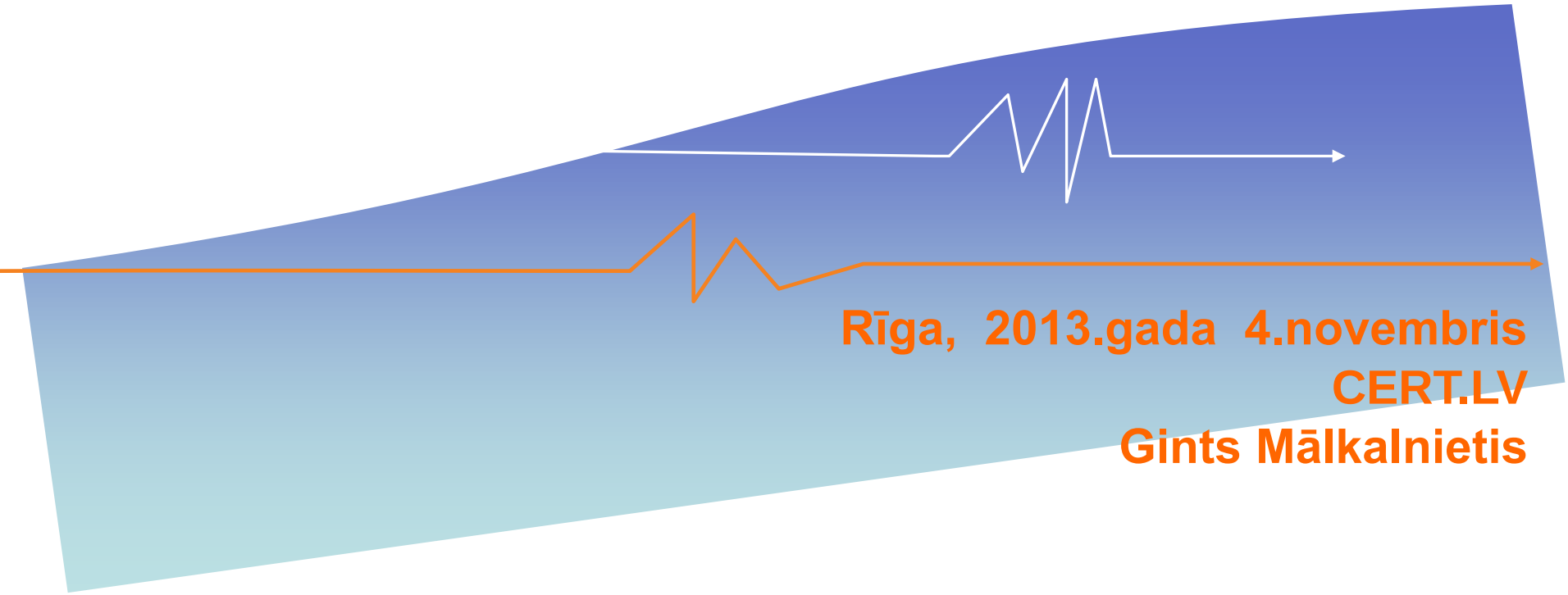
Cīņa ar robotu tīkliem un citām infekcijām



Rīga, 2013.gada 4.novembris

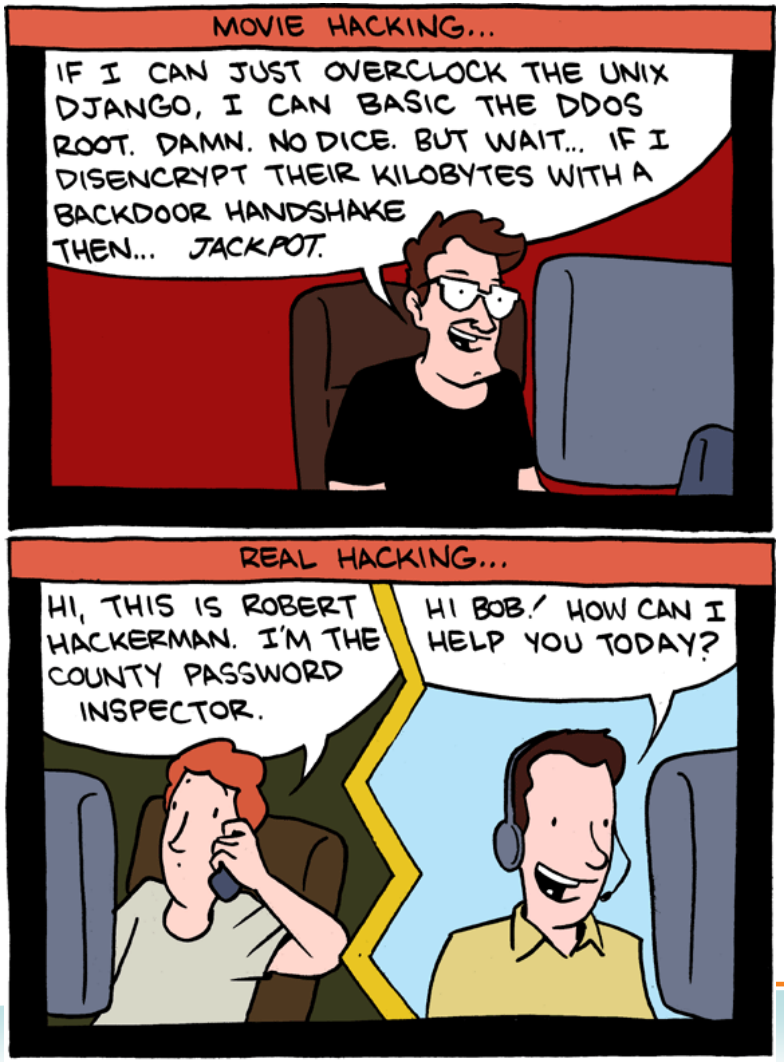
CERT.LV
Gints Mālkalnietis

Saturs

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

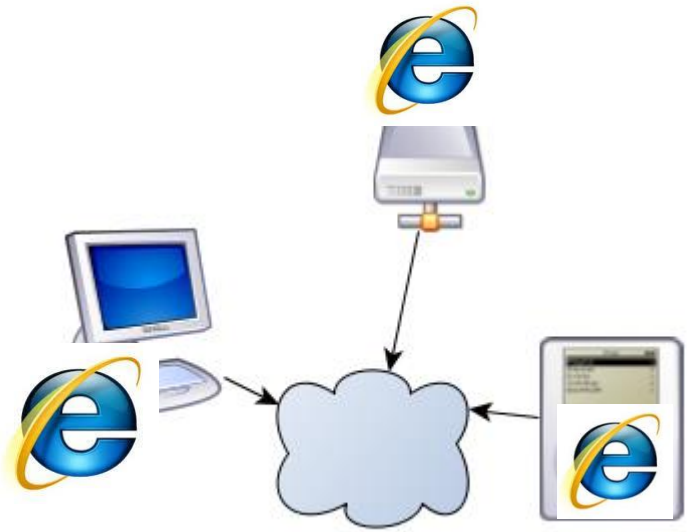
Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



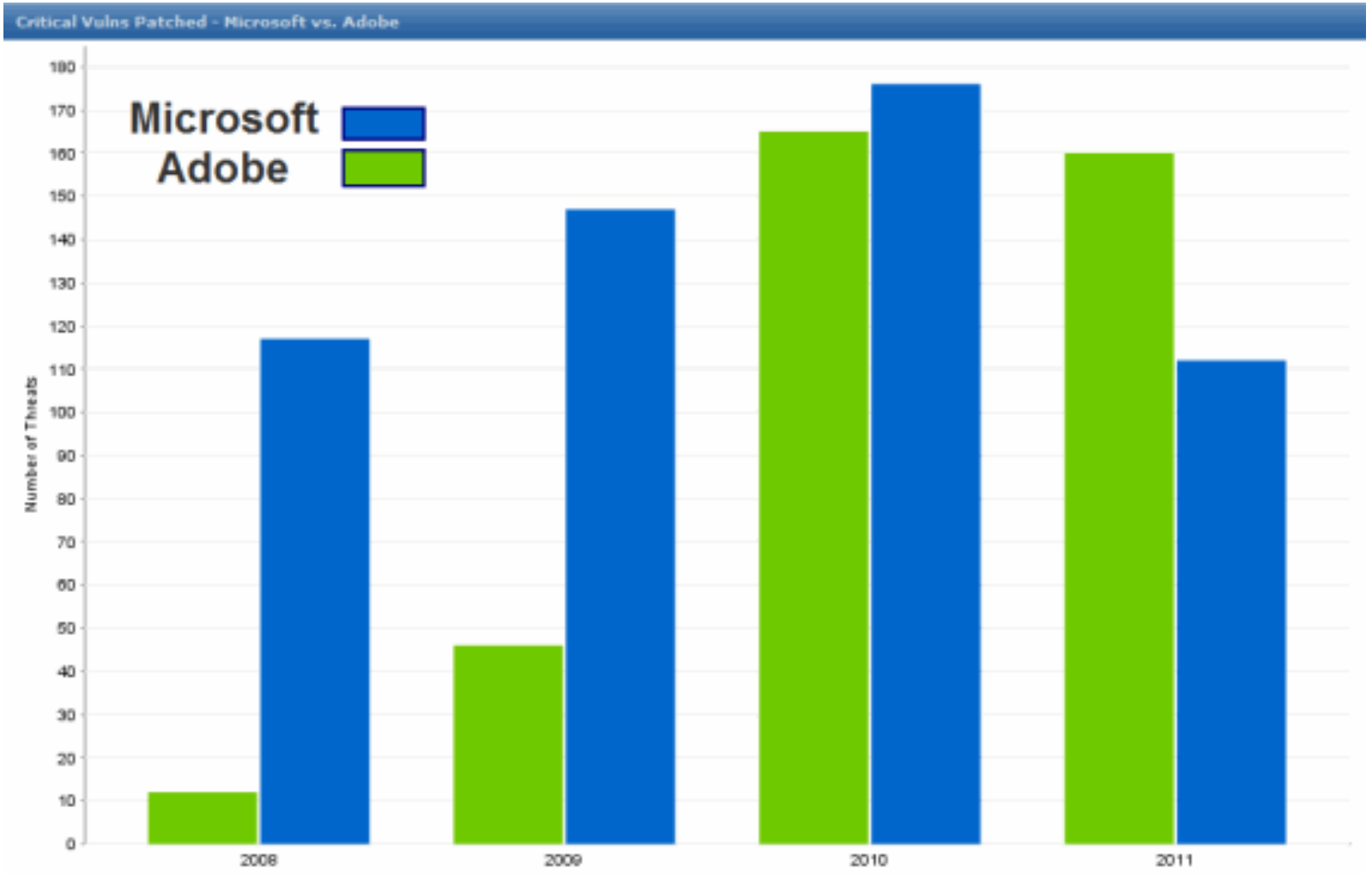
Interneta pārlūks = dators (OS + app.)

- 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\.)
2. 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.*
```

2. Ne visas Windows versijas ir “interesantas” uzbrucējam

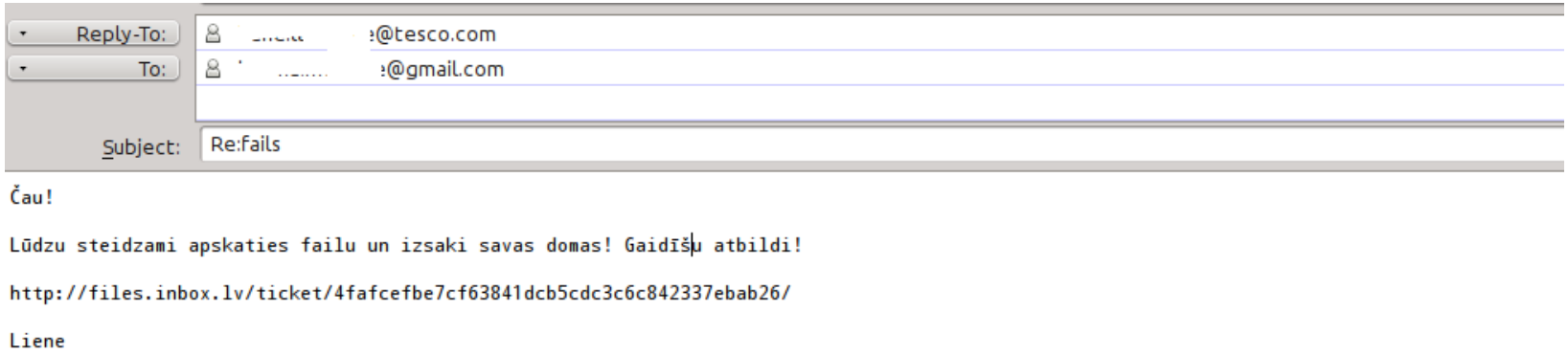
```
%{HTTP_USER_AGENT}
    !^.*(Win16|Win95|Win98|Windows\s95|Windows\s98|Windows\sCE|
    Windows\sNT\s4)
```

3. Uzturēt vīrusa versijas visām OS ir darbietilpīgi un dārgi
4. 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

Uzbrukuma mērķis – cilvēks!



- Saistošs teksts, lai mudinātu atvērt failu

Čau!
Lūdzu steidzami apskaties failu un izsaki savas domas! Gaidīšu atbildi!

- Vēstule atsūtīta no zināmas personas
- Fails izvietots Latvijas vietnē

http://files.inbox.lv/ticket/4fafcefbe7cf63841dcb5cdc3c6c842337ebab26/

virustotal

SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9cfc8f6

File name: rc_atskaite_371.exe

Detection ratio: 0 / 48

Analysis date: 2013-10-03 07:39:42 UTC (0 minūšu ago)

More details

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum		20131002
AhnLab-V3		20131002
AntiVir		20131002
Antiy-AVL		20131003
Avast		20131003
AVG		20131002
Baidu-International		20131002
BitDefender		20131003
Bkav		20131002
ByteHero		20130928
CAT-QuickHeal		20131003
ClamAV		20131003
Commtouch		20131003
Comodo		20131003
DrWeb		20131003
Emsisoft		20131003
ESET-NOD32		20131002
F-Prot		20131003
F-Secure		20131003
Fortinet		20131003

CERT.LV

- Reāla datorvīrusa izplatīšanas kampaņa
- Jauna vīrusa versija – ik pa 12 stundām
- Profesionāli kaitīgā koda veidotāji izmanto automatizētus rīkus sava koda slēpšanai

virustotal

SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9cfc8f6

File name: rc_atskaite_371.exe

Detection ratio: 12 / 47

Analysis date: 2013-11-04 07:36:01 UTC (0 minūšu ago)

More details

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum	✓	20131103
AhnLab-V3	Trojan/Win32.Zbot	20131104
AntiVir	✓	20131104
Antiy-AVL	✓	20131101
Avast	Win32:Malware-gen	20131104
AVG	✓	20131103
Baidu-International	✓	20131103
BitDefender	✓	20131104
Bkav	✓	20131102
ByteHero	✓	20131028
CAT-QuickHeal	✓	20131103
ClamAV	✓	20131104
Commtouch	✓	20131104
Comodo	UnclassifiedMalware	20131104
DrWeb	✓	20131104
Emsisoft	✓	20131104
ESET-NOD32	a variant of Win32/Injector.ANTK	20131103
F-Prot	✓	20131104
F-Secure	✓	20131104
Fortinet	✓	20131104

CERT.LV

- Atkārtota analīze mēnesi vēlāk – detektē tikai 12 no 47 AV!
- Citas šīs kampaņas vīrusa versijas ķer vairāki AV
- Datorvīruss nodarbojas ar vairāku Latvijas banku tiešsaites piekļuves paroļu zādzību
- Kopē arī citas datorā ievadītās paroles

Atbalsts un aizsardzība:

Atlikušais laiks: 47:52:08

paysafecard

IP: [redacted]

Valsts: **LV Latvia**
Rajons: **Riga**
Pilsēta: **Riga**
ISP: **SIA Lattelecom**
OperētājSistēma: **Windows XP (32-bit)**
Lietotāja Vārds: **Ginc**

UZMANĪBU! Jūsu dators ir bloķēts zemāk norādīto drošības apsvērumu dēļ.

Jūs esat apsūdzēts par aizliegtu pornogrāfisku datu (bērnu pornogrāfija/zoofilija/izvarošana utt.) skatīšanos/uzglabāšanu un/vai izplatīšanu. Jūs esat pārkāpis Vispasaules deklarāciju par bērnu pornogrāfijas neizplatīšanu. Jūs esat apsūdzēts noziegumā, kas paredzēts Latvijas Republikas Krimināllikuma 161. pantā.

Latvijas Republikas Krimināllikuma 161. pants paredz brīvības atņemšanu uz laiku no 5 līdz 11 gadiem.

Tāpat jūs tiekat turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiekat turēts aizdomās par Latvijas Republikas Krimināllikuma 148. panta pārkāpšanu.

Latvijas Republikas Krimināllikuma 148. pants paredz brīvības atņemšanu uz laiku no 3 līdz 7 gadiem vai naudas sodu no 150 līdz 550 minimālo algu apmērā.

No jūsu datora ar nelikumīgas piekļuves starpniecību iegūta pieeja valsts nozīmes informācijai un publiskai pieejai slēgtiem datiem.

Iespējams, nesankcionēto piekļuvi jūs organizējāt pats ar savtīgu nolūku, vai tā tika organizēta, jums nezinot, bez jūsu piekrišanas, ja jūsu datora darbību ietekmē kaitīga programmatūra. Jūs tiekat turēts aizdomās - līdz brīdim, kad tiks izbeigta izmeklēšana - par Latvijas Republikas Krimināllikuma 215. panta pārkāpšanu ("Likums par nolaidīgu un nevērīgu apiešanos ar datoru un datoru palīglīdzekļu").

Latvijas Republikas Krimināllikuma 215. pants paredz brīvības atņemšanu uz laiku no 5 līdz 8 gadiem un/vai soda naudu līdz LVL 100.000 latu apmērā.

PIN Kods | Summa: 50

1 2 3 4 5 6 7 8 9 0

Apmaksāt PaySafeCard

Kur es varu saņemt naudas sertifikātu PaySafeCard?

Pārskats par tirgotājiem: Latvijā PaySafeCard tu vari iegādāties visos **Plus Punkts** veikalos un **Narvesen** un **Qiwi** mašīna. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (**R-Kiosk**).

R kiosk

ca copyright alliance

“Policijas vīrusa” versijas

- Izspiež naudu, traucējot datora darbu
- Atsaucas uz Valsts Policiju un neesošiem Krimināllikuma pantiem
- Maksājumu pieprasa veikt, izmantojot UKASH kodu
- Jaunā versija vienkāršota līdz parastai weblapai – viegli novācama, toties strādā datoros ar dažādām OS!

vp.gov.lv.id146025375-5118247904.n2195.com/?flow_id=3289&569750=39670/case_id=94281

VALSTS POLICIJA

Jūsu informācija ir šifrēta. Nemēģiniet atbloķēt jūsu datoru.

Uzmanību!

Jūs pārkapāt citu personu autortiesības vai saistītas tiesības (videomateriāli, mūzika, programmatūra) un nelegāli izmantojat aizsargātus materiālus, pārkapājot 1. panta, 8. daļas, 8. noteikumu, zināmu arī, kā Latvijas republikas krimināllikums.
1. panta, 8. daļas, 8. noteikums paredz sodu no diviem līdz pieciem simtiem minimālu algu apmērā, vai brīvības atņemšanu no diviem līdz astoņiem gadiem.
Jūs esat skatījis/jusi vai izplatījis/jusi aizliegtus pornogrāfiskus materiālus (pornogrāfija ar bērniem vai citi materiāli tika atrasti jūsu datorā). Jūs pārkapāt Latvijas krimināllikuma 202. Pantu, kas paredz brīvības atņemšanu no četriem līdz divpadsmit gadiem.
Nelegāla piekļuve datiem tika iniciēta no jūsu datora bez jūsu zināšanas, kas varētu but datora piesārņojuma dēļ ar vīrusiem, toties jūs pārkapāt likumu par nolaidīgu datora izmantošanu. Latvijas krimināllikuma 210. Pants paredz sodu līdz 100,000 Eur un brīvības atņemšanu no četriem līdz deviņiem gadiem. Ievērojot krimināllikuma grozījumus (ja pārkāpums tika konstatēts pirmo reizi), jūs netiksiet sodīts, ja samaksāsiet sodu.
Lai atbloķētu jūsu datoru un izvairīties no legālam sekām, jums ir obligāti jāsamaksā atbrīvošanas maksa 100 Eur apmērā caur PAYSAFECARD (jums ir jāiegādājas PAYSAFECARD, jāpapildina konts par 100 Eur un jāievadā kods). Jūs varat nopirkt kodu jebkura veikalā vai DUS. PAYSAFECARD ir pieejama visos nacionālajos veikalos.

Kā es varu samaksāt sodu un atbloķēt savu datoru?
1. Atrādiet PAYSAFECARD tirgošanas vietu jums blakus:

QIWI · plus punkts svarīgi sīkumi · NARVESEN · R kiosk

2. Saņemiet PAYSAFECARD ar priekšapmaksas opciju un papildiniet balansu par 100 Eur skaidrā naudā pie kases.
3. Ievadiet jusu PAYSAFECARD kodu un nospiediet submit un "Atbloķējiet jūsu datoru tagad"

Jūsu IP adrese: [redacted]
Atrašanas vieta: Riga, Riga, Latvia

paysafecard — pay cash. pay safe — Drošas transakcijas forma

Ievadiet PAYSAFECARD kodu

Lūdzu ievadiet PAYSAFECARD kodu izmantojot PIN tastatūru apakšā

1	2	3	4	5	6	7	8	9	0	Izdzēst

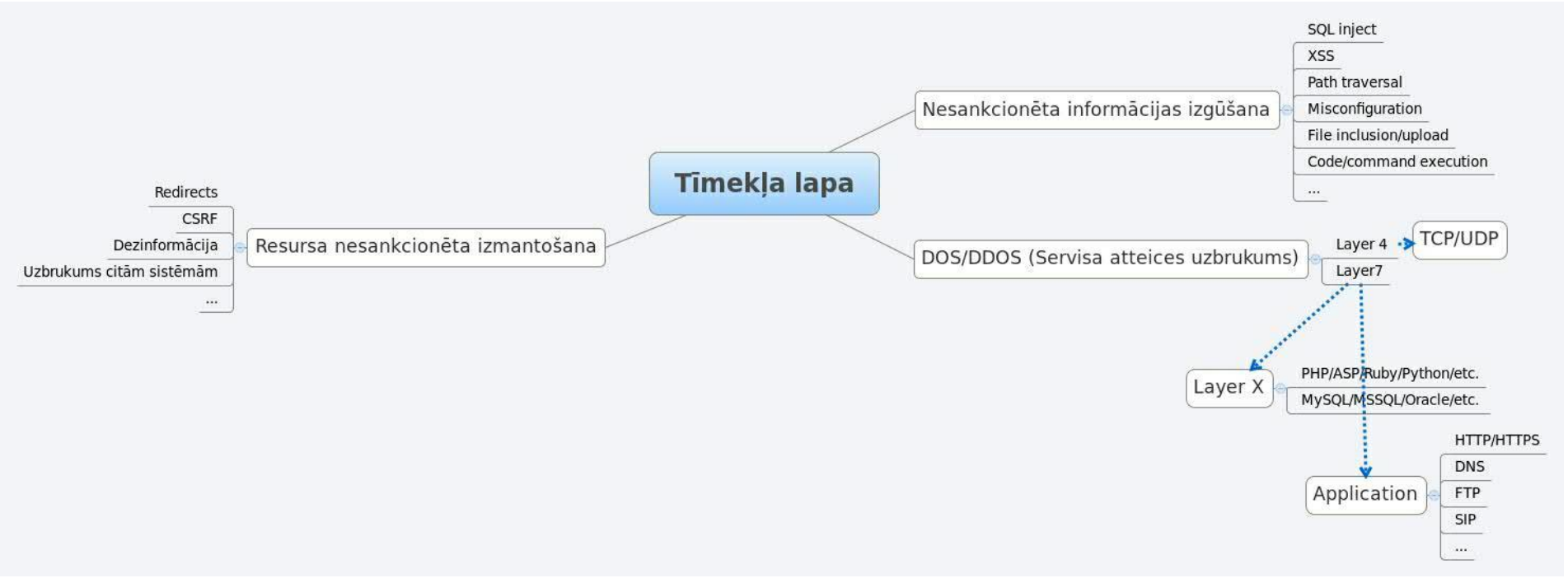
Atbloķējiet jūsu datoru tagad!

Uzmanību: Soda naudai jābūt samaksātai **12.** stundu laikā. Pēc 12. stundām nebūs iespējas samaksāt sodu.
Visi jūsu dati tiks aizturēti un pret jums tiks uzsākts kriminālprocess, ja sods nebūs samaksāts.

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

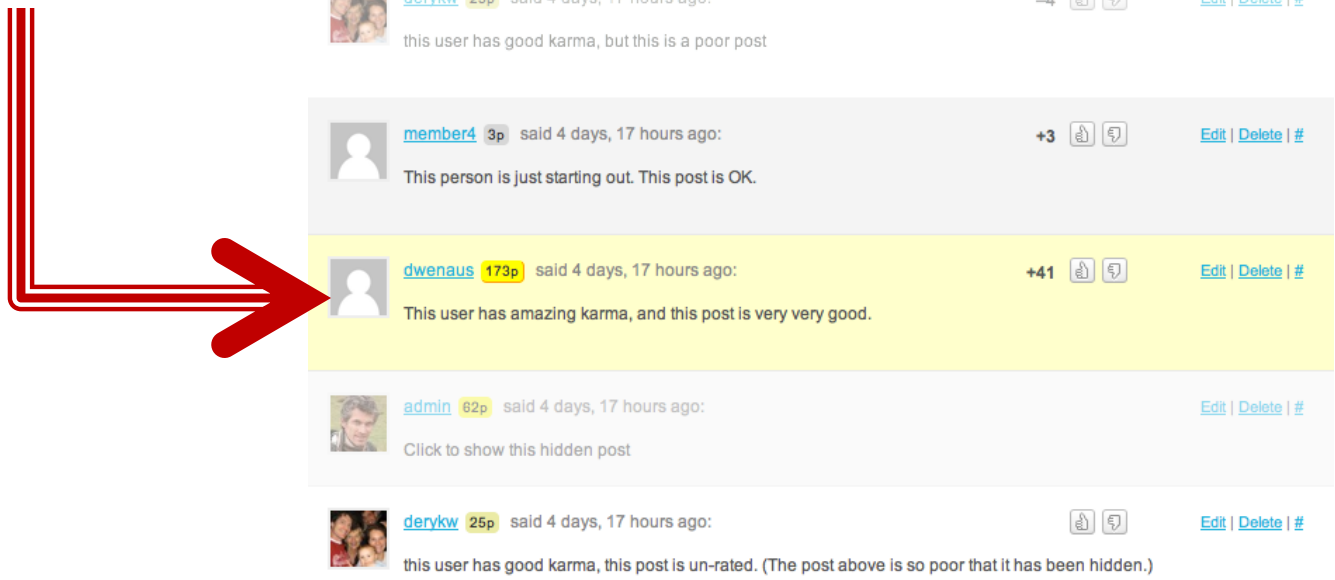
- Nelikumīgi iegūtā informācija parasti tiek publicēta ārvalstu bezmaksas resursos
- Darbības tiek veiktas no “anonīmiem” proxy servisu tīkliem, publiskiem WiFi tīkliem vai uzlauztām sistēmām
- Robotu tīkla lietošanai jābūt labai motivācijai un/vai līdzekļiem:
  - Uzbrukums vienai mājas lapai “izgaismo” robotu tīkla IP adreses
  - Vai tas ir tā vērts?

Nozieguma pēdu slēpšana

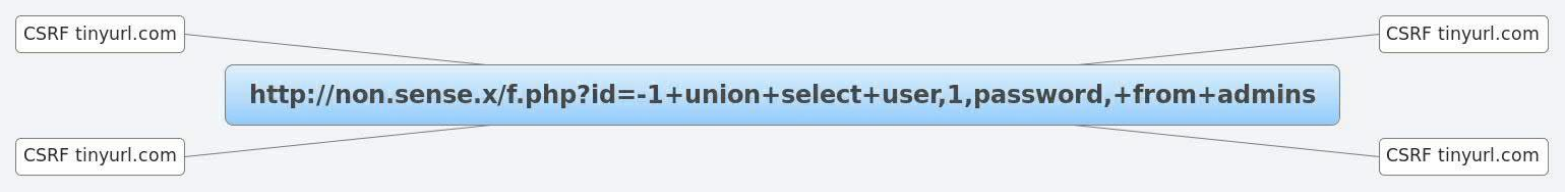
- Tiek lietoti redirect servisi - bit.ly, tinyurl.com, tiny9.com, etc.
- Saites tiek noformētas kā uzbrukums vai identiskas pieprasījumiem, ko veicis uzbrucējs
- Publicētas dažādos publiskos resursos kā saites uz bildi vai citu saturu, kas tiek automātiski pieprasīts, atverot lapu

Nozieguma pēdu slēpšana

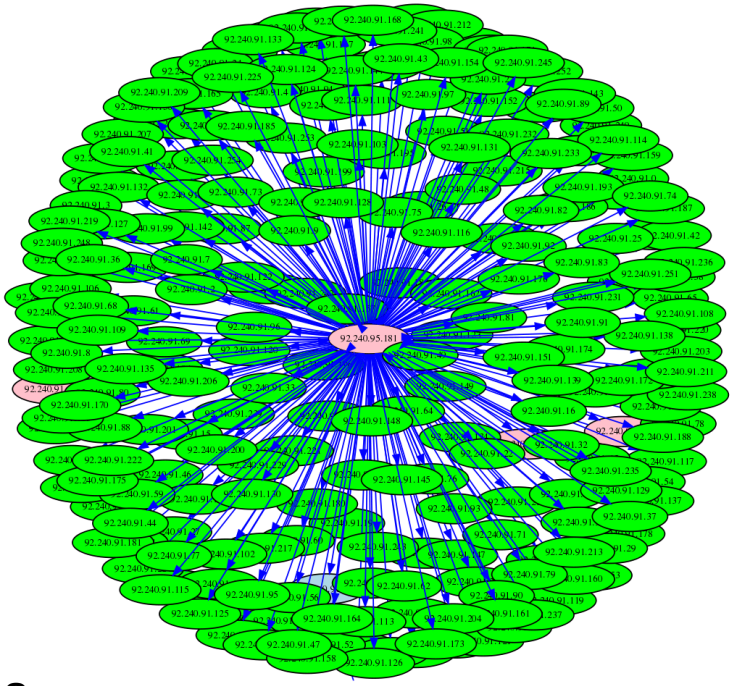
```
<img src='http://tinyurl.com/abcdf'
style='width:16px;
height:16px;' alt='[Face] ' />
```



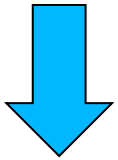
Nozieguma pēdu slēpšana



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



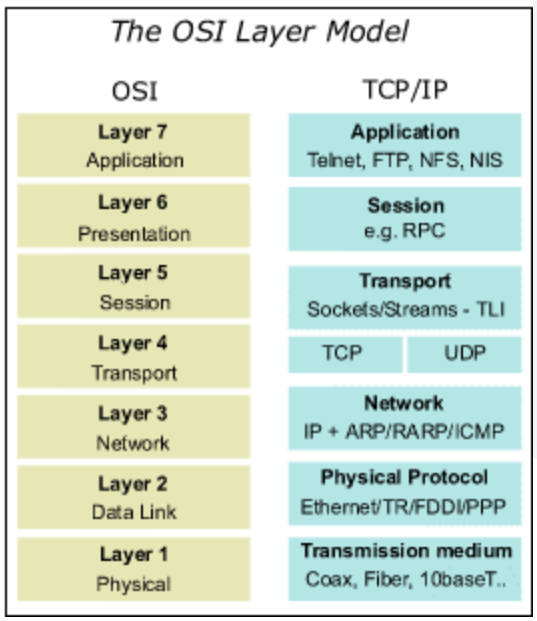
http://tinyurl.com/abcdf

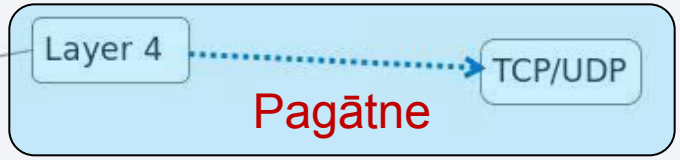


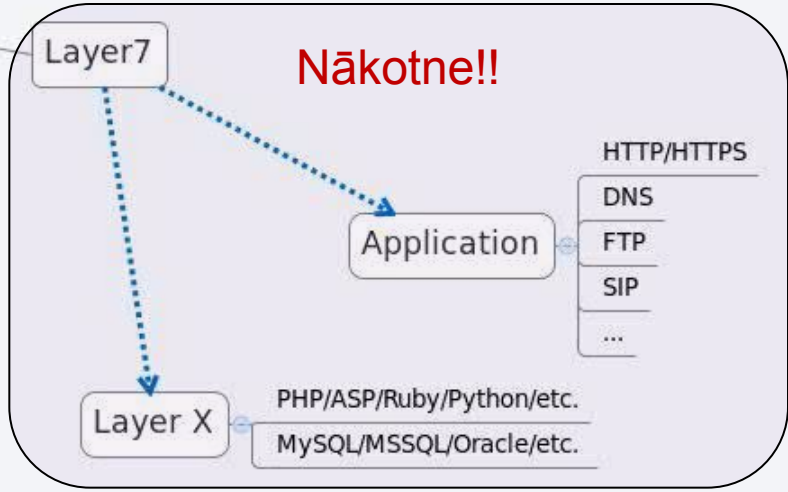
http://non.sense.x/f.php?id=-1+union+select+user,1,password,+from+admins

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.

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
E-pasts: gints.malkalnietis@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