi5\.|blogspot\.|friendfeed\.|friendster\.|google\.)
1. Apmeklētāji no dažādiem meklēšanas rīkiem
   - %{HTTP_REFERER} ^(yahoo\.|bing\.|msn\.|ask\.|excite\.|altavista\.|netscape\.)
   - %{HTTP_REFERER} ^(aol\.|hotbot\.|goto\.|infoseek\.|mamma\.|alltheweb\.)
   - %{HTTP_REFERER} ^(lycos\.|metacrawler\.|mail\.|dogpile\?)



Uzbrukumam izvēlētās OS

1. Visvairāk uzbrukumu tēmēti populārākajai OS – MS Windows

```
%{HTTP_USER_AGENT}  .*Windows.*
```

1. Ne visas Windows versijas ir “interesantas” uzbrucējam

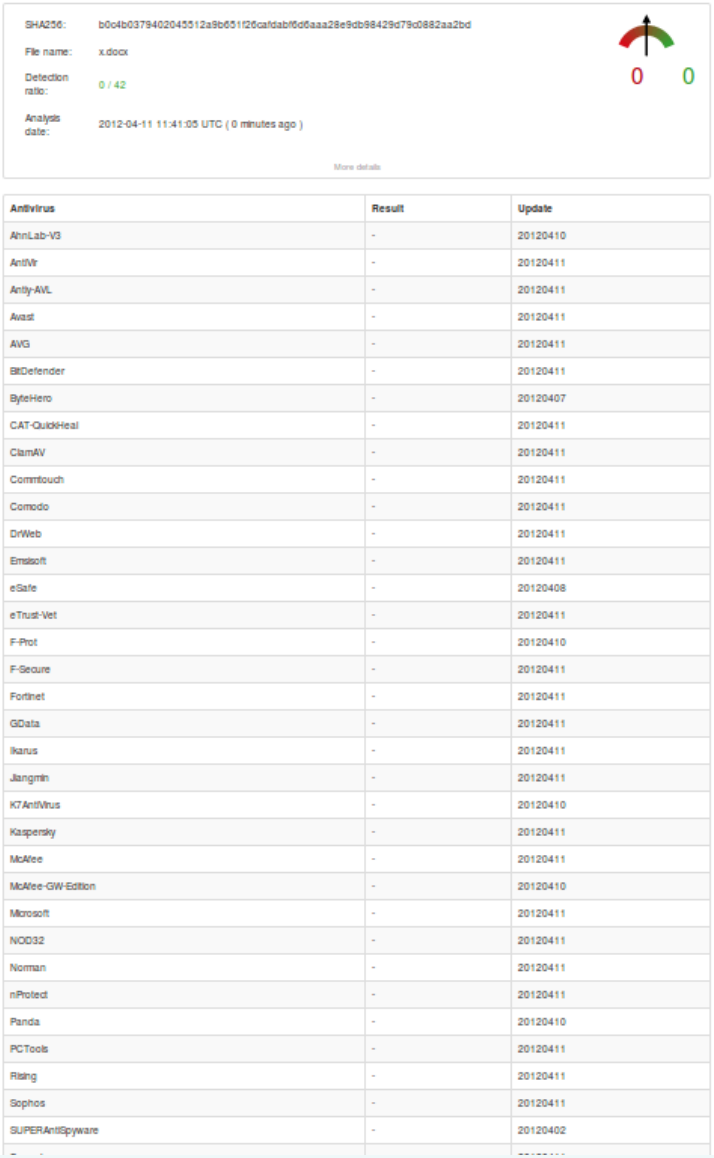
```
%{HTTP_USER_AGENT}  !^.*(Win16|Win95|Win98|Windows\s95|
    Windows\s98|Windows\sCE|Windows\sNT\s4)
```

1. Uzturēt vīrusa versijas visām OS ir darbietilpīgi un dārgi
2. Tas nenozīmē, ka nelietojot Windows nebūsiet apdraudēts!

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

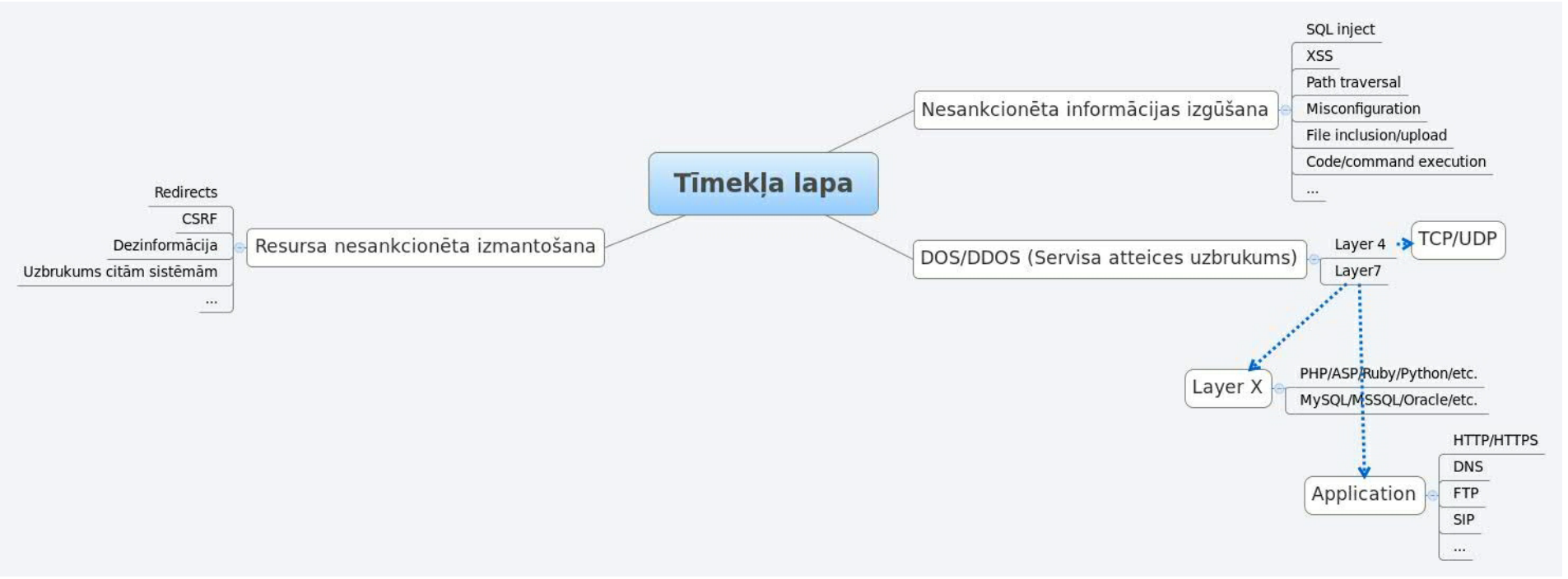
Analysis date: 2012-04-11 11:41:05 UTC

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

Vērtības jūsu datorā

1. Nauda bankas kontā
2. Kredītkaršu dati
3. Gmail konts – tajā ir ne tikai e-pasts
4. Twiitter, Facebook, Hotmail konts
5. Tiešsaistes spēļu konti un virtuālie spēļu rīki
6. Pases dati – var tikt izmantoti viltotas pases izgatavošanā!
7. Privātas fotogrāfijas šantāžai
8. Datora resursi – webcoin mining, paroļu uzlaušana, DDOS, mēstuļu izsūtīšana

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 robotu tīklu
- 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
- Robotu tīkla lietošanai jābūt labai motivācijai un/vai līdzekļiem:
  - Uzbrukums vienai mājas lapai “izgaismo” robotu tīkla IP adreses
  - Vai tas ir tā vērts?

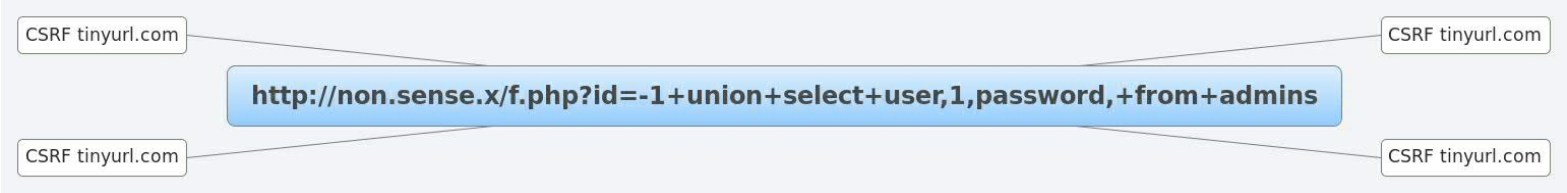
Nozieguma pēdu slēpšana

- 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

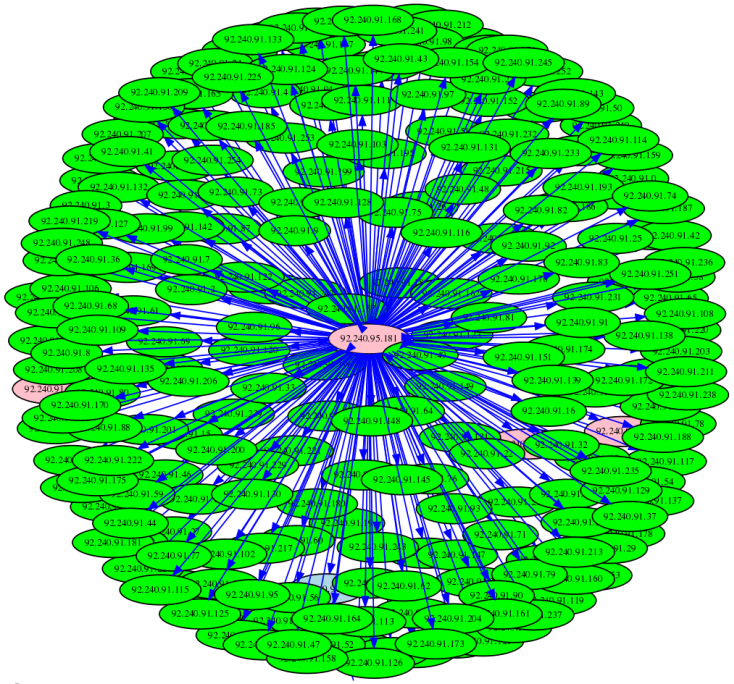
Nozieguma pēdu slēpšana

```
<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, ...

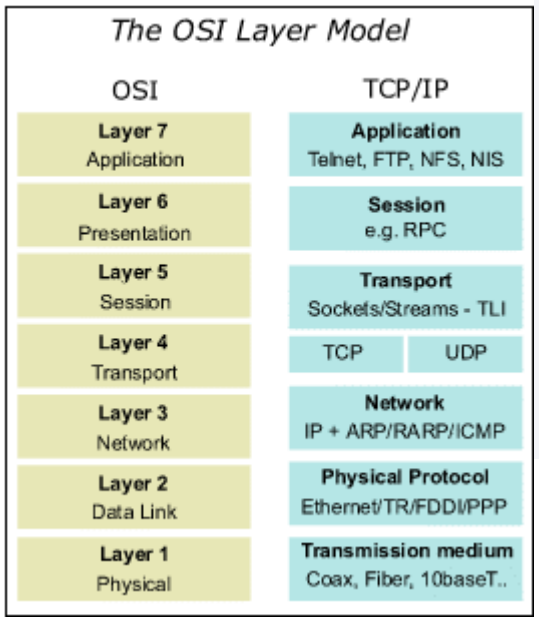


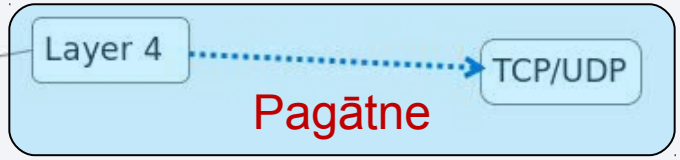
http://tinyurl.com/abcdf

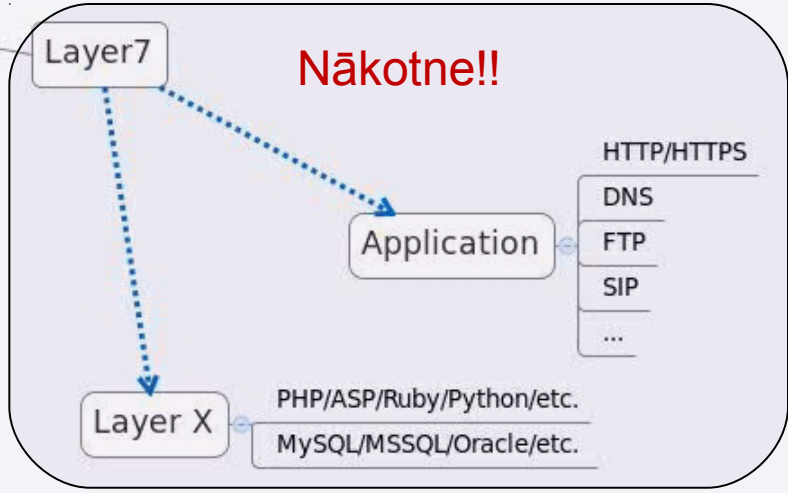
http://non.sense.x/f.php?id=-1+union+select+user,1,password,+from+admins

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 robotu tīklu
- SIP/HTTP/HTTPS/DNS
- ASP/PHP/Ruby/Python...

Robotu tīkls

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

Robotu tīkla datori

•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!

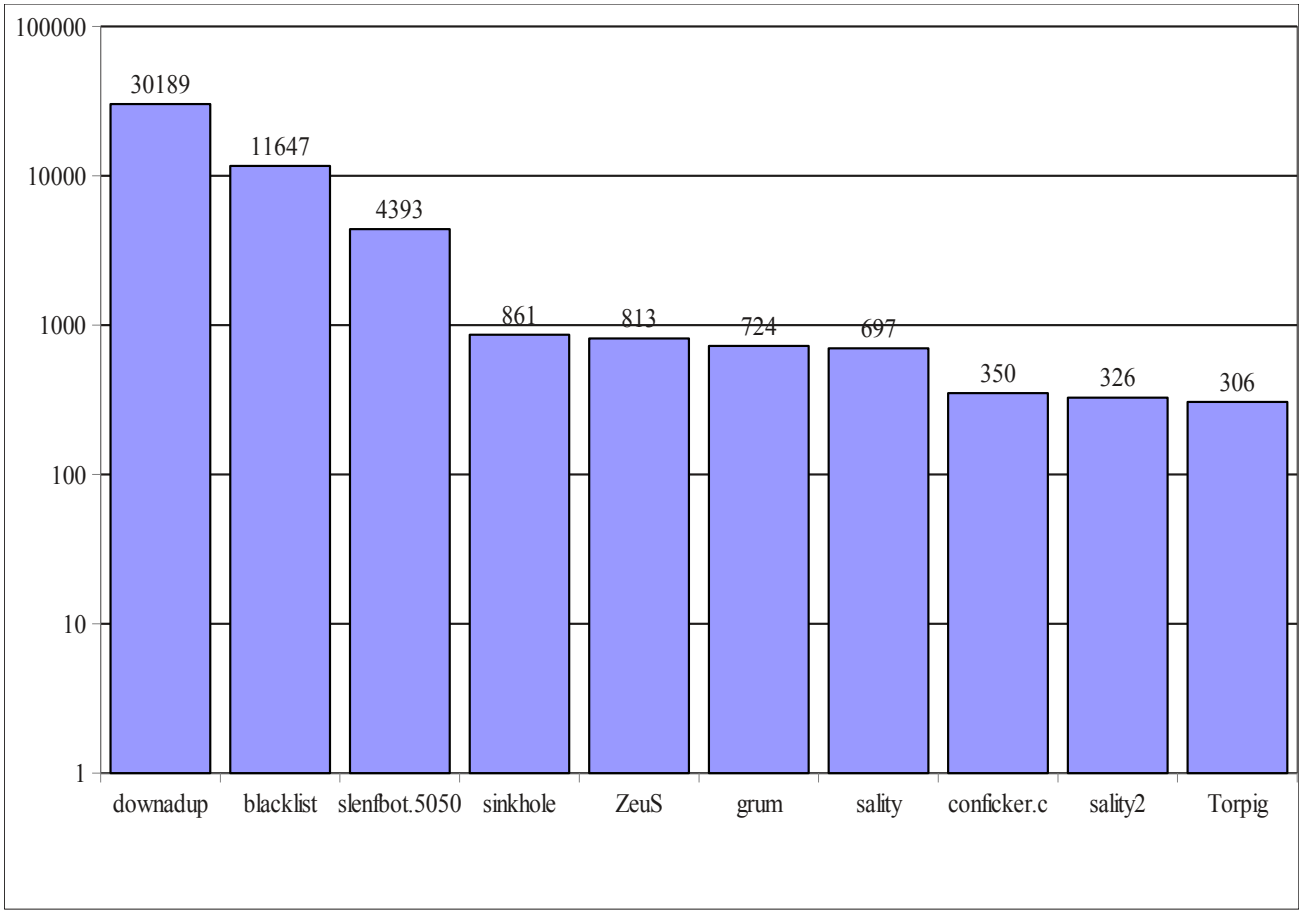
Datu “mākonis” – neglābj no vecām kļūdām!

• 2009 – Vairāk kā 300 dokumentu par TWITTER biznesa plāniem tika nozagti no Google Apps. Iemesls – vāja parole.
• 2010 – Izveidota programma WiFi paroļu uzlaušanai, 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.

Aktuālā situācija

- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS

Zemas prioritātes incidenti – 3.ceturksnis – 52066 - Infekciju TOP10



Atbildīgs interneta pakalpojumu sniedzējs

ATBILDĪGS INTERNETA PAKALPOJUMU SNIEDZĒJS ir kvalitātes zīme, kuru var saņemt Elektronisko sakaru pakalpojumu komersants, kurš:

- Sadarbojas ar CERT.LV un informē gala lietotājus par to, ka viņu datori ir inficēti ar kādu no datorvīrusiem un kļuvuši par robotu tīklu sastāvdaļu
- Sadarbojas ar Net-Safe Latvia Drošāka interneta centru, lai nodrošinātu iespējami ātru nelegālā satura (bērnu pornogrāfijas) izņemšanu no publiskas aprites internetā
- Pēc klientu pieprasījuma nodrošina bezmaksas interneta satura filtru uzstādīšanu atbilstoši Elektronisko sakaru likumam

Atbildīgie interneta pakalpojumu sniedzēji

IZZI

LATNET
biznesa klases internets

dtg
Datu tehnoloģiju grupa

interneta pasaule

sigma net

SPX IT

ILVA

lattelecom

LANET
Latvian Academic Network

Ukash – izspiedējvīruss latviski

LATVIJAS POLICJA

Uzmanību!

IP: [redacted]
Vieta: LV,Latvia,Riga

Uzmanību! Jūsu dators ir bloķēts, vismaz viena iemesla dēļ no tiem, kuri ir noradīti zemāk.

Jūs pārkāpat «Autortiesību un blakustiesību aizsardzības likumu» (Video, mūzika, programmatūra) un nelikumīgi izmantojiet vai izplatiet informāciju, kas aizsargāta ar autortiesībam, tādējādi pārkāpjot Latvijas Kriminālprocesa kodeksa 128. pantu.

Krimināprocesa kodeksa 128. pants paredz sodu no **2** līdz **500** minimālu algu vai brīvības atņemšanu no **2** līdz **8** gadiem.

Jūs skatījāt vai izplatāt aizliegta pornogrāfiska satura (Bērnu pornogrāfija / zoofīlija u t.t.) informāciju, tādējādi pārkāpjot Latvijas Kriminālprocesa kodeksa 202. pantu.

Krimināprocesa kodeksa 202. pants paredz brīvības atņemšanu no ▫▫**4** līdz **12** gadiem.

Nelikumīga piekļuve datora datiem ir uzsākta no Jūsu datora, vai Jūs...

Krimināprocesa kodeksa 208. pants paredz sodu līdz **LVL 100.000** un / vai brīvības atņemšanu no **4** līdz **9** gadiem.

Nelegālā piekļuve ir uzsākta no Jūsu datora bez Jūsu ziņas vai piekrišanas, Jūsu dators var būt inficēts ar ļaunprātīgu programmatūru, tādējādi Jūs pārkāpjat likumu par nevīžīgu personāla datora izmantošanu.

Krimināprocesa kodeksa 210. pants paredz naudas sodu no **LVL 2.000** līdz **LVL 8.000**.

Spama izplatīšana vai cita prettiesiska reklāma ir veikta no Jūsu dator,a kā peļņas iegušanas aktivitāte vai bez Jūsu zināšanas, Jūsu dators var būt inficēts ar ļaunprātīgu programmatūru.

Krimināprocesa kodekss paredz naudas sodu līdz **LVL 250.000** un brīvības atņemšanu līdz **6** gadiem. Ja šī darbība ir veikta bez Jūsu zināšanas, Jums tiek piemerots Latvijas

paysafecard Ukash

Code | Sum 100

1 2 3 4 5 6 7 8 9 0

Pay PaySafeCard | Pay Ukash

Kur es varu nopirkt PaySafeCard?

Latvijā PaySafeCard tu vari iegādāties visos **Plus Punkt** s veikalos un **Narvesen**.

plus punkts NARVESEN

Kur es varu nopirkt Ukash?

Jūs varētu iegādāties Ukash daudzās vietās,

LATVIJAS POLICIJAS
KIBERNOZIEGUMI DEPARTAMENTS

Lai atbloķētu Jūsu datoru un izbēgtu no kriminālvajāšanas, Jums nepieciešams veikt samaksu 50 LVL izmērā.

Visas operācijas, kas ir veiktas uz šī datora, pierakstās.
Ja jūs izmantojat veb-kameru, video un foto saglabājas identificējumam.

Video ierakstīšanas: **PAR**

Jūs var viegli identificēt pa Jūsu IP adresi un saistītu ar viņu domēna vārdu.

Jūsu IP adrese:
Domēna vārds: **SIA Lattelekom**
Atrašanās vieta: **Latvia , Riga**

Jūsu dators ir bloķēts!

Jūsu datora darbs ir apturēts neatrisinātas kiberaktivitātes pazīmju dēļ.

Zemāk ir minēti iespējamie pārkāpumi, ko Jūs paveicat:

Pants 274. - Autortiesības
Naudas sods vai brīvības atņemšana uz laiku līdz 4 gadiem
(Failu, ko aizsargā autortiesības, izmantošana vai izplatīšana - filmas, programmatūra)

Pants 183. – Pornogrāfiska produkcija
Naudas sods vai brīvības atņemšana uz laiku līdz 2 gadiem
(Pornogrāfisku failu izmantošana vai izplatīšana)

Pants 184. – Pornogrāfiska produkcija ar bērnu piedalīšanos (līdz 18 gadiem)
Brīvības atņemšana uz laiku līdz 15 gadiem
(Pornogrāfisku failu izmantošana vai izplatīšana)

Pants 104. – Terorisma Popularizēšana
Brīvības atņemšana uz laiku līdz 25 gadiem
(Jūs apmeklējat teroristisku organizāciju portālus)

Pants 297. – Nevērīga datora lietošana, kuras dēļ rādījās grūtas sekas
Naudas sods vai brīvības atņemšana uz laiku līdz 2 gadiem
(Jūsu dators ir inficēts ar vīrusu, kurš, savukārt, inficēja citus datorus)

Pants 108. - Azartspēles
Naudas sods vai brīvības atņemšana uz laiku līdz 2 gadiem
(Jūs spēlējāt azartspēles, bet ar Jūsu valsts likumu azarta bizness ir aizliegts)

Sakarā ar Valdības lēmumu 22.augusta, visi dotie tiesību pārkāpumi var būt aplūkoti kā nosacīti, naudas soda apmaksas gadījumā.

Naudas soda summa ir 50 LVL. Apmaksa jāveic 48 stundu laikā, pēc pārkāpšanas atklāšanas.

Ja naudas sods netiks apmaksāts, uz jums automātiski tiks uzsākta kriminālliet a.

Pēc naudas soda apmaksas Jūsu dators tiks atbloķēts

Ukash

Jūs varat saņemt Ukash no simtiem tūkstošu vietnēs visā pasaulē, tiešsaistes portfeļi, kioskos un bankomāti.

Samainiet skaidru naudu uz Ukash vaučeru un ievediet vaučera kodu formā, kas ir sniegta zemāk.

Kods: 1 2 3 4 5 6 7 8 9 0 **Iesniegt**

Kur var nopirkt Ukash

sfera
WenaCallshop
e-Bizz

paysafecard

Latvijā paysafecard tu vari iegādāties visos Plus Punkts veikalos un Narvesen.

Samainiet skaidru naudu uz Paysafecard vaučeru un ievediet vaučera kodu formā, kas ir sniegta zemāk.

Kods: 1 2 3 4 5 6 7 8 9 0 **Iesniegt**

Kur var nopirkt Paysafecard

NARVESEN
plus punkts sveigi sīkumi

Lūdzu, pievērsiet uzmanību: naudas sods ir jāapmaksā 48 stundu laikā. Ja jums neizdevās veikt samaksu norādītajā laika, atbloķēt Jūsu datoru būs neiespējams.

Šajā gadījumā uz jums automātiski tiks uzsākta kriminālliet a.

100%
Droši Maksājumi

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 par uzmanību!!!

Gints Mālkalnietis
Baiba Kaškina
E-pasts: gints@cert.lv, baiba@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