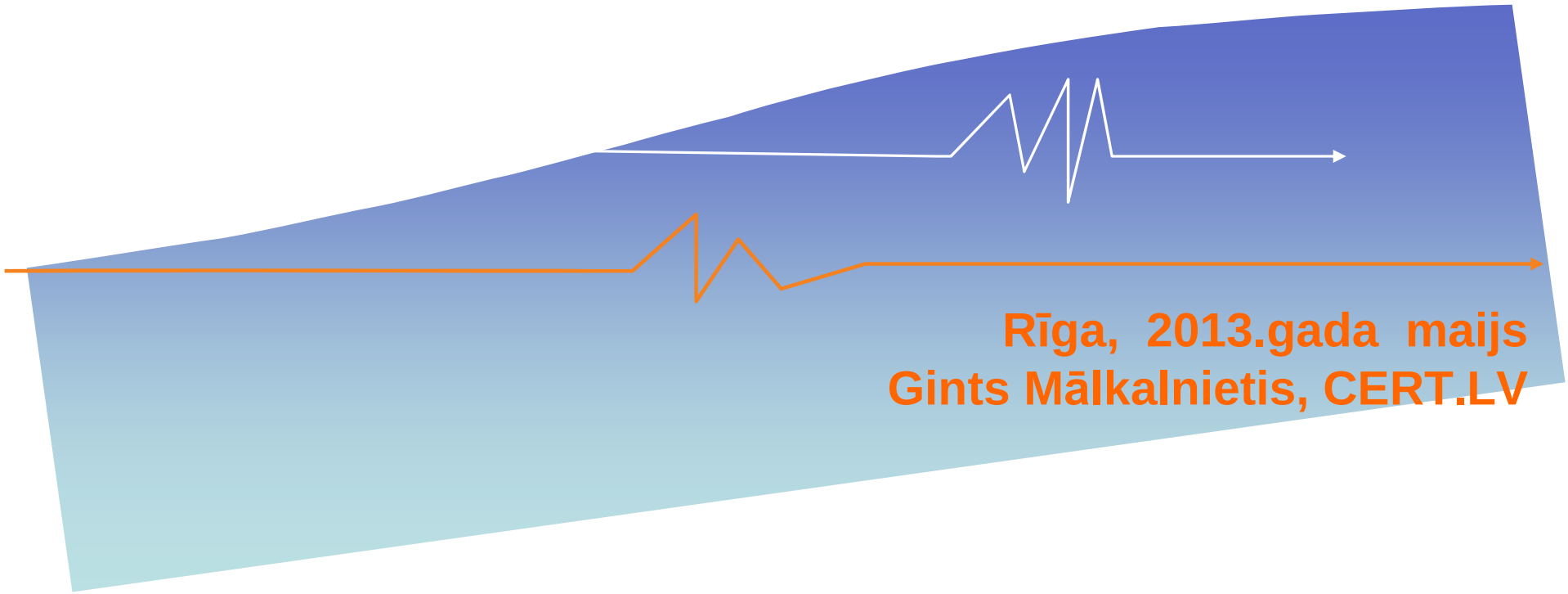
“Datorvīrusu kaitējums”



Rīga, 2013.gada maijs

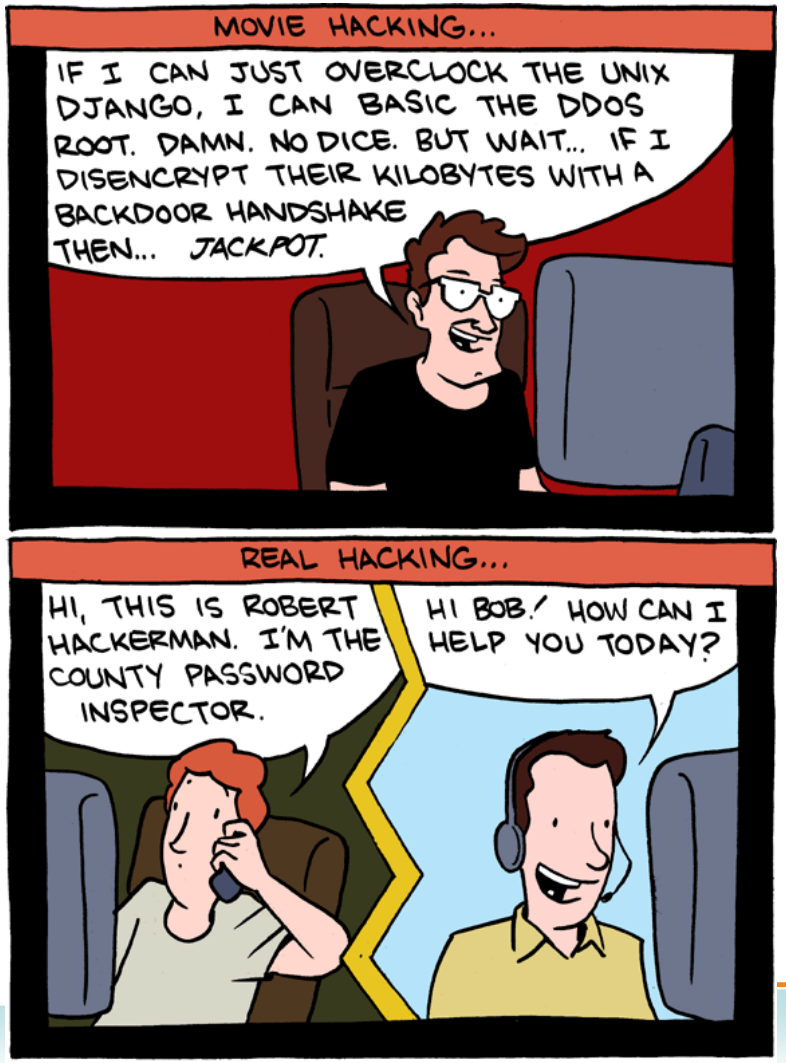
Gints Mālkalnietis, CERT.LV

Saturs

- Kā inficē darbstacijas
- Ko nepamana serveru īpašnieki
- Populārākie datorvīrusi

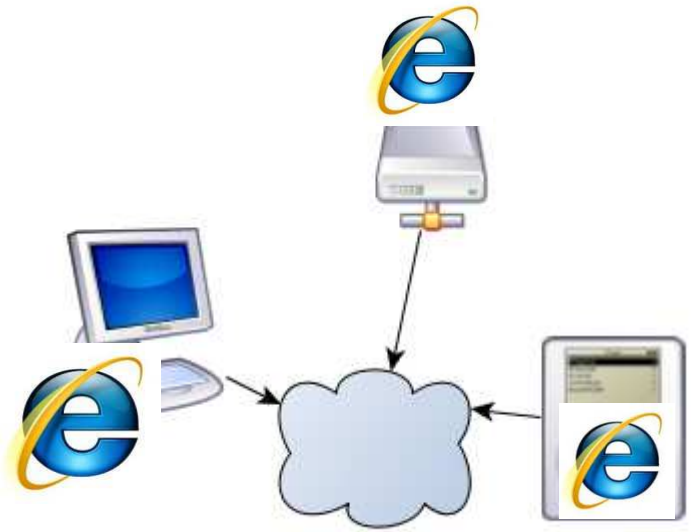
Riski darbstacijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



Interneta pārlūks = dators (OS + app.)

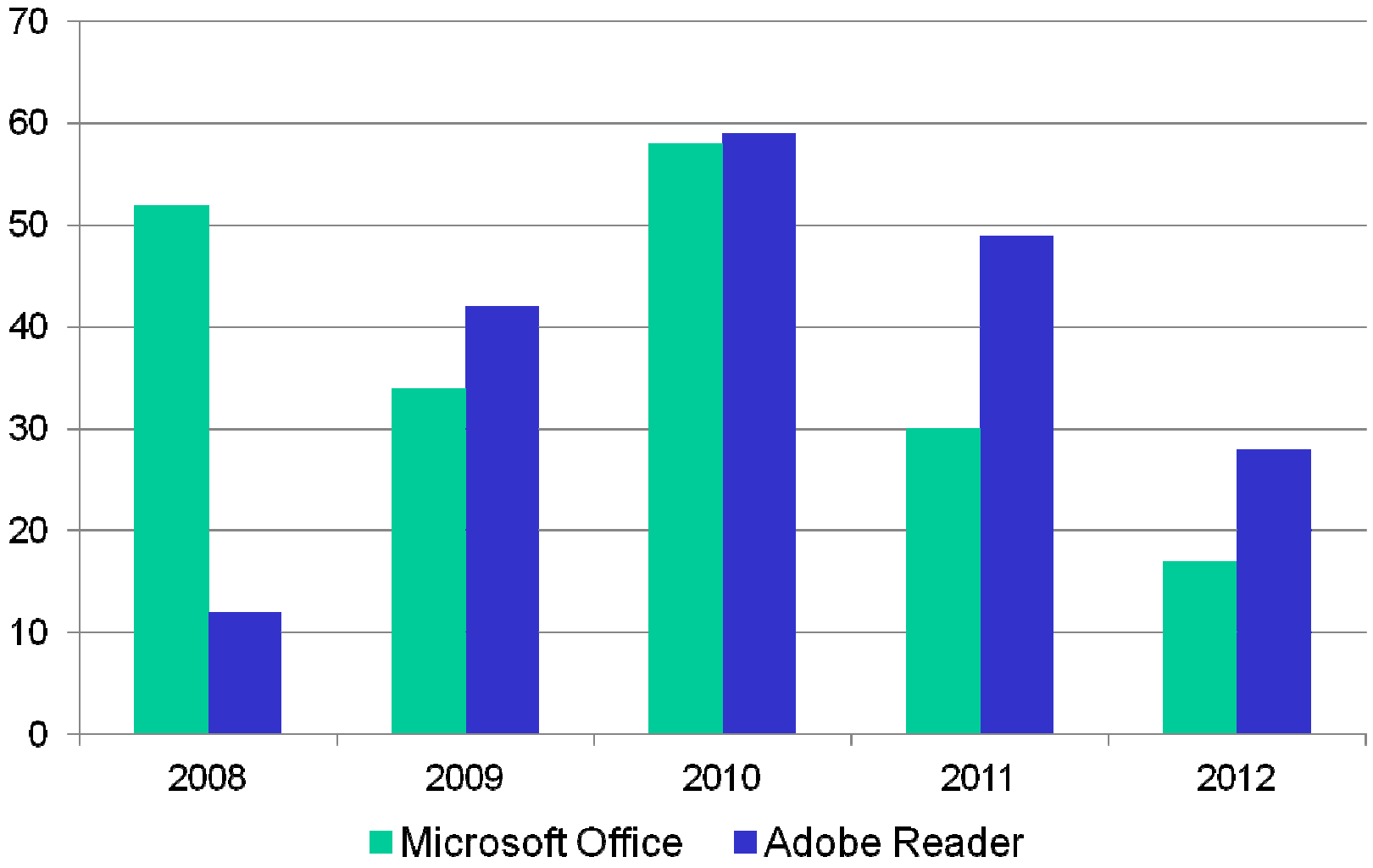
- Interneta pārlūks = pilnvērtīgs dators
- Veiksmīgs uzbrukums pārlūkam – pilnīga kontrole pār lietotāja datiem
- Dažādas ierīces – viena ievainojamība



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

Kritiskas ievainojamības



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!

MOBILĀS ierīces!

```
RewriteCond %{HTTP_ACCEPT} "text/vnd.wap.wml|application/vnd.wap.xhtml+xml"
[NC,OR]
RewriteCond %{HTTP_USER_AGENT}
"acs|alav|alca|amoi|audi|aste|avan|benq|bird|blac|blaz|brew|cell|cldc|cmd-" [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
"dang|doco|eric|hipt|inno|ipaq|java|jigs|kddi|keji|leno|lg-c|lg-d|lg-g|lge-" [NC,OR]
RewriteCond %{HTTP_USER_AGENT} "maui|maxo|midp|mits|mmef|mobi|mot-
|moto|mwbp|nec-|newt|noki|opwv" [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
"palm|pana|pant|pdxg|phil|play|pluc|port|prox|qtek|qwap|sage|sams|sany" [NC,OR]
RewriteCond %{HTTP_USER_AGENT} "sch-|sec-|send|seri|sgh-|shar|sie-
|siem|smal|smar|sony|sph-|symb|t-mo" [NC,OR]
RewriteCond %{HTTP_USER_AGENT} "teli|tim-|tosh|tsm-|upg1|upsi|vk-
v|voda|w3cs|wap-|wapa|wapi" [NC,OR]
RewriteCond %{HTTP_USER_AGENT} "wapp|wapr|webc|winw|winw|xda|xda-"
[NC,OR]
RewriteCond %{HTTP_USER_AGENT}
"up.browser|up.link|windowssce|iemobile|mini|mmp" [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
"symbian|midp|wap|phone|pocket|mobile|pda|psp|PPC|Android
```

Kā vīrusi inficē datorus - 1
Drive-by download

Legālās, populārās vietnēs tiek ievietotas saites uz lapām kas uztur exploit-kit – automatizētu rīku pārlūkprogrammas ievainojamību meklēšanai un izmantošanai.

Kasjauns.lv, BBC Radio 3, GoDaddy

Kā vīrusi inficē datorus - 1
Drive-by download

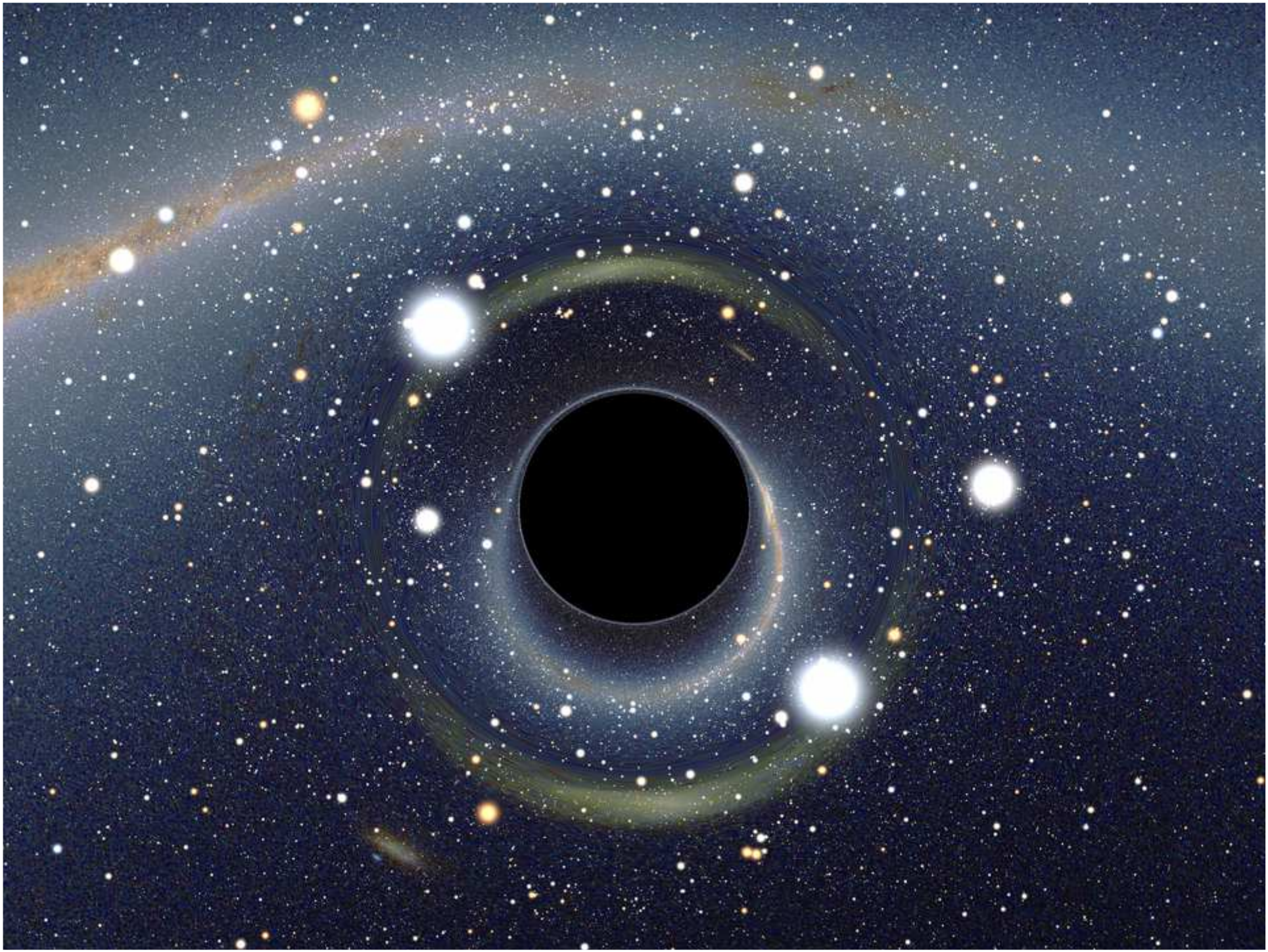
1. Kaitīgais kods tiek izsaukts, izmantojot slēptu iframe
2. Tiek izmantots kaitīgs javascript, kas novirza apmeklētāju pie noteiktām darbībām uz uzbrucēja serveri
3. Tiek pārrakstīts .htaccess fails un, “vēlamie apmeklētāji”, tiek novirzīti uz uzbrucēja serveri

LAPAS APMEKLĒTĀJS PATS UZ SAITĒM NEKLIKŠĶINA!!

Kā vīrusi inficē datorus - 1
Drive-by download

4. Saites uz uzbrucēja serveri tiek atsūtītas e-pastā
5. Dažādu portālu komentāros tiek ievietoti aicinājumi apmeklēt kādu vietni
6. Saites tiek pievienotas Youtube utt. video materiāliem
7. Saites uz kaitīgu lapu tiek ievietotas dokumentos, kas tiek atsūtīti upurim

UPURIS PATS IZVĒLAS APMEKLĒT KAITĪGO LAPU!!



Kā vīrusi inficē datorus - 1
Drive-by download

Blackhole Exploit kit – šobrīd populārākais datorvīrusu izplatīšanas serviss!!!

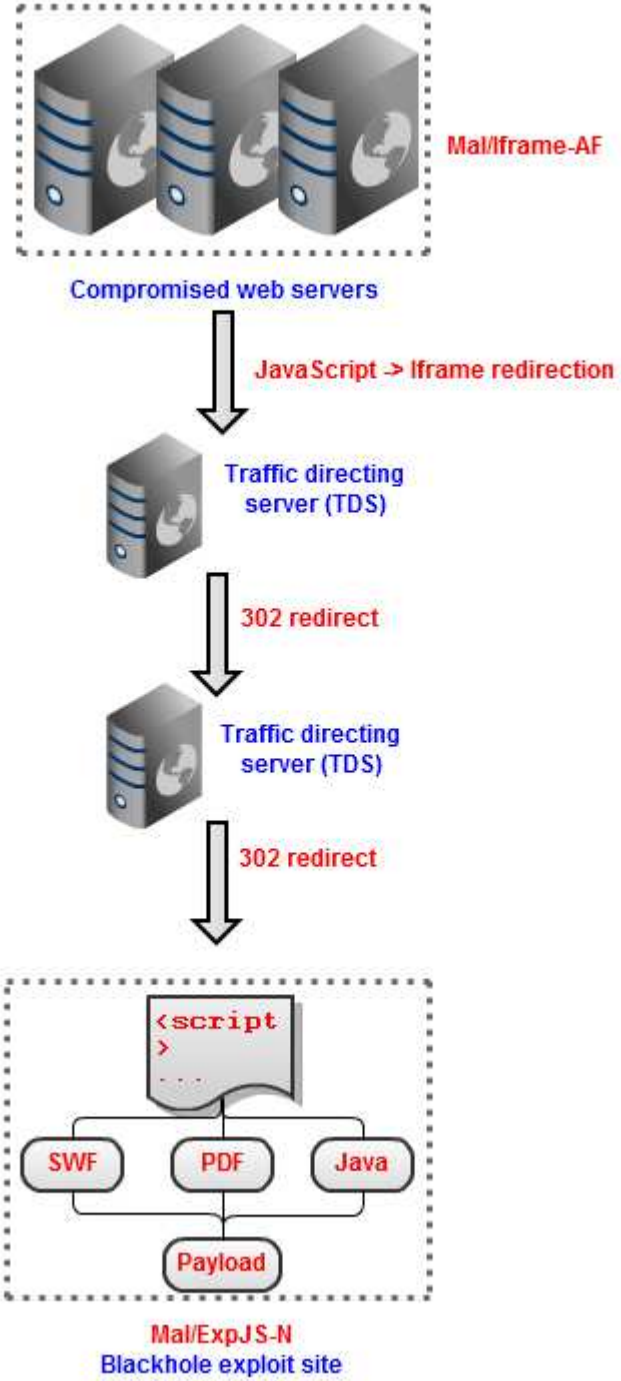
Populārākās izmantotās ievainojamības:

1. Adobe Flash - field.swf (CVE-2011-0611), flash.swf (CVE-2011-2110)

2. JAVA CVE-2012-5076 (Sept 2012), CVE-2012-1723

3. Adobe PDF PDF LibTiff CVE-2011-2462

4. Microsoft Windows MDAC MS07-009


Mal/Iframe-AF
Compromised web servers
JavaScript -> Iframe redirection
Traffic directing server (TDS)
302 redirect
Traffic directing server (TDS)
302 redirect
<script >
...
SWF
PDF
Java
Payload
Mal/ExpJS-N
Blackhole exploit site

LATVIJAS POLICIJAS
KIBERNOZIEGUMI DEPARTAMENTS

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

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

1. 
2. 
3. 
4. 

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 svarīgi 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

Kā vīrusi inficē datorus - 2
Inficēti faili

1. **E-pasts –** populārākais veids kā iesūtīt datorvīrusu. Mūsdienās reti notiek mēģinājumi iesūtīt izpildāmu programmas failu, biežāk tiek izmantoti zināmi PDF vai MS Office failu exploiti.
2. **USB datu nesēji –** inficē draugu un darba datorus, publiski pieejamas iekārtas.
3. **Viltus atjauninājumi** - datorvīrusi tiek uzdoti par pārlūkprogrammu, to papildinājumu, antivīrusu atjauninājumiem.
4. **Viltus video kodeki –** tiek izplatīti kopā ar filmām.

Kā vīrusi inficē datorus – 3
Inficēti faili – arī mobilajos telefonos

Antivīrusu programmas – ne tik drošas kā solīts!

- Efektivitāte pret jauniem vīrusiem < 10-20%
- Nav laicīgi atjaunotas
- Ķer tikai “zināmus” vīrusus
- Palēnina datora darbību – lietotāji tās atslēdz

Ko “noguļ” serveru administratori

1. Serveru administrēšanas rīkiem nav ierobežota piekļuve
2. Nav ieviesti rīki nesekmīgo piekļuves mēģinājumu uzskaitei, netiek veidoti pietiekami žurnālfaili
3. Vājas paroles
4. Novēlota programmatūras “ielāpu” uzstādīšana

Ko “noguļ” serveru administratori

1. Serverī tiek uzturētas “cauras” tīmekļa lapas
2. Novecojušas satura vadības sistēmas un to pielikumi
3. Nepareizas failu piekļuves, izpildes tiesības – viens uzlauzts lietotāja konts sabojā visas serverī esošās lapas
4. Datubāzēs tiek glabātas neaizsargātas, vai nepareizi «sajauktas» paroles

Izplatītākie datorvīrusi

1. **Conficker -** izplatītākais datorvīruss, sastopams 8x biežāk kā otrs populārākais. Konstatēts vairāk kā 30000 IP adresēs 2013 gadā.
   Pirmoreiz konstatēts 2008 gada 21 novembrī.
   C&C infrastruktūra sagrauta un pārņemta pateicoties Microsoft vadītās Conficker Working Group aktivitātēm.

   Šis vīruss turpina automātiski izplatīties, bet neesošās C&C infrastruktūras dēļ, nekādas papildus kaitīgas darbības neveic!

   Izplatās izmantojot ievainojamību RPC protokolā, ar pārnēsājamiem datu nesējiem, kā arī piemeklējot nedrošas paroles tīkla koplietošanas mapēm.

Izplatītākie datorvīrusi

2. **VIRUT -** botnets darbojas, vismaz, kopš 2006 gada. 2013 gada sākumā tā darbība traucēta, patiecoties Polijas CERT NASK, kas pārņēmis tā C&C domēnus.

   Inficētie datori veic DDOS uzbrukumus, izsūta mēstules, pārtver lietotāja paroles un piekļuves datus, var tikt izmantoti citu kaitīgo programmu instalācijai upura datorā.

   Tiek izplatīts izmantojot pārnēsājamus datu nesējus un inficētas tīmekļa vietnes.

Izplatītākie datorvīrusi

3. **Slenfbot –** Pirmoreiz konstatēts 2007 gadā.
   Zināms arī kā «Skype» vīruss. Izplatās caur dažādām IM programmām (ICQ, Skype, Gtalk, AIM, Facebook). Tiek izplatīts kā fails, kas tiek lejupielādēts apmeklējot IM pārsūtīto saiti.
   Automātiski pārsūta savas kopijas visiem upura IM programmas kontaktiem, kā arī inficē pārnēsājamos datu nesējus.
   Komandas no botneta uzturētājiem saņem caur IRC, tiek izmantots lai izplatītos pats, vai lai lejupielādētu un izpildītu kādu citu kaitīgu programmu (šobrīd tiek aktīvi lietots «Policijas vīrusa» izplatīšanai).

Izplatītākie datorvīrusi

4. **Pushdo –** Pirmoreiz konstatēts 2007 gadā.
   Tiek izmantots citu kaitīgu programmu lejupielādei (Zeus, SpyeEye), kā arī masveida mēstuļu izsūtīšanai. Iebūvēta keyloger funkcionalitāte.
   Tiek izplatīts caur inficētām tīmekļa vietnēm, kā pielikums e-pastam utt.
   Atbildīgs par lielu daļu no kopējā mēstuļu daudzuma.
   Kopš 2013 gada izmanto DGA (domain generation algorithm) kontroles noturēšanai.

Izplatītākie datorvīrusi

5. **ZEUS –** Pirmoreiz konstatēts 2007 gadā.
   Pamatmērķis –naudas zādzība, izmainot tiešsaites maksājumu formu modificēšanu, ka arī banku piekļuves paroļu zādzību. Spēj pārtvert arī citu resursu paroles un formu datus.
   Tiek izplatīts caur Drive-by Download, kā arī pielikums dažādām phishing mēstulēm.
   Izejas kods tiek izīrēts «personificētu» vīrusa variantu izveidei.

Izplatītākie datorvīrusi

6. **SALITY –** Pirmoreiz konstatēts 2003 gadā.
   Plaša polimorfisku vīrusu saime, tiek izmantota dažādu uzdevumu veikšanai – mēstuļu izsūtīšanai (māk pārmeklēt upura failu saturu, meklējot e-pasta adreses), citu programmu izplatīšanai, informācijas zādzībai, HTTP starpniekservera uzturēšanai, datoru resursu izmantošana paroļu uzlaušanai utt. Izplatās kā e-pasta pielikums, tīkla mapēs un pārnēsājamos datu nesējos, izmanto arī .LNK ievainojamību.

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