“Datorvīrusu izplatīšanas ķēdes”

Rīga, 2012.gada 4.decembris

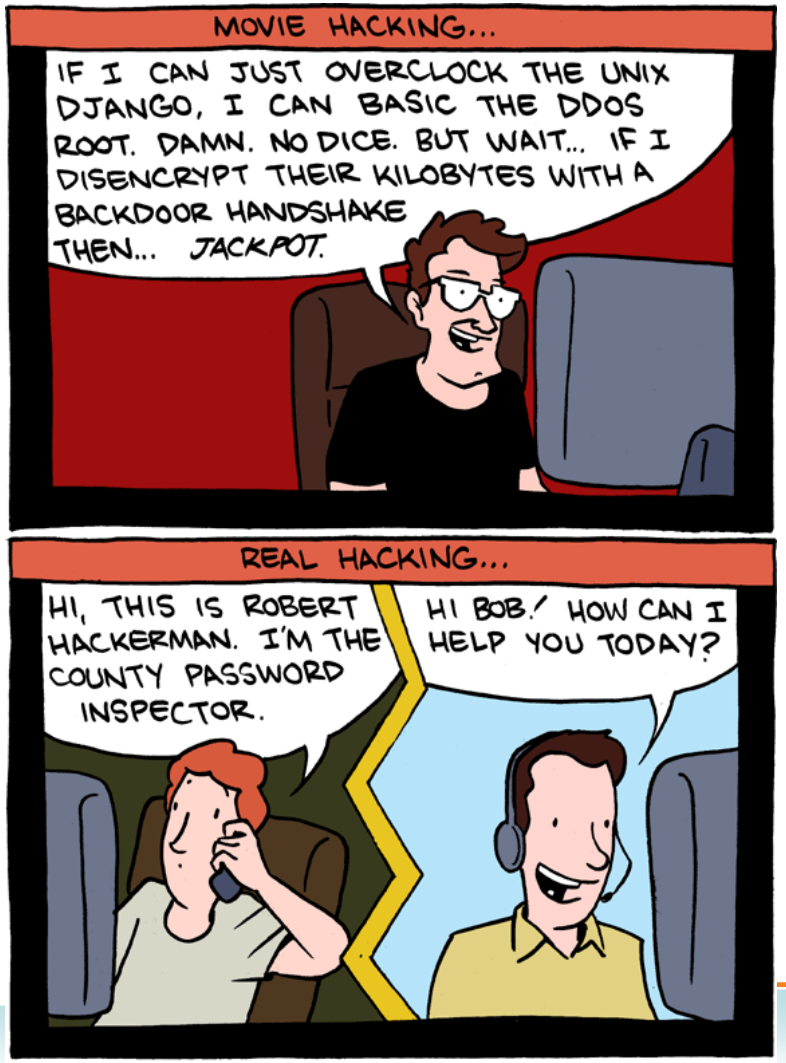
Gints Mālkalnietis, CERT.LV

Saturs

- Kā inficē darbstacijas
- Ko “noguļ” serveru administratori
- Vērtīgā informācija datoros

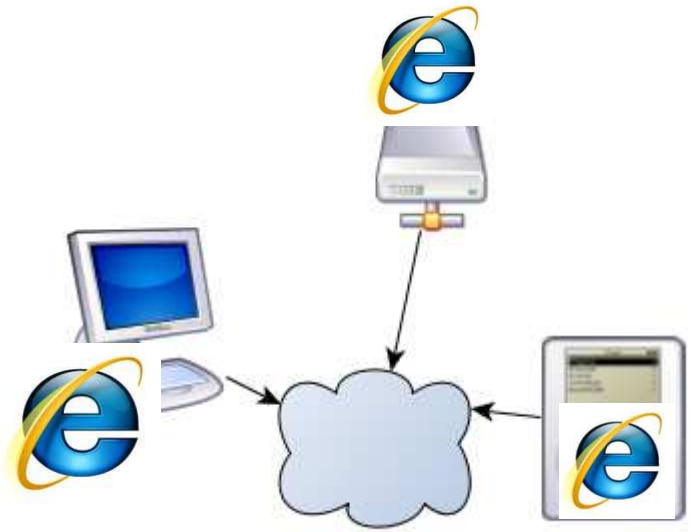
Riski darbstacijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



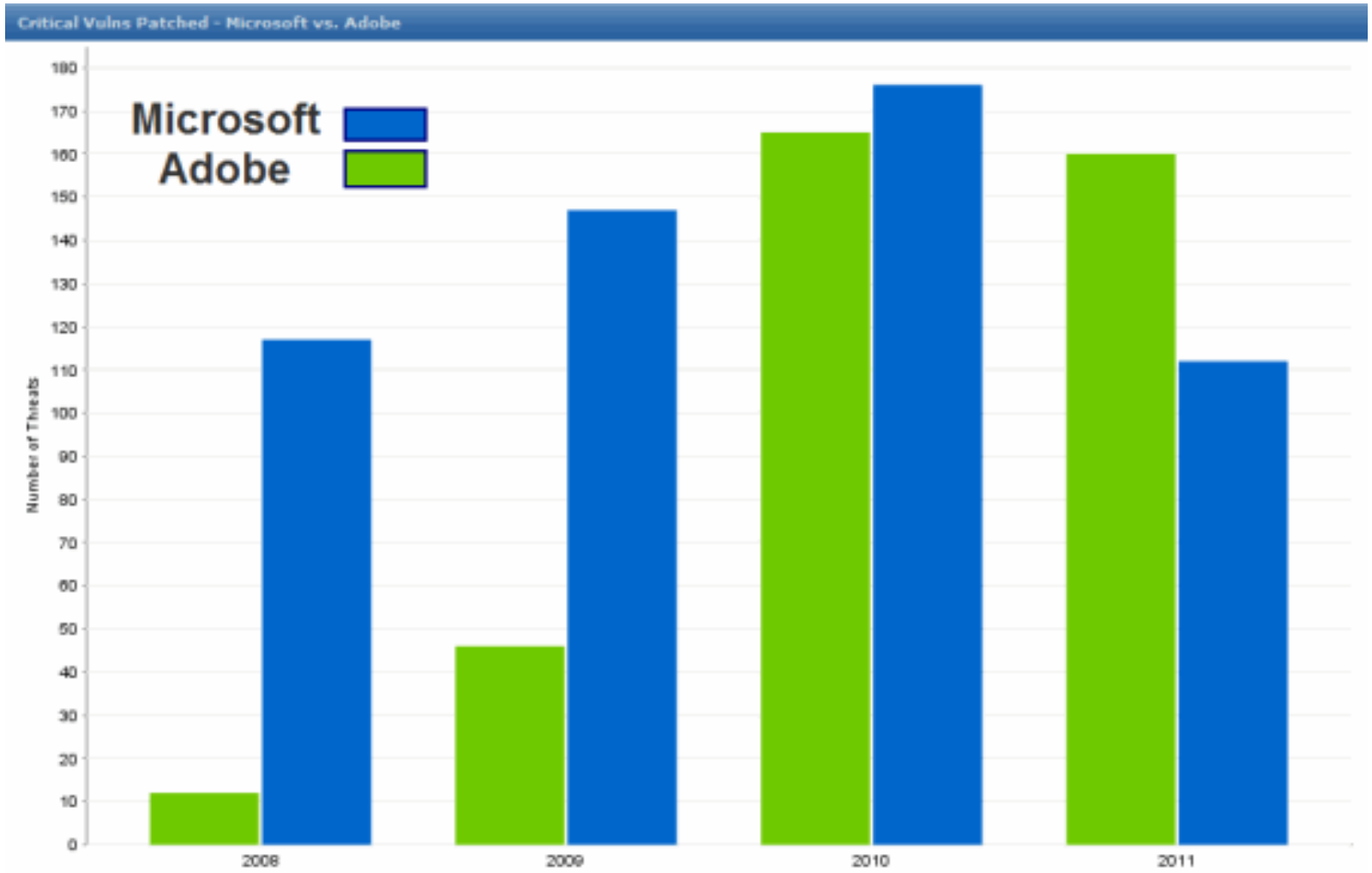
Interneta pārlūks = dators (OS + app.)

- 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


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!

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

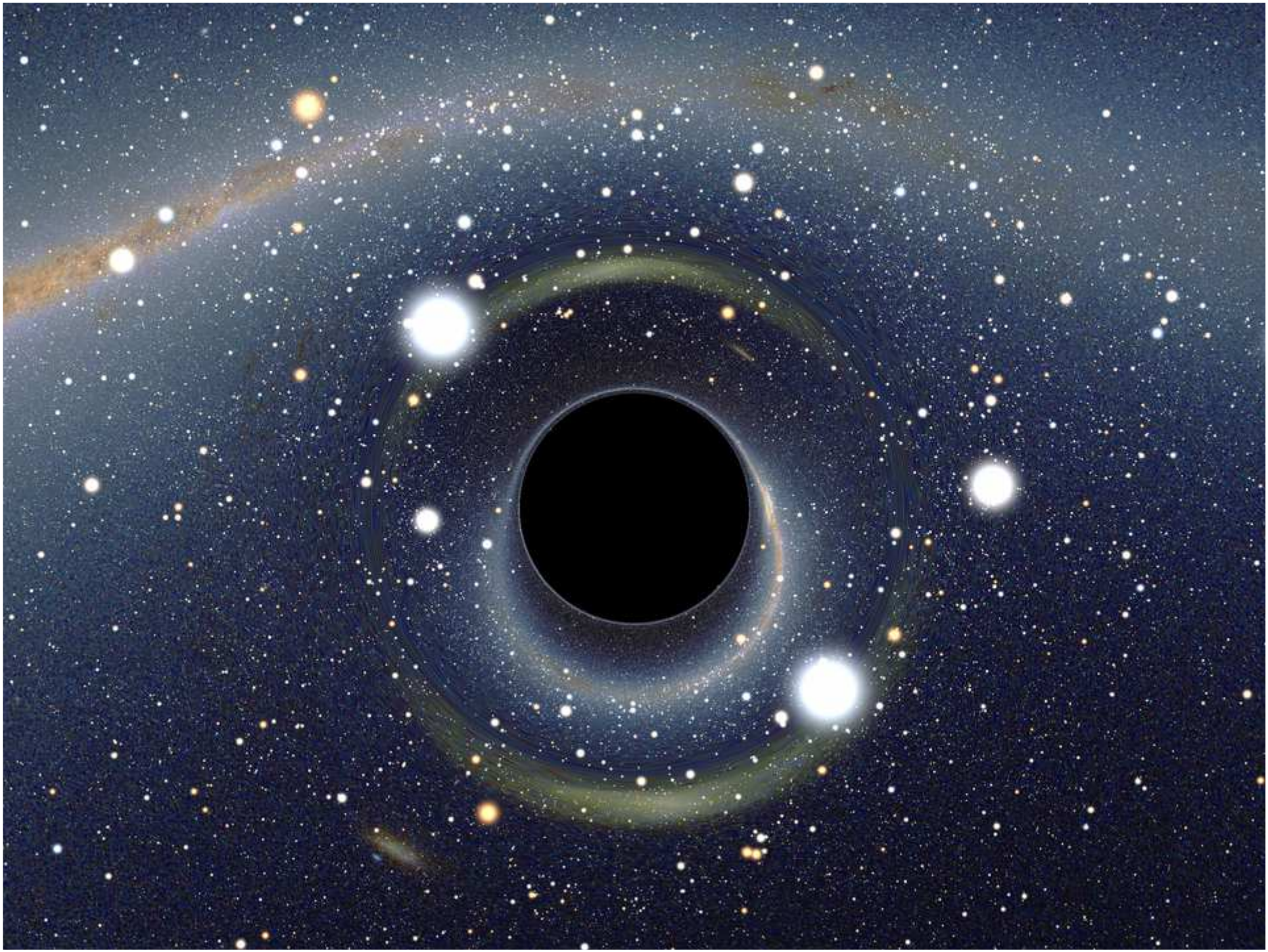
1. Kaitīgais kods tiek izsaukts, izmantojot slēptu iframe
2. Tiek izmantots kaitīgs javascript, kas novirza apmeklētāju pie noteiktām darbībām uz uzbrucēja serveri
3. Tiek pārrakstīts .htaccess fails un, “vēlamie apmeklētāji”, tiek novirzīti uz uzbrucēja serveri

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!!!

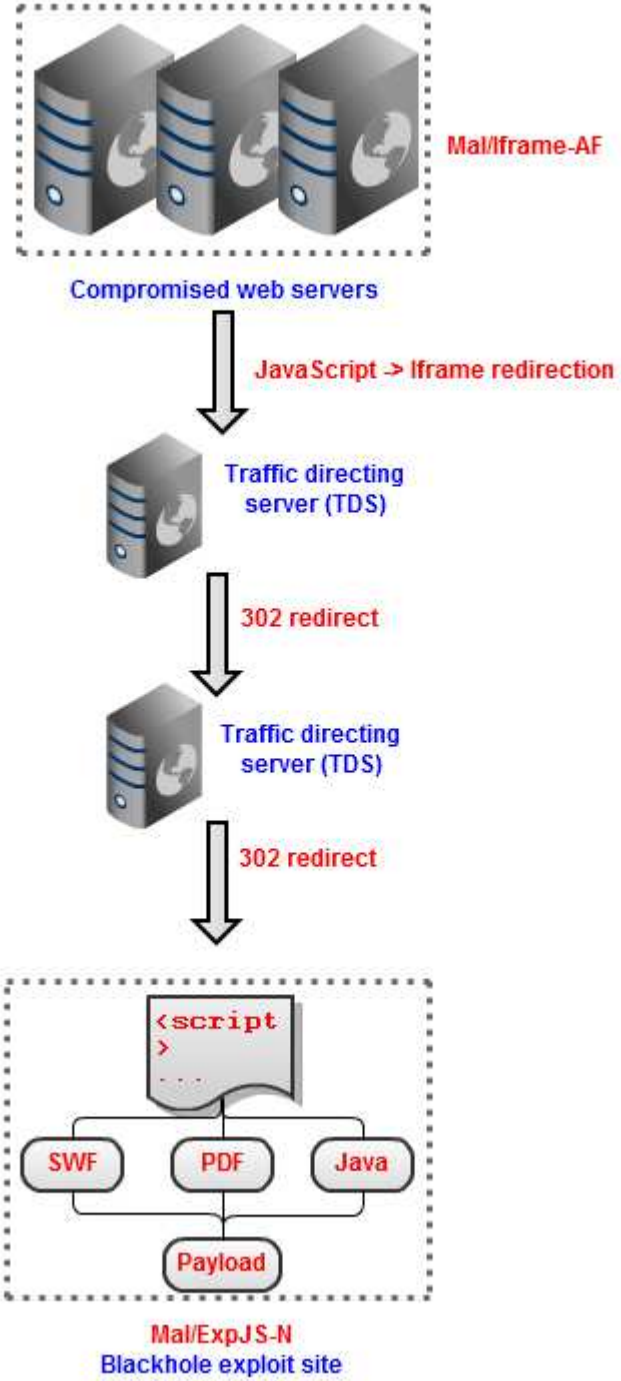
Populārākās izmantotās ievainojamības:

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. **Viltus atjauninājumi** - datorvīrusi tiek uzdoti par pārlūkprogrammu, to papildinājumu, antivīrusu atjauninājumiem.
3. **Video kodeki –** tiek izplatīti kopā ar filmām.
4. **Alternatīvs** mehānisms, ja pārlūkprogramma nav ievainojama ar Drive-By.

Kā vīrusi inficē datorus - 2
Inficēti faili – arī mobilajos

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

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: b0c4b0379402045512a9b

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

Jauna dienā kantorī,
Brīnas visi darboņi,
Kam tu, tupais direktor,
Darbā jēmi pajoli?

Admins nulle, lohs "pa dzīvi"
Saņem algu, lamers, brīvi,
Pa to laiku "hakeri"
Piesmēj arī routeri...

P.S. Algot kārtīgu adminu vienmēr ir lētāk nekā pārmaksāt par pulveri. Esošo pajolu vienmēr var atlaist bez kompensācijām, parādot šo izdruku.

Ko “noguļ” serveru administratori

• 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!

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 hashotas paroles

Jaunums – rootkit kaitīgu iframe injekcijai HTTP lapās

```
; =============== S U B R O U T I N E =======================================


                public set_http_injection
set_http_injection proc near                    ; CODE XREF: mod_init+31↓p
                sub     rsp, 8
                call    get_http_injection_var
                test    eax, eax
                jz      short loc_A4B4
                xor     eax, eax
                call    load_zlib_module
                test    eax, eax
                jz      short loc_A4B4
                mov     rdi, cs:this_tcp_sendmsg
                mov     rsi, offset new_tcp_sendmsg
                call    splice_func_in_memory
                test    eax, eax
                setnz   al
                movzx   eax, al
                jmp     short loc_A4B6
; ---------------------------------------------------------------------------

loc_A4B4:                                       ; CODE XREF: set_http_injection+B↑j
                                                ; set_http_injection+16↑j
                xor     eax, eax

loc_A4B6:                                       ; CODE XREF: set_http_injection+33↑j
                pop     rdi
                retn
set_http_injection endp
```

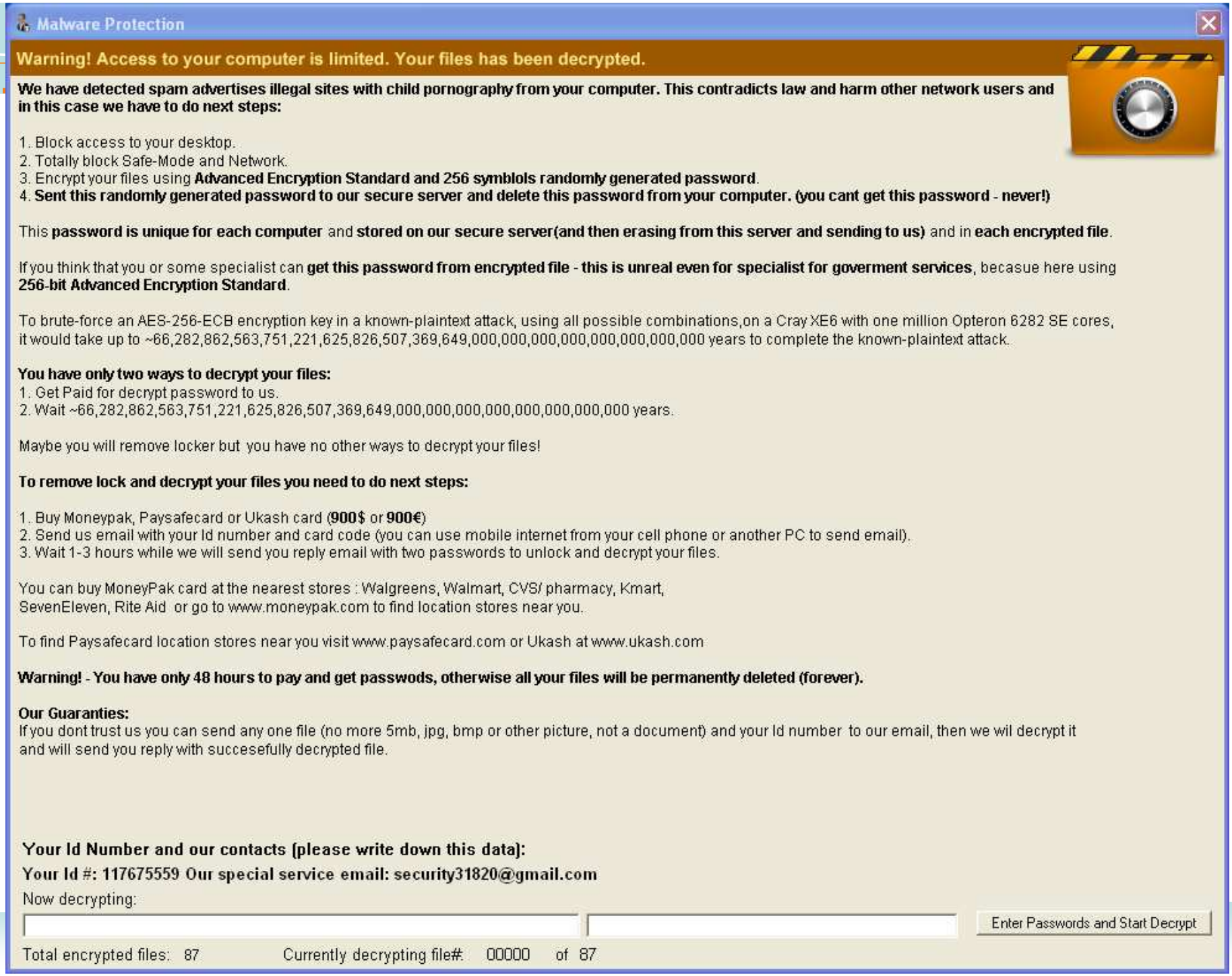
Jaunums – rootkit kaitīgu iframe injekcijai HTTP lapās

1. Paredzēts 64-bit Linux datoriem
2. Var veikt precīzu injekciju tikai konkrētai mērķauditorijai
3. Attālināti vadāms

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, paroļu uzlaušana, DDOS, mēstuļu izsūtīšana

Vērtības jūsu serverī??


Malware Protection
Warning! Access to your computer is limited. Your files has been decrypted.
We have detected spam advertises illegal sites with child pornography from your computer. This contradicts law and harm other network users and in this case we have to do next steps:
1. Block access to your desktop.
2. Totally block Safe-Mode and Network.
3. Encrypt your files using Advanced Encryption Standard and 256 symblols randomly generated password.
4. Sent this randomly generated password to our secure server and delete this password from your computer. (you cant get this password - never!)
This password is unique for each computer and stored on our secure server(and then erasing from this server and sending to us) and in each encrypted file.
If you think that you or some specialist can get this password from encrypted file - this is unreal even for specialist for goverment services, becasue here using 256-bit Advanced Encryption Standard.
To brute-force an AES-256-ECB encryption key in a known-plaintext attack, using all possible combinations,on a Cray XE6 with one million Opteron 6282 SE cores, it would take up to ~66,282,862,563,751,221,625,826,507,369,649,000,000,000,000,000,000,000,000,000 years to complete the known-plaintext attack.
You have only two ways to decrypt your files:
1. Get Paid for decrypt password to us.
2. Wait ~66,282,862,563,751,221,625,826,507,369,649,000,000,000,000,000,000,000,000,000 years.
Maybe you will remove locker but you have no other ways to decrypt your files!
To remove lock and decrypt your files you need to do next steps:
1. Buy Moneypak, Paysafecard or Ukash card (900$ or 900€)
2. Send us email with your Id number and card code (you can use mobile internet from your cell phone or another PC to send email).
3. Wait 1-3 hours while we will send you reply email with two passwords to unlock and decrypt your files.
You can buy MoneyPak card at the nearest stores : Walgreens, Walmart, CVS/ pharmacy, Kmart, SevenEleven, Rite Aid or go to www.moneypak.com to find location stores near you.
To find Paysafecard location stores near you visit www.paysafecard.com or Ukash at www.ukash.com
Warning! - You have only 48 hours to pay and get passwods, otherwise all your files will be permanently deleted (forever).
Our Guaranties:
If you dont trust us you can send any one file (no more 5mb, jpg, bmp or other picture, not a document) and your Id number to our email, then we wil decrypt it and will send you reply with succesefully decrypted file.
Your Id Number and our contacts (please write down this data):
Your Id #: 117675559 Our special service email: security31820@gmail.com
Now decrypting:
Enter Passwords and Start Decrypt
Total encrypted files: 87
Currently decrypting file#: 00000 of 87

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