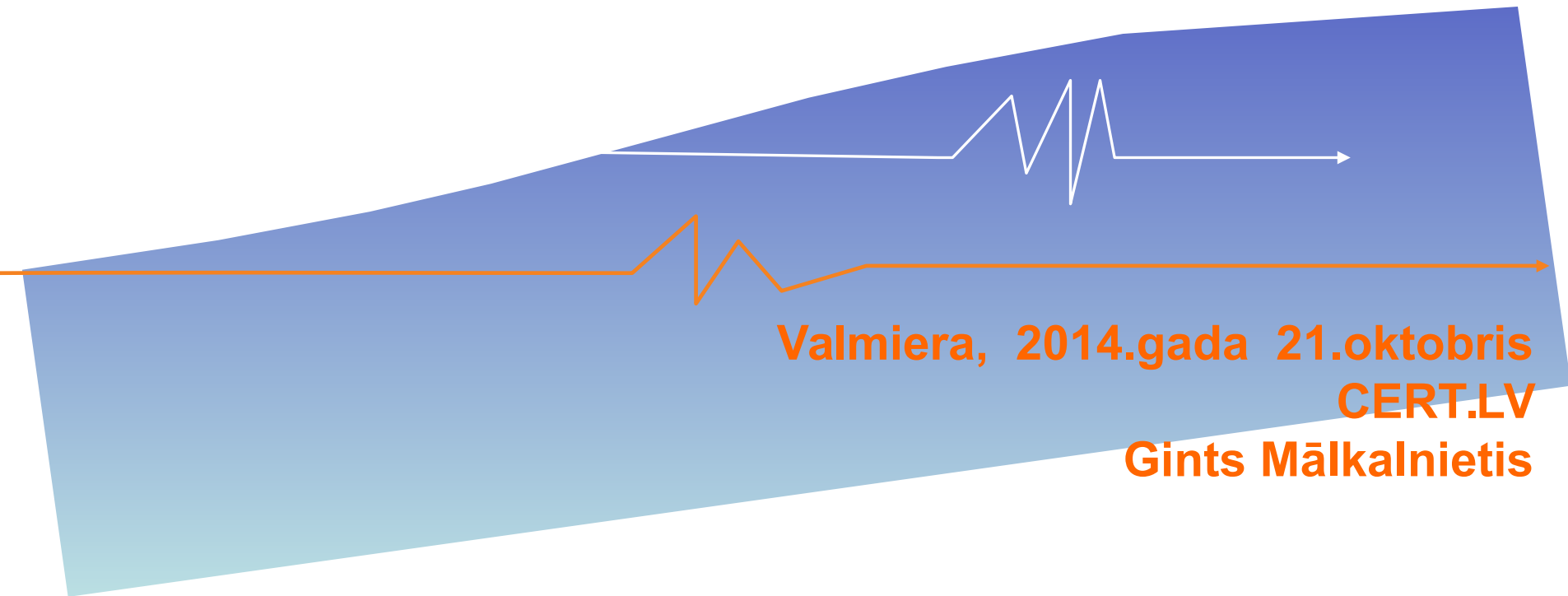


# *Cīņa ar robotu tīkliem un citām infekcijām*



## Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



## Riski mūsdienu tehnoloģijās

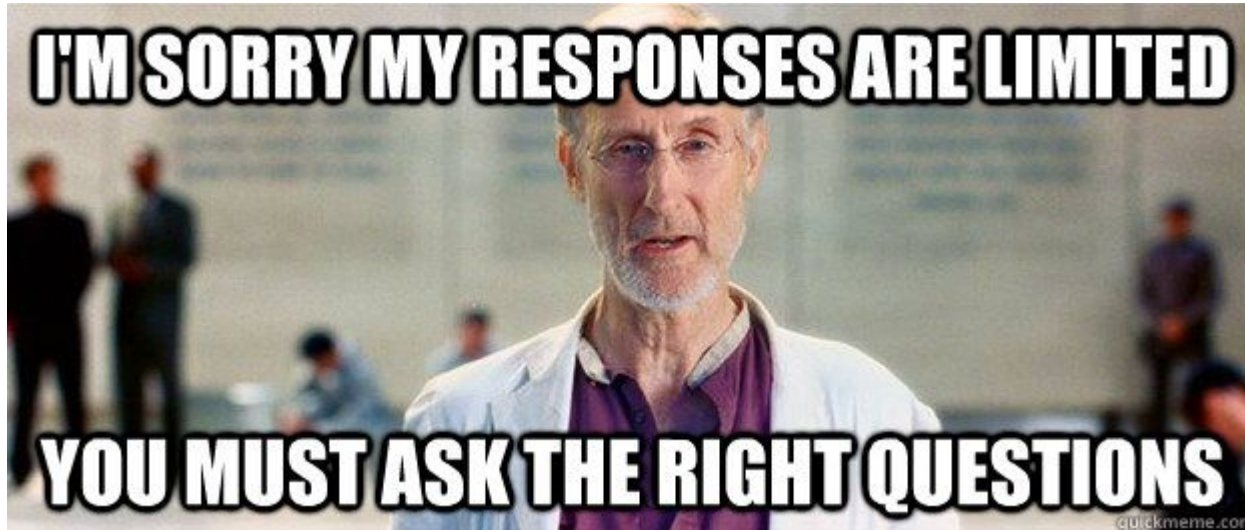
- Neviens drošības tehniskais risinājums nav 100% drošs!







Ko mēs saņemam?



Ko mēs saņemam?

The Ultimate Question of Life, the Universe,  
and Everything?



42





## Cik ātri Latvijā risināja “Heartbleed” ievainojamību:

<b>11.04.2014.</b>	<b>- 2159</b>
<b>07.05.2014.</b>	<b>- 1671</b>

Neviens no publiskajiem Latvijas servisiem nav atklāti atzinis šīs ievainojamības ietekmi uz to, un publiski brīdinājis lietotājus !



# ShellShock

{bashbug}



# POODLE Test

If you see a poodle below, then your browser supports SSLv3 and you maybe vulnerable. If you see a Springfield Terrier below, your browser doesn't support SSLv3.

The image may take a bit time to appear. The test requires JavaScript.

[Flash Webcast: What do you need to know about POODLE? \(12pm PDT, 3pm EDT, 9pm CEST\)](#)



# Neievainojamu datorsistēmu nav!

- Jebkura reāla datorsistēma satur daudz, dažādu komponentu
- Jaunatklātu ievainojamību labošanas laiks nav iepriekš zināms
- Nopietnu, bet nesalabotu, ievainojamību gadījumā, datorsistēmas īpašniekiem rodas dilemma:
  1. Turpināt izmantot sistēmu ar zināmu ievainojamību
  2. Neizmantot/ierobežot datorsistēmu līdz labojuma ieviešanai

# Pagaidu risinājumi

- Ražotāji piedāvā dažādus risinājumus operatīvai ievainojamību ietekmes novērsšanai:
  1. Uzbrukumu ierobežošana izmantojot ugunsdmūru un DPI iekārtas – tiek analizēti ienākošie dati, bloķējot zināmu uzbrukumu indikātorus saturošas paketes
  2. “Virtual patching” serverī - papildus programmas, kas pārtver/labot ienākošos pieprasījumus pirms nodošanas tālākai apstrādei
  3. Papildinājumi/filtri esošajām programmām



# Ievainojamības ietekmes izvērtēšana

- Kritiskas ievainojamības, kas atklāj sensitīvus datus, ilgtermiņa ietekmi ir sarežģīti izvērtēt:
  1. Bieži, nav precīzi zināms ievainojamības atklāšanas laiks (tas var atšķirties no publiski zināmā)
  2. Žurnālfaili var nesaturēt informāciju, kas nepieciešama, lai konstatētu sekmīga uzbrukuma faktu
  3. Sekmīgs uzbrukums var atklāt piekļuves datus citām, neievainotām, sistēmām.

# Ievainojamības ietekmes izvērtēšana

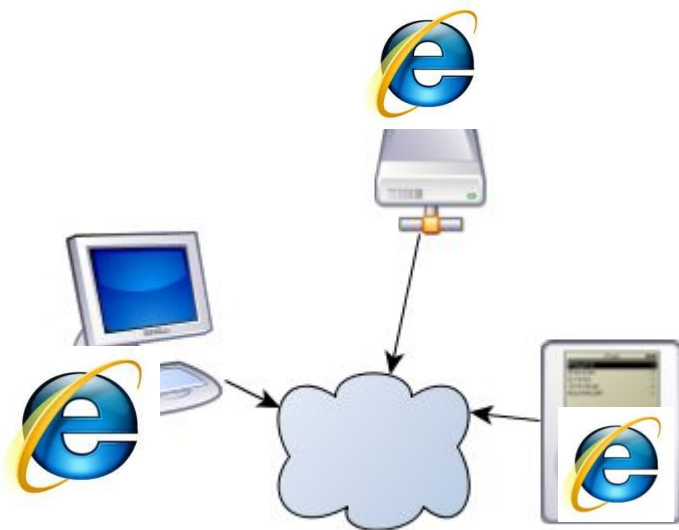
- Savstarpēji saistītas datorsistēmas:
  1. Savstarpēji saistītu datorsistēmu savstarpējā ietekme praktiski ir daudz spēcīgāka, nekā plānots tās veidojot.
  2. “Vienvirziena” komunikāciju modelis būtiski ietekmē nepieciešmo funkciju realizāciju, tāpēc praksē tiek izmantots ļoti reti.
  3. Pilnīga datorsistēmu komunikāciju apzināšana un dokumentēšana ir sarežģīta, un laiktēlpīga!

# Ievainojamības ietekmes izvērtēšana

- Uzbrukumā iegūtie autentifikācijas dati var, un tiks izmantoti atkārtoti!
  1. Vienādas paroles
  2. Nepareizi saglabātas, viegli atšifrējamās paroles
  3. SSH privātās atslēgas bez paroles
  4. Saglabāti autentifikācijas dati
- Jāparedz procedūras straujai autentifikācijas datu maiņai!
- Nav “nenozīmīgu” ievainojamību!
- Nav “lokālu” ievainojamību, ja dators ir pieslēgts tīklam, vai tam var pievienot ārējus datu nesējus!

# Interneta pārlūks = dators (OS + app.)

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





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







2.5GHz Quad Core CPU, 2GB RAM, 32 GB flešatmiņa



# 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



# 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)
```

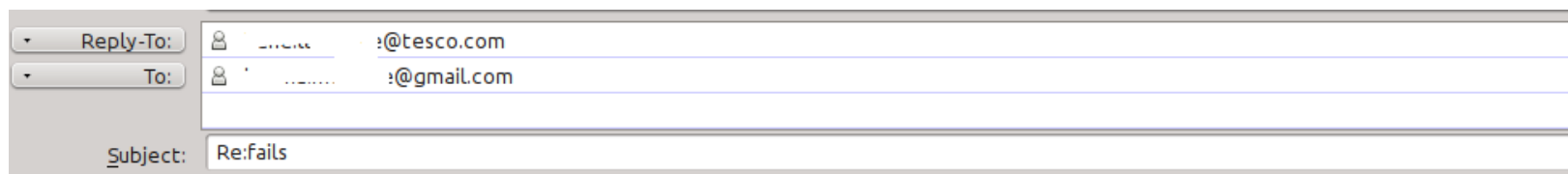
3. Uzturēt vīrusa versijas visām OS ir darbietilpīgi un dārgi
4. Tas nenozīmē, ka nelietojot Windows nebūsiat apdraudēts!

# 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!



Čau!

Lūdzu steidzami apskatiet failu un izsaki savas domas! Gaidīšu atbildi!

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

Liene

- Saistošs teksts, lai mudinātu atvērt failu

Čau!

Lūdzu steidzami apskatiet failu un izsaki savas domas! Gaidīšu atbildi!

- Vēstule atsūtīta no zināmas personas
- Fails izvietots Latvijas vietnē

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

SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9cfc8f6

File name: rc\_ataskaite\_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

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



SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9fc8f6

File name: rc\_ataskaite\_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

- 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 parolu zādzību
- Kopē arī citas datorā ievadītās paroles





Atbalsts un aizsardzība:



Atlikušais laiks: 47:52:08



IP: [REDACTED]

Valsts: LV Latvija  
Rajons: Rīga  
Pilsēta: Rīga  
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 tiek turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiek 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 organizējat pats ar savtīgu nolūku, vai tā tika organizēta, jums nezinot, bez jūsu piekrišanas, ja jūsu datora darbību ietekmē kaitīga programmatūra. Jūs tiek turēts aizdomās - līdz brīdim, kad tiks izbeigta izmeklēšana - par Latvijas Republikas Krimināllikuma 215. panta pārkāpšanu ("Likums par nolaidīgu un nevērtīgu apiešanos ar datoru un datoru palīgīdzekļiem").

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 mašīnā. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (R-Kiosk).



# “Policijas vīrusa” versijas

- Izspiež naudu, traucējot datora darbu
- Atsaukas 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!





# 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 būt 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 pārkapums tika konstatēts pirmo reizi), jūs netiksiet sodīts, ja samaksāsit 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:



**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 jūsu PAYSAFECARD kodu un nospiediet submit un "Atbloķējiet jūsu datoru tagad"



**Jūsu IP adrese:** [redacted]

**Atrašanas vieta:** Rīga,  
Rīga,  
Latvia



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. Twitter, 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, parolu 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 žurnālēšana 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

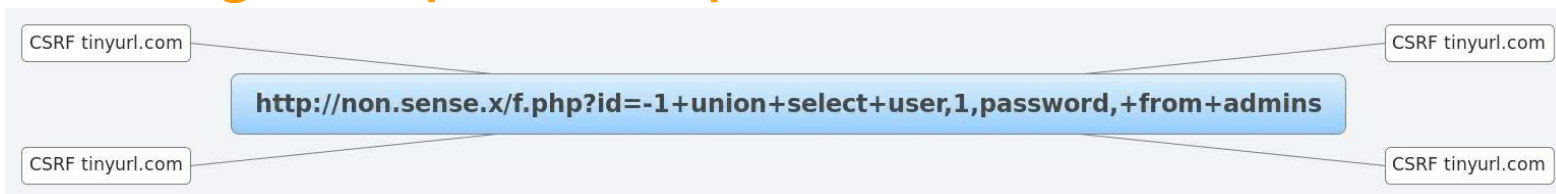
# Nozieguma pēdu slēpšana

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

The screenshot shows a forum thread with several posts. Each post includes a user profile picture, a karma value, a timestamp, and the post content. The posts are as follows:

- admin** (62p) said 4 days, 19 hours ago: This user has very good karma, and this is a good post. (+15 karma)
- derykw** (25p) said 4 days, 17 hours ago: this user has good karma, but this is a poor post. (-4 karma)
- member4** (3p) said 4 days, 17 hours ago: This person is just starting out. This post is OK. (+3 karma)
- dwenaus** (173p) said 4 days, 17 hours ago: This user has amazing karma, and this post is very very good. (+41 karma)
- admin** (62p) said 4 days, 17 hours ago: Click to show this hidden post.
- derykw** (25p) said 4 days, 17 hours ago: this user has good karma, this post is un-rated. (The post above is so poor that it has been hidden.)

# Nozieguma pēdu slēpšana

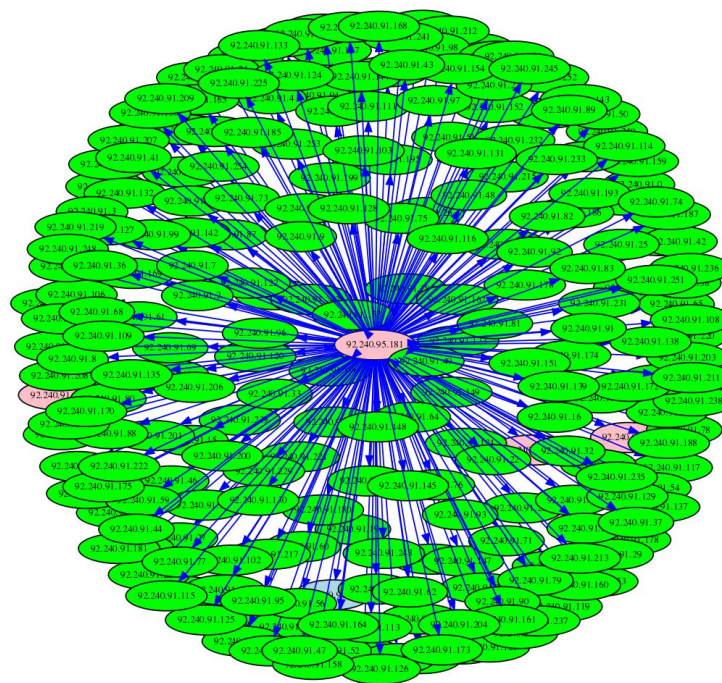


Rezultātā par uzbrucēju kļūst katrs CSRF tīmekļa lapas apmeklētājs, web meklētāji, ...

<http://tinyurl.com/abcdf>



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

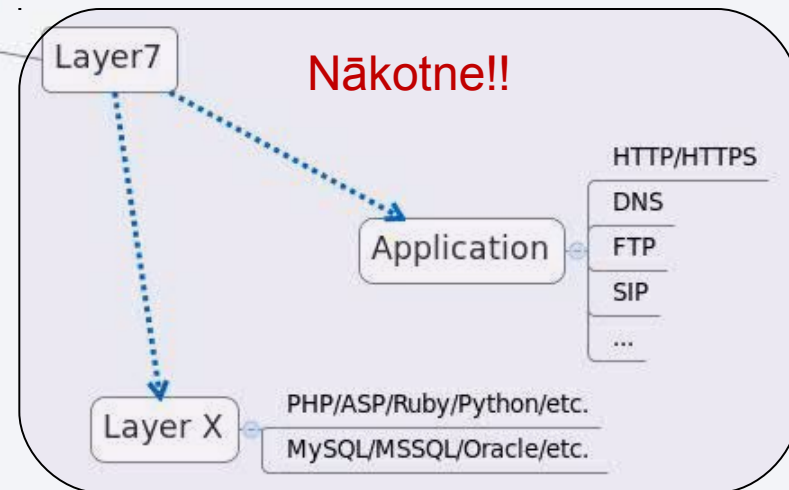


# DOS/DDOS tendencies

## DOS/DDOS (Servisa atteices uzbrukums)


*The OSI Layer Model*

OSI	TCP/IP
<b>Layer 7</b> Application	<b>Application</b> Telnet, FTP, NFS, NIS
<b>Layer 6</b> Presentation	<b>Session</b> e.g. RPC
<b>Layer 5</b> Session	<b>Transport</b> Sockets/Streams - TLI
<b>Layer 4</b> Transport	TCP    UDP
<b>Layer 3</b> Network	<b>Network</b> IP + ARP/RARP/ICMP
<b>Layer 2</b> Data Link	<b>Physical Protocol</b> Ethernet/TR/FDDI/PPP
<b>Layer 1</b> Physical	<b>Transmission medium</b> Coax, Fiber, 10baseT..



# DOS/DDOS tendencies

## 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
- Skaitis 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!**

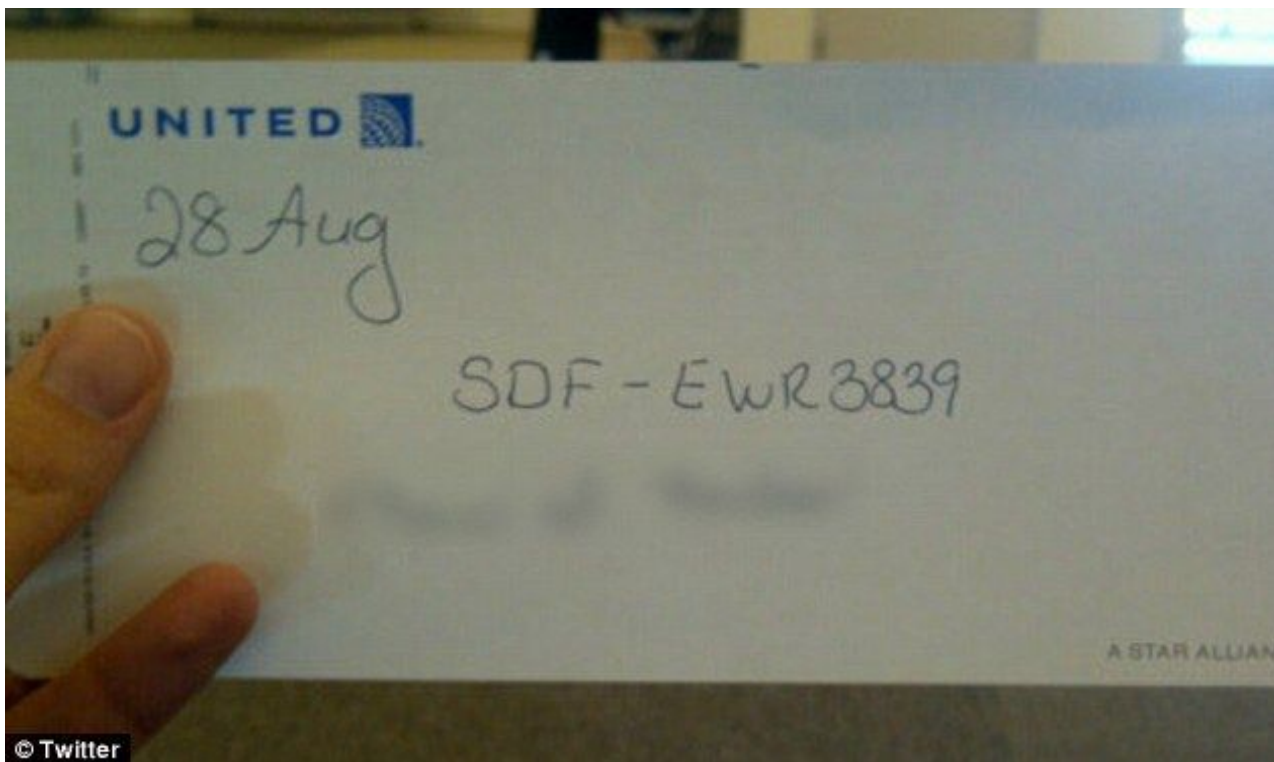
## Datu “mākonis” – neglābj no vecām kļūdām!

- 2009 – Vairāk kā 300 dokumentu par TWITTER biznesa plāniem tika nozagti no Google Apps. Iemesls – vāja parole.
- 2010 – Izveidota programma WiFi parolu 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.



## Ko darīt pēc sekmīga uzbrukuma?

- Izmantojam rezerves darba plānu :)



# Paldies par uzmanību!!!

**Gints Mākalnietis**

E-pasts: [gints.malkalnietis@cert.lv](mailto: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>

