Semināra programma

13:30-14:00 “Situācija Latvijā IT drošības jomā un CERT.LV attīstības perspektīvas” – Baiba Kaškina, CERT.LV vadītāja

14:00-14:30 „Tīmekļa vietņu drošība” - Ēriks Dobelis, ISACA Latvijas nodaļas biedrs

14:30-15:00 „Bezvadu tīklu drošība” – Varis Teivāns, CERT.LV vadītāja vietnieks

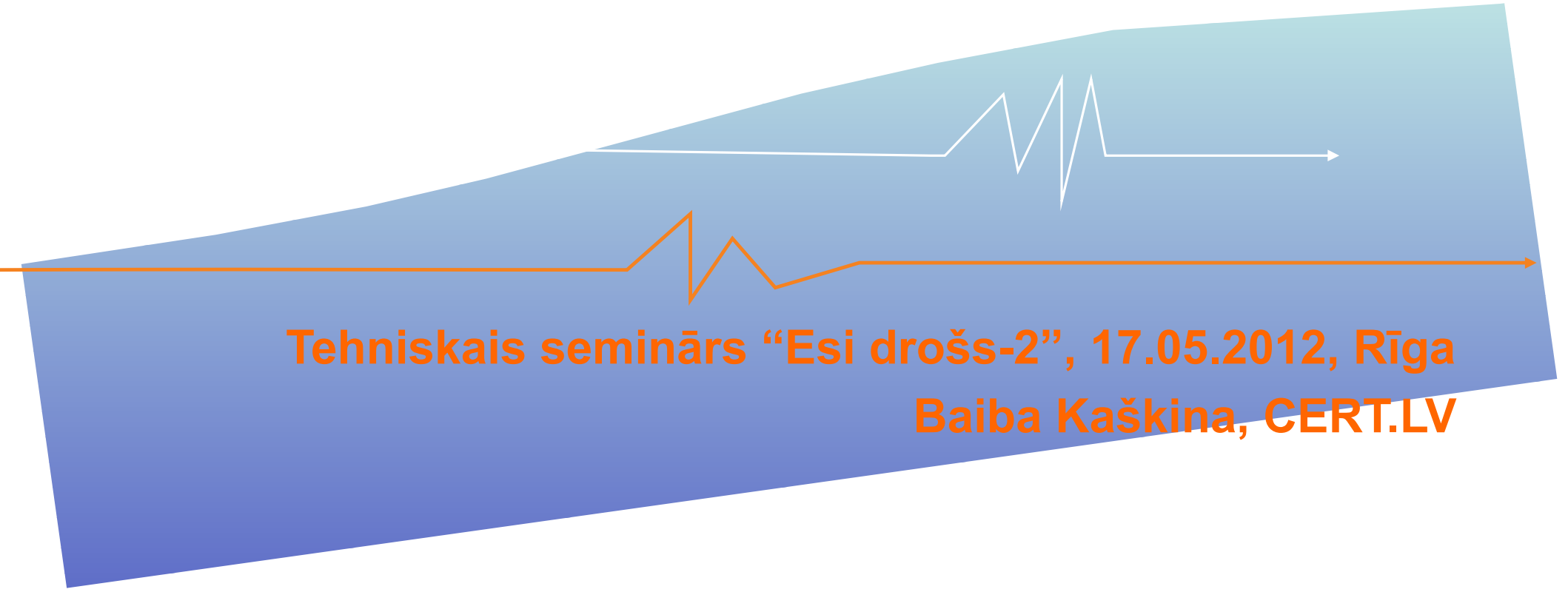
15:00-15:30 pārtraukums

15:30 – 16:00 „Praktisks piemērs – risku novērtēšana un mazināšanas pasākumi” – Sintija Deruma, ISACA Latvijas nodaļas biedrs

16:00 – 16:30 „Rīcība ārkārtas situācijā” – Kristaps Miļevskis, LR CSP, Informācijas sistēmas drošības pārvaldnieks

16:30 – 17:00 „7 būtiski jautājumi par IT drošību” – CERT.LV un LV CSIRT grupas speciālistu sagatavotas atbildes

Situācija Latvijā IT drošības jomā un CERT.LV attīstības perspektīvas

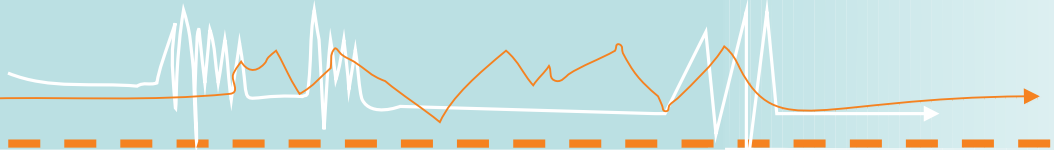


Tehniskais seminārs “Esi drošs-2”, 17.05.2012, Rīga

Baiba Kaškina, CERT.LV

Saturs

- Par CERT.LV
- Aktuālā situācija Latvijā
- Padomi un palīdzība
- Nākotne un attīstības perspektīvas



CERT.LV

Par CERT.LV

CERT.LV

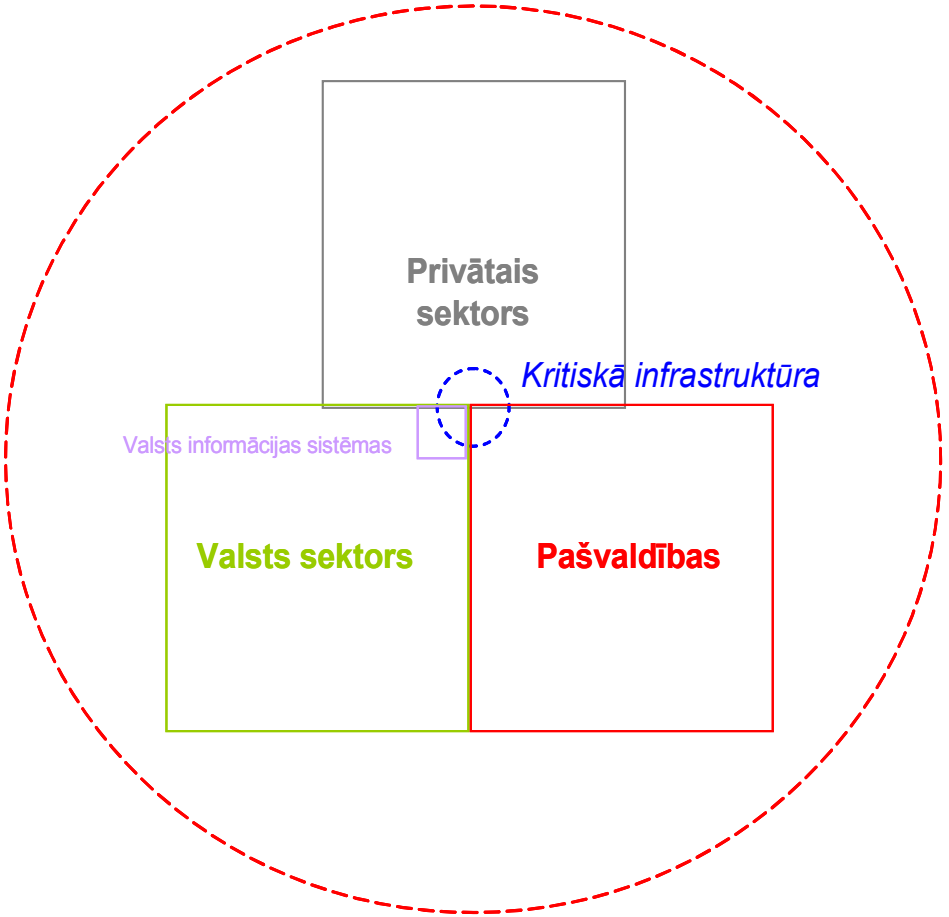
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Misija: “Veicināt IT drošību Latvijā”

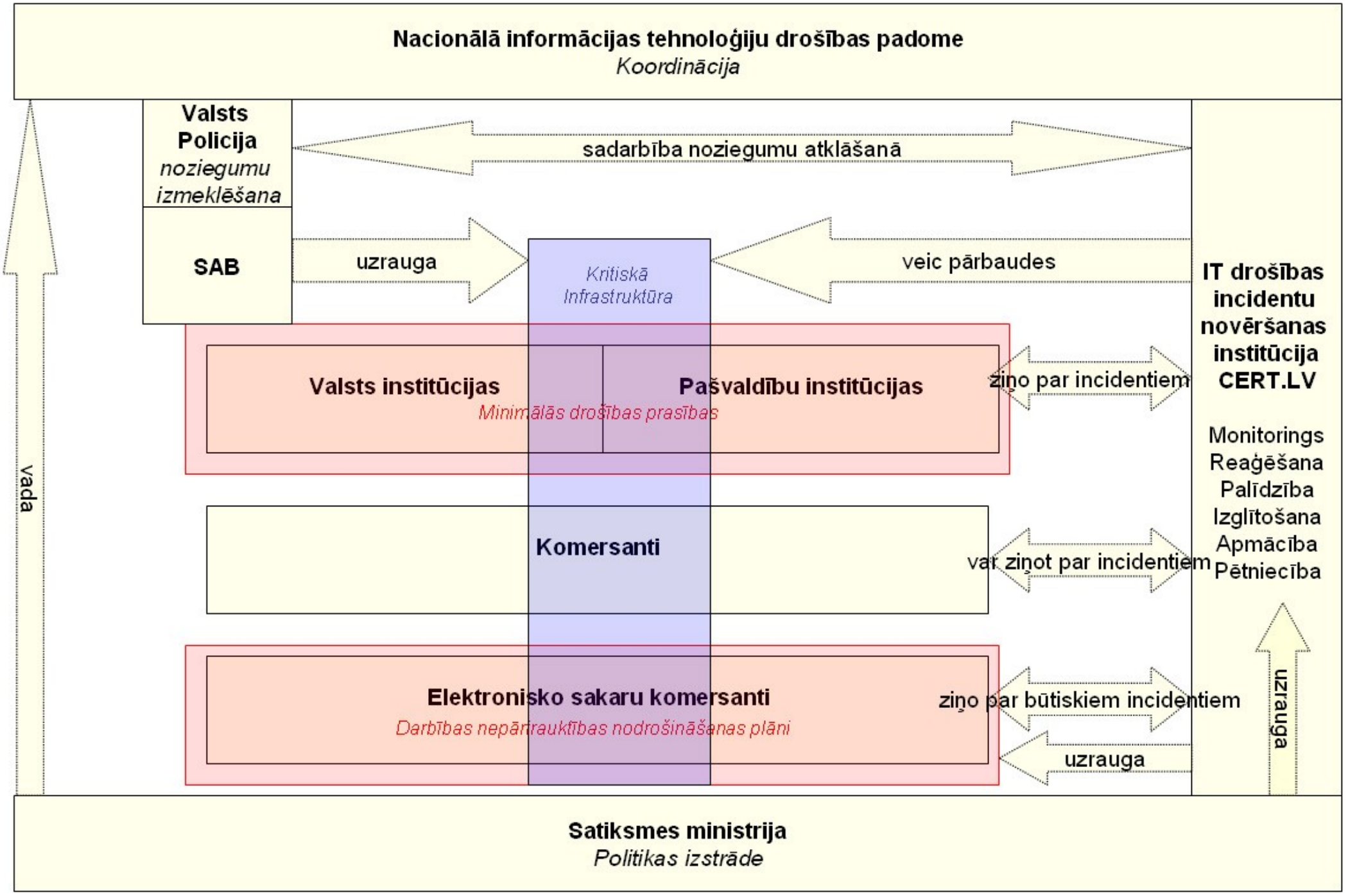
CERT.LV

- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu” kopš 2011.gada 1.februāra
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”
- Finansēta no valsts budžeta
- Visi pakalpojumi ir bezmaksas

CERT.LV kopiena

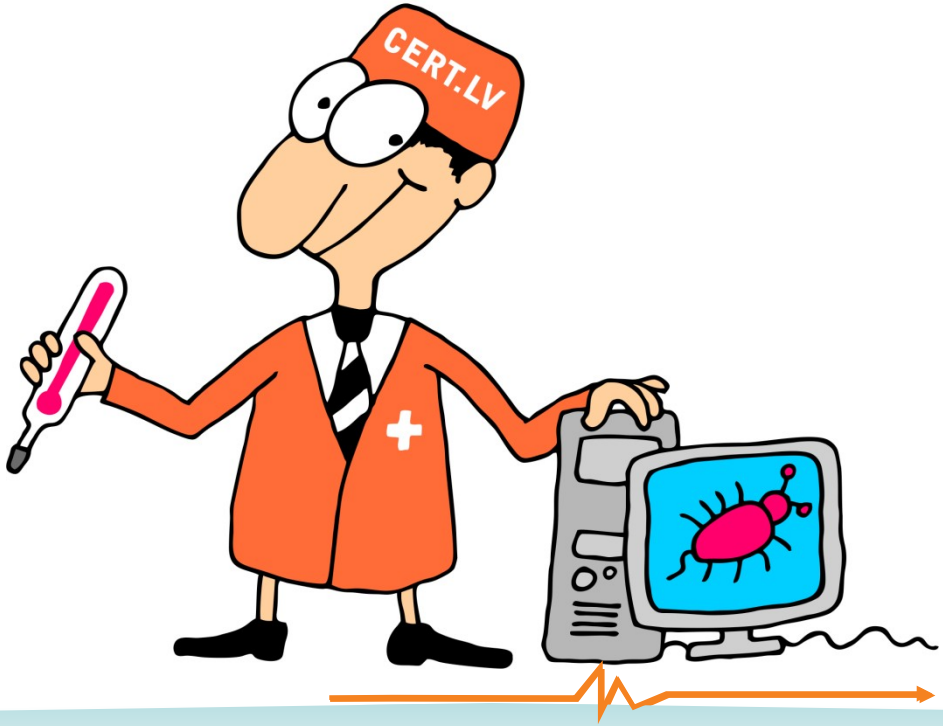


Latvijas IT drošības sistēmas ataino jums – būtiskākie elementi



Kas ir CERT.LV?

- “Ģimenes ārsts” un “ugunsdzēsējs” e-vidē



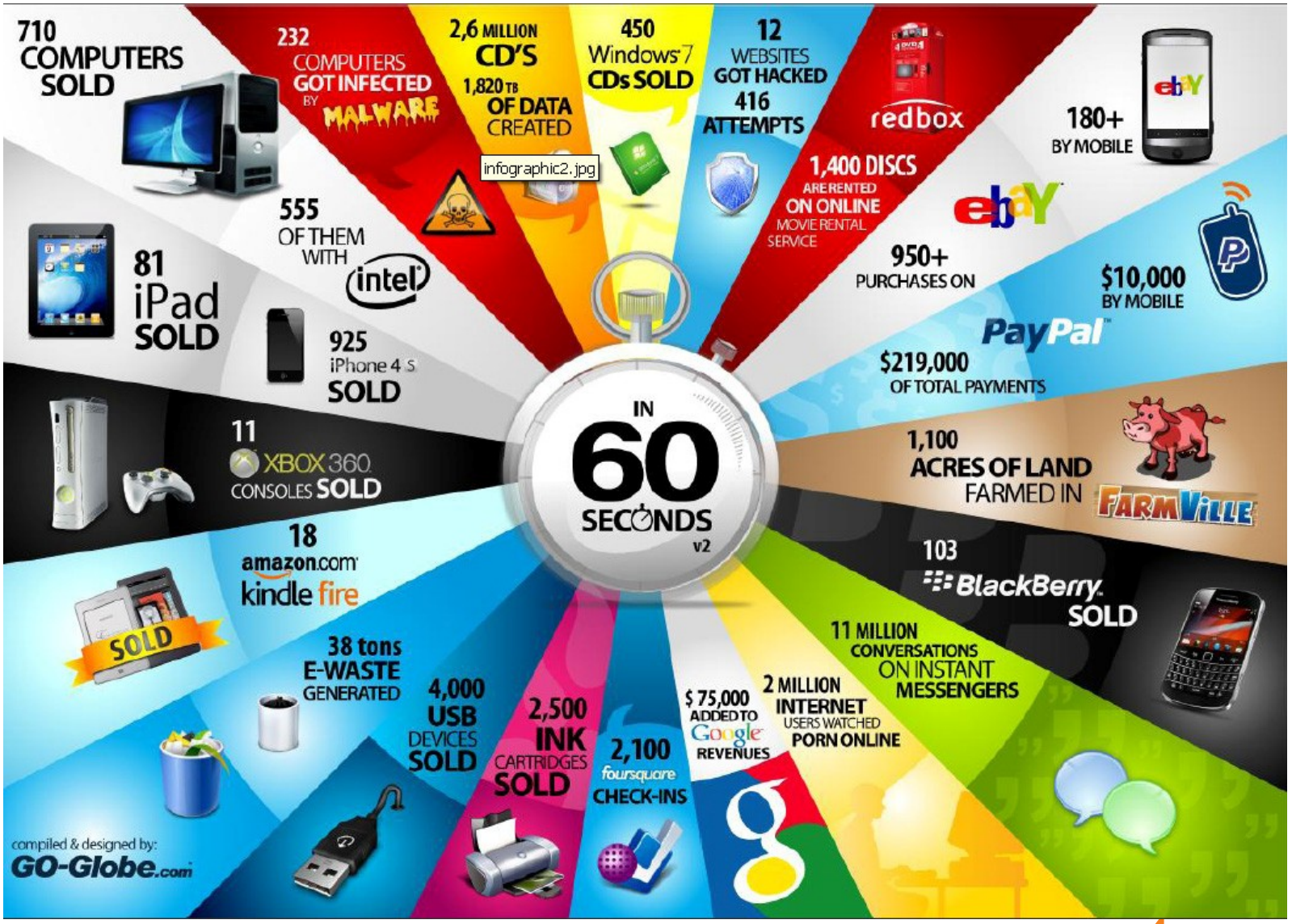
Aktuālā situācija Latvijā

Saprašanās memorands ar NATO – 2012.gada janvāris

Mūsdienu pasaule 60 sekundēs (1)

http://www.businessinsider.com/

Mūsdienu pasaule 60 sekundēs (2)

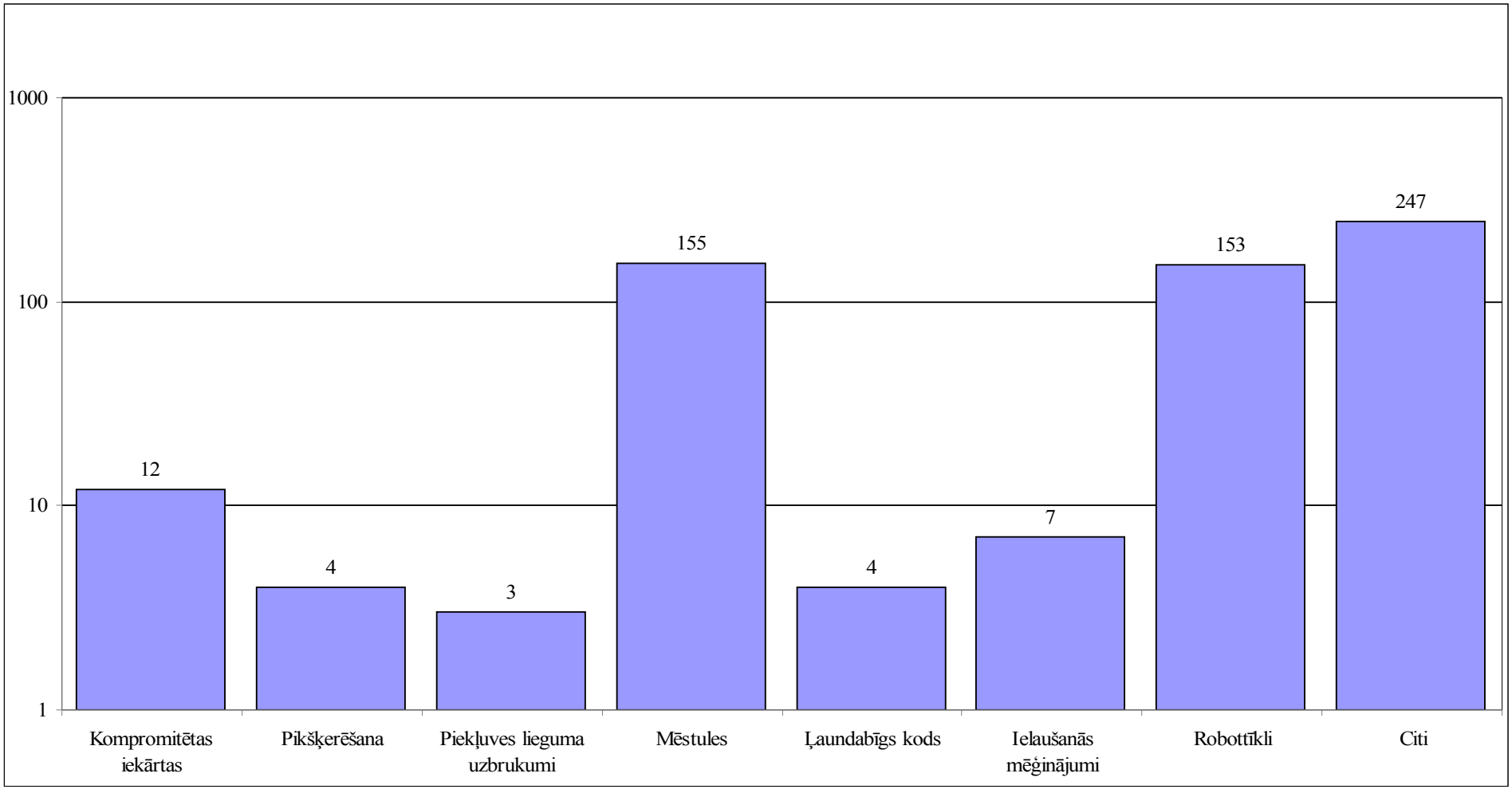


http://www.businessinsider.com/

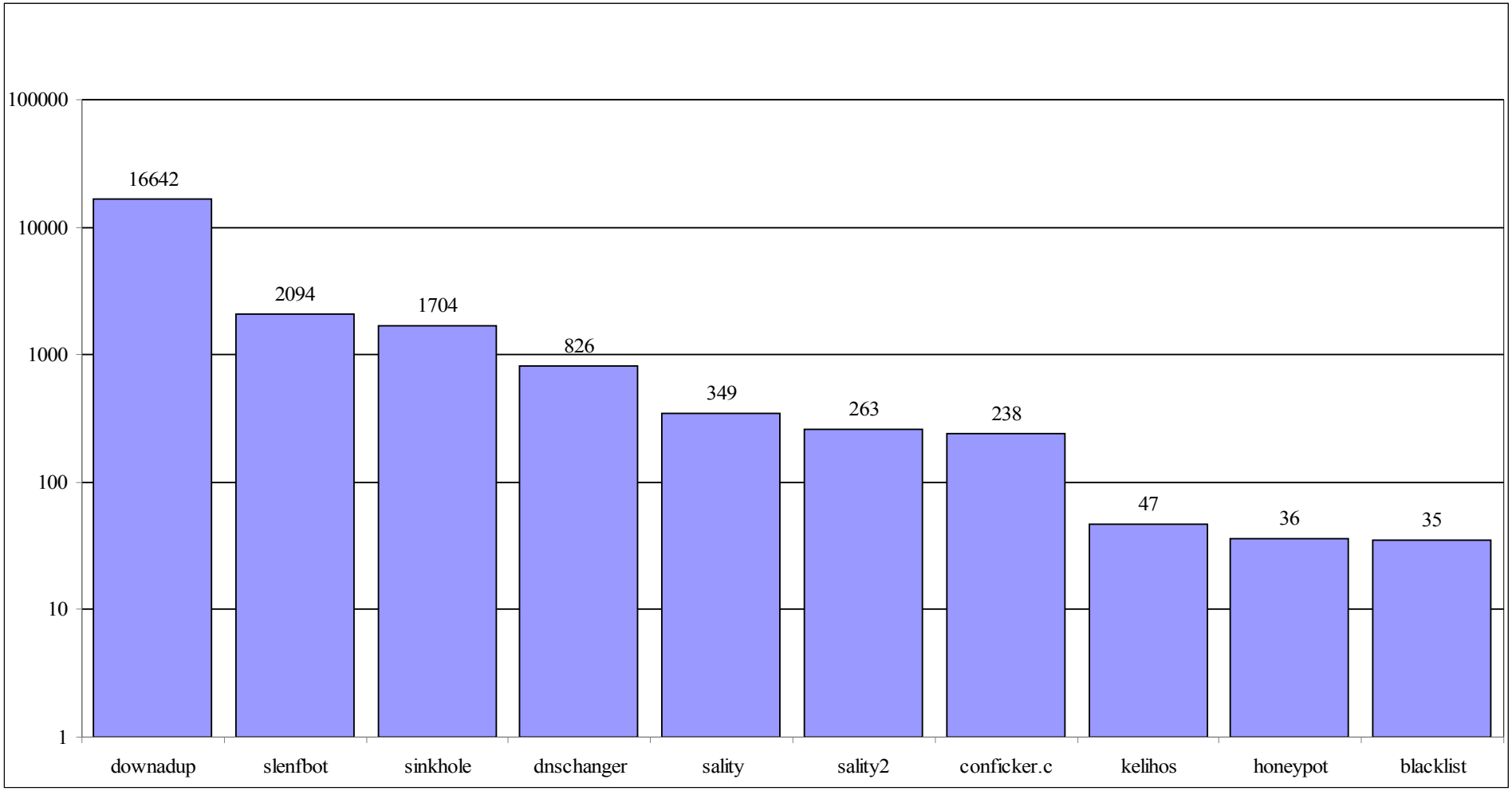
Aktuālā situācija

- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS
  - "Kvalitātes zīme" – kopā ar LIA
  - Lattelecom, Latnet Serviss, LMT, Baltkom, IZZI, Telia, Ilva, CSDD, Telecentrs

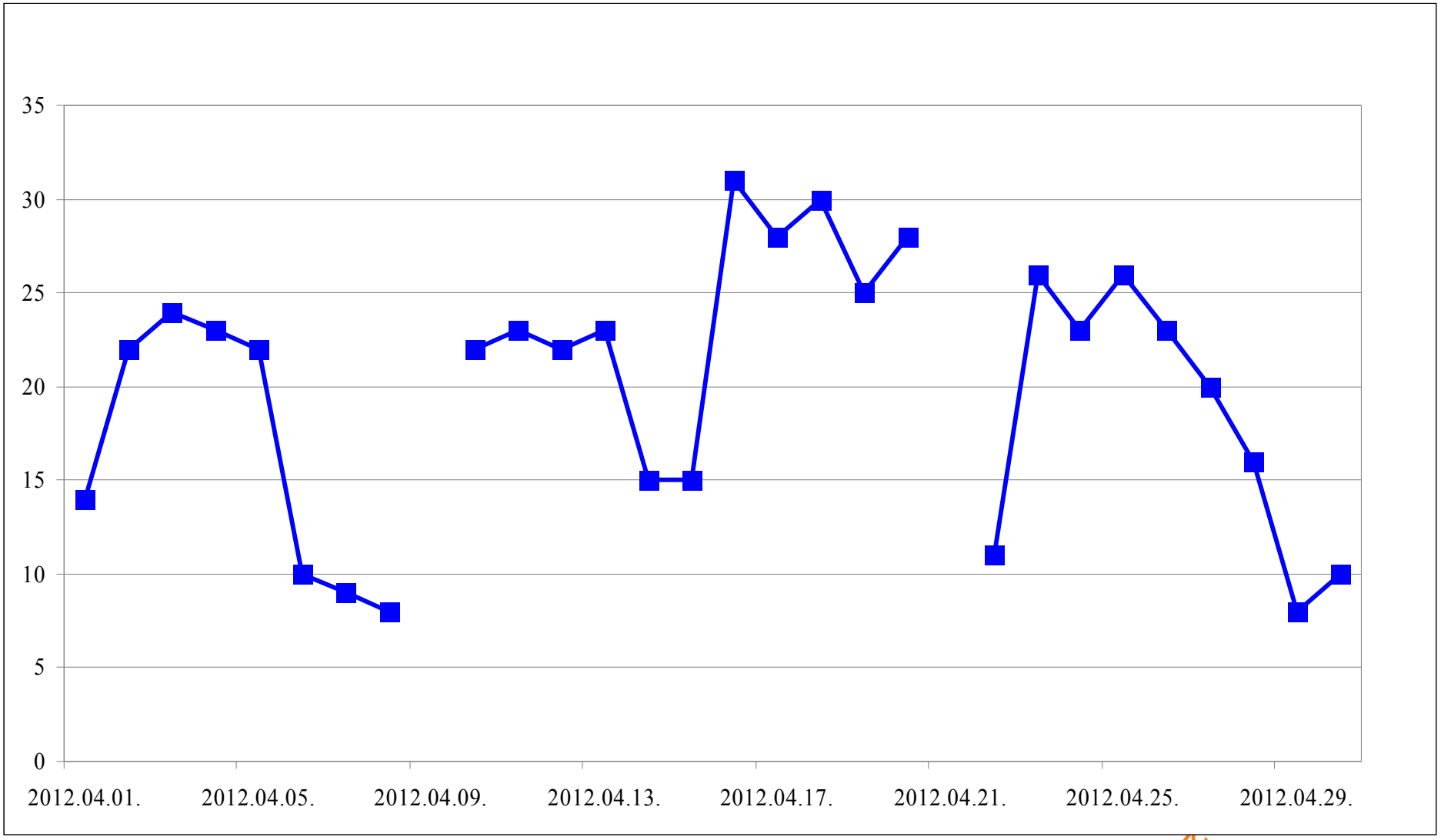
Augstas prioritātes incidenti – aprīlis 2012 - 585



Zemas prioritātes incidenti – aprīlis 2012 – 22457
Infekciju TOP10



Inficētās IP adreses Valsts & pašvaldību iestādēs

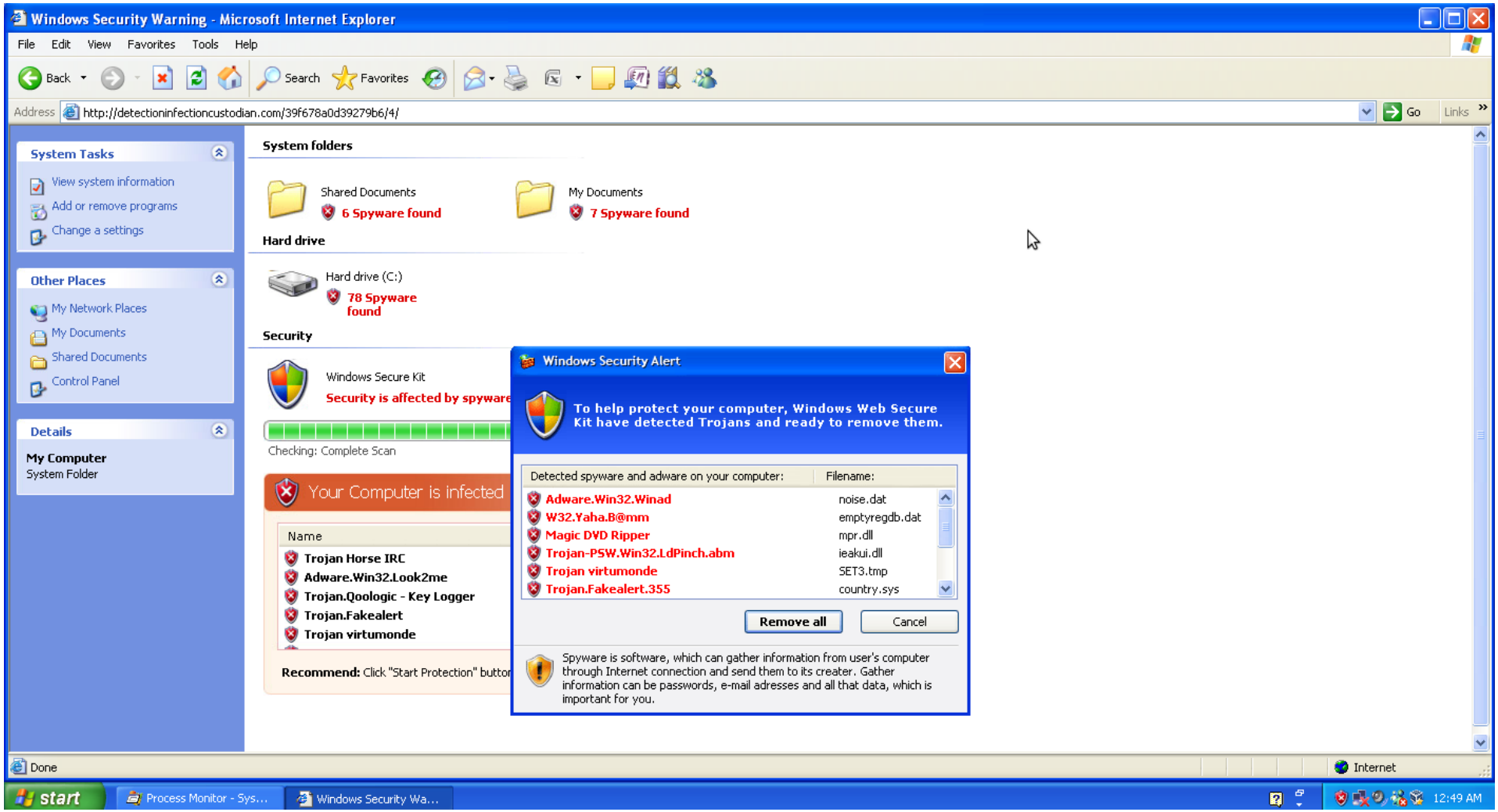


Delfi incident

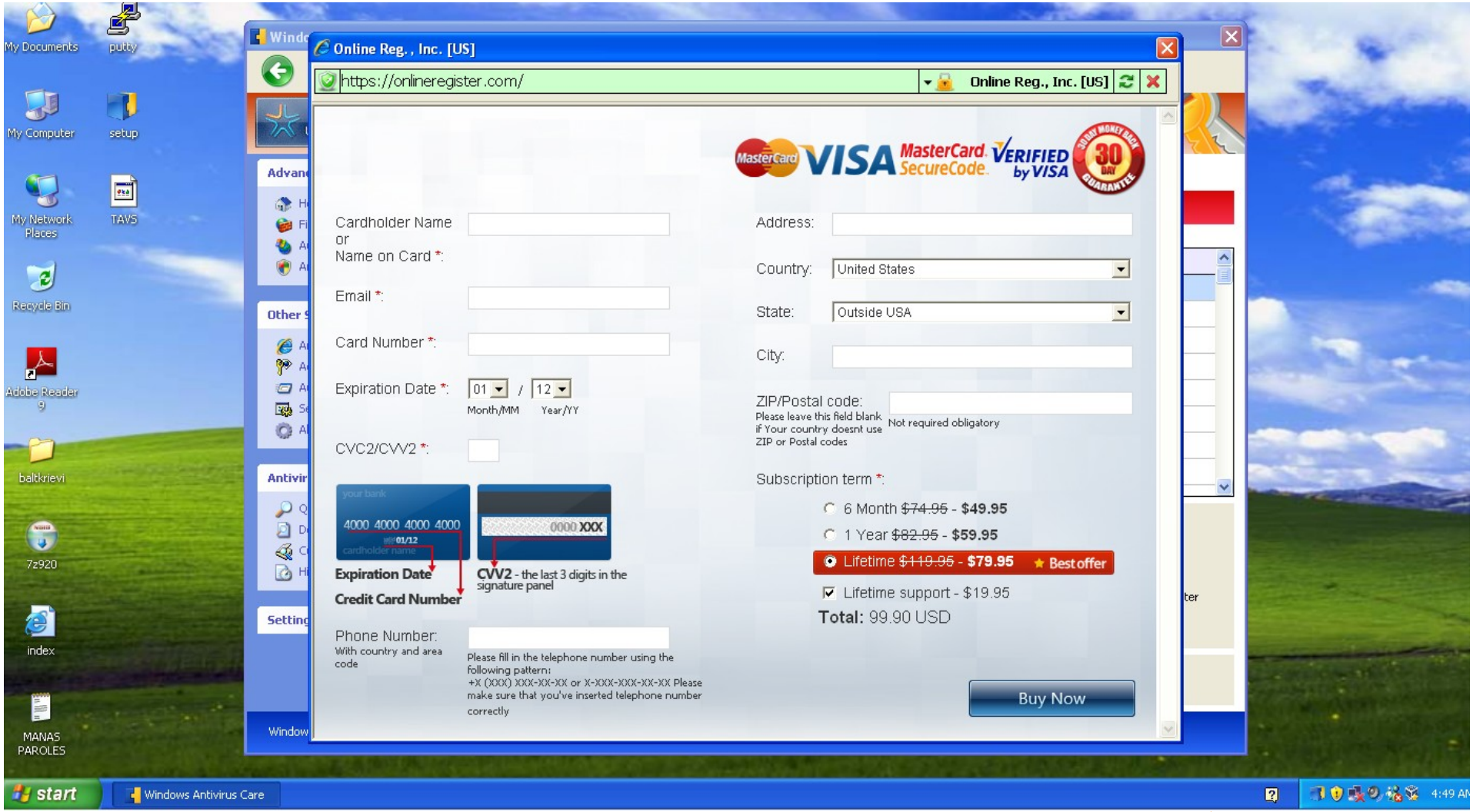
Piektdiena, 20. aprīlis (2012) 19:55

Riskē "saķert" datorvīrusu, ja pieļausi gramatiskas kļūdas portāla nosaukumā

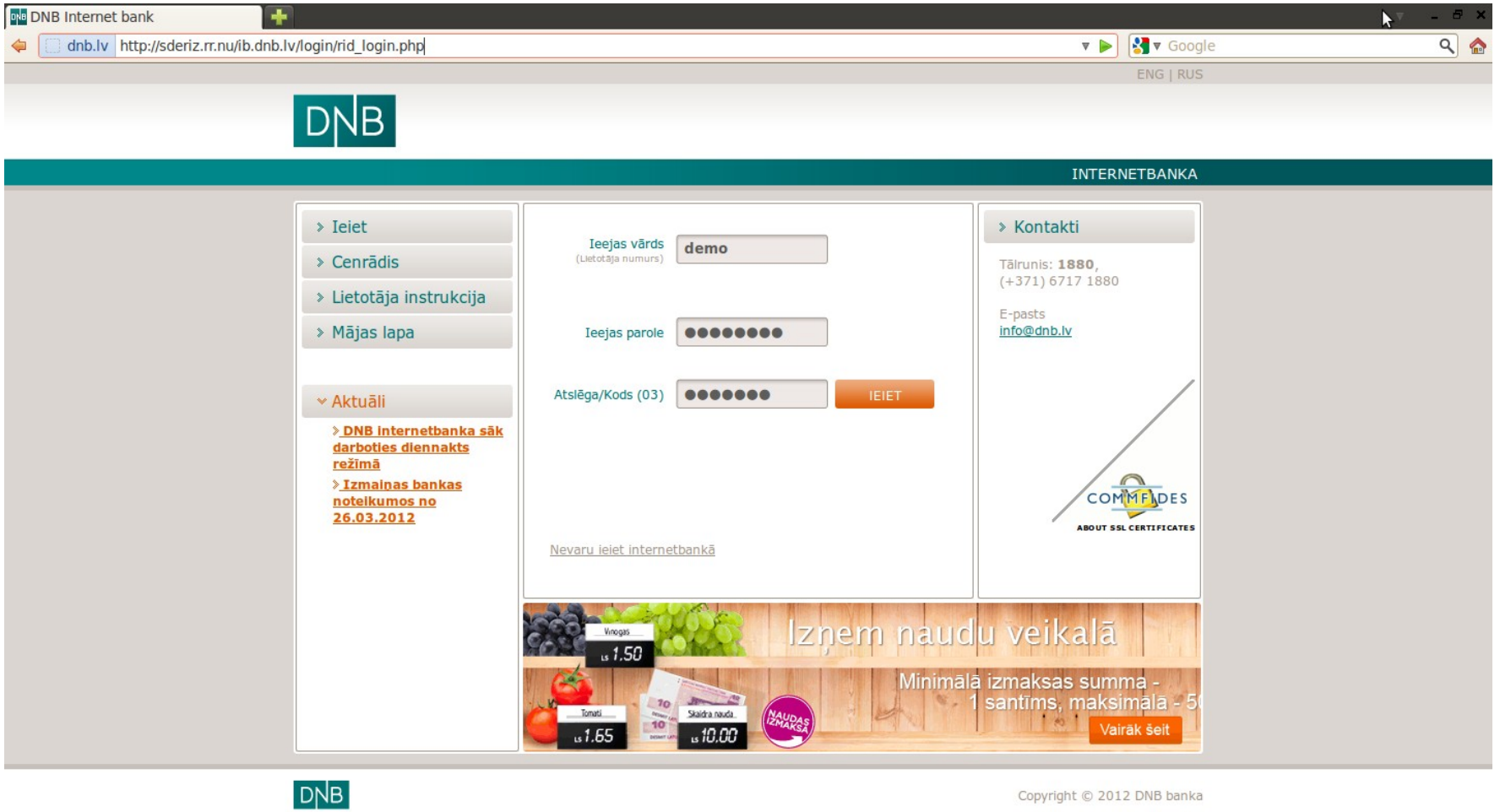
Delfi incident



Delfi incident



DNB bank incident



International cooperation – attacks to Azerbaijan

Subject	From	Date
Re: [1st-t] Helpdesk functionality	Marco Thorbruegge	10/19/2011 12:55 PM
[1st-t] Attack!!! Urgent HELP needed!!!	CERT.GOV.AZ	04/22/2012 06:31 PM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	hillar	04/22/2012 07:41 PM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	SWO@us-cert.gov	04/22/2012 08:24 PM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	first-teams-owner@lists.first.org	04/22/2012 09:09 PM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	Varis Teivans	04/22/2012 09:18 PM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	Brian Honan	12:00 AM
Re: [1st-t] Attack!!! Urgent HELP needed!!!	**Chad Greene**	**02:22 AM**
Re: [1st-t] Attack!!! Urgent HELP needed!!!	**mizamil**	**06:13 AM**
Re: [1st-t] Attack!!! Urgent HELP needed!!!	**Khalifa Al Shamsi**	**08:15 AM**
Re: [1st-t] Attack!!! Urgent HELP needed!!!	**Rohana Palliyaguru**	**08:56 AM**

reply | reply list | forward | archive | junk

from CERT.GOV.AZ <first-team@cert.gov.az>

subject **[1st-t] Attack!!! Urgent HELP needed!!!** 04/22/2012

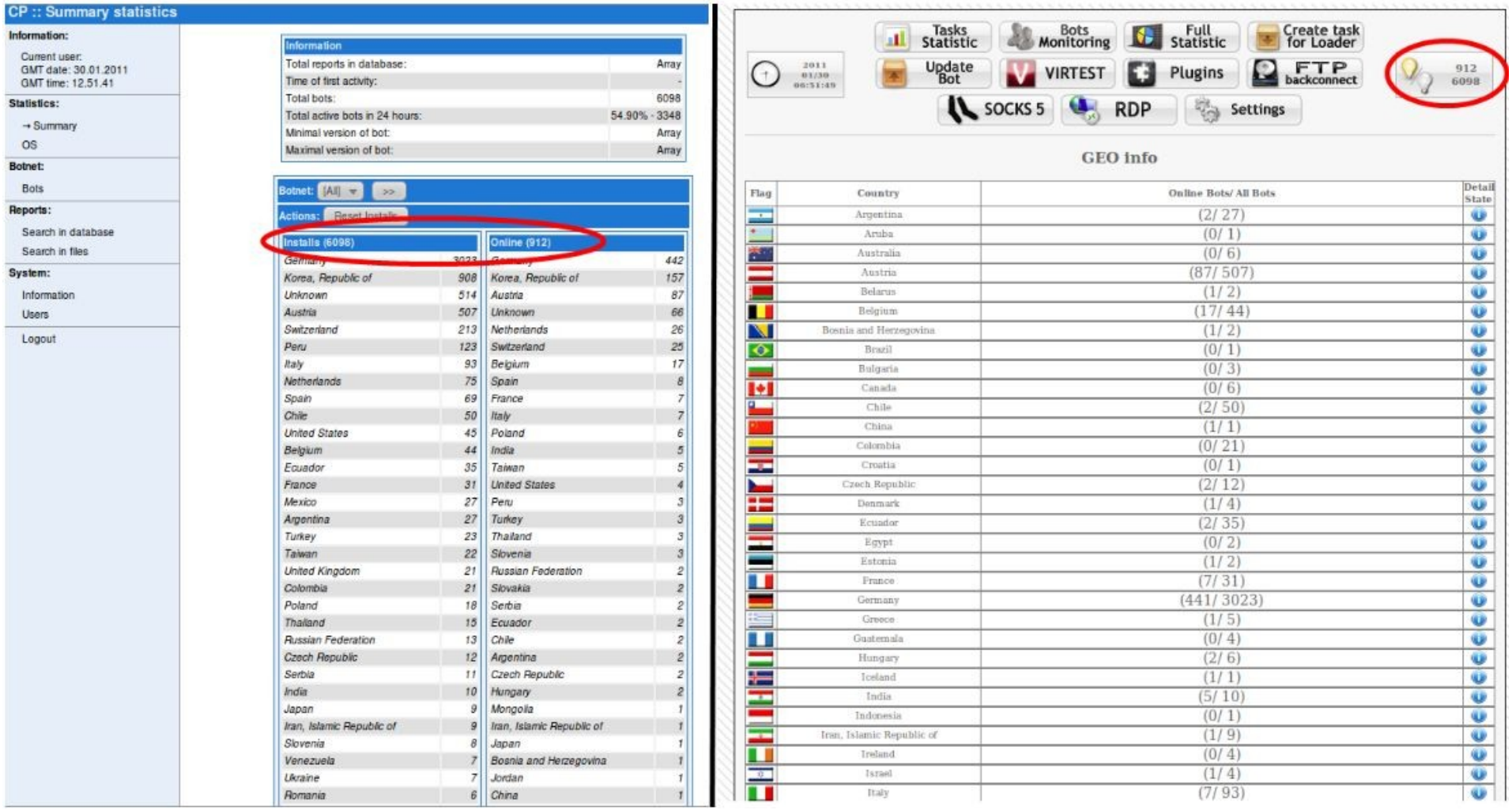
to 'FIRST Secretariat' <first-sec@first.org>

cc first-teams@first.org other

```
Dear Sirs,

I would like to inform you about the DDOS attack that we faced on
18/Apr/2012:19:59:18 +0500 - 18/Apr/2012:20:14:51 +0500 and on
18/Apr/2012:20:43:54 +0500 - 18/Apr/2012:20:57:37 +0500

During this attack the following proxy servers were used:

Attackers' ips (proxy servers)
 174.121.134.34 - UNITED STATES, TEXAS, DALLAS - THEPLANET.COM INTERNET
SERVICES INC
 209.140.23.180 - UNITED STATES, TEXAS, FULSHEAR - LANDIS HOLDINGS INC
 66.148.120.124 - UNITED STATES, NEVADA, SPARKS - HOPONE INTERNET
CORPORATION
 184.172.176.54 - UNITED STATES, TEXAS, DALLAS - THEPLANET.COM INTERNET
SERVICES INC
```

Chart info of... attack.xlsx | Country list of Attackers.txt | Ip list of ddos attacking.txt | Part 1.5

Uzbrucēja saskarne – Zeus robotu tīkls



Draudi

- Politiskās situācijas saasinājumi
- Mērķētie uzbrukumi
- Ļaunatūras izplatīšana no uzlauztajām lapām
- Pikšķerēšanas un citu uzbrukumu ticamības palielināšanās

Padomi un palīdzība

CERT.LV piedāvā

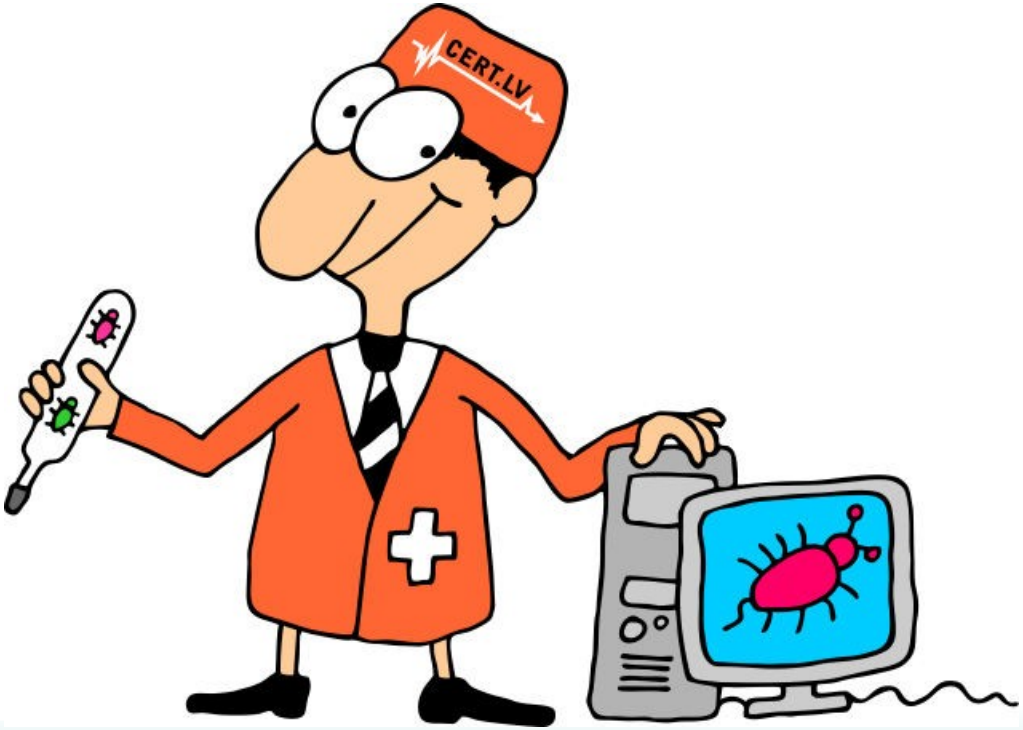
- Palīdzību incidentu risināšanā
- Piemēru darbinieku apmācības programmai
- Piemērus IT drošības dokumentiem
- Informāciju par inficētām IP adresēm un incidentiem
- Reģionālos seminārus

Noderīgi

- Incidenta gadījumā – sadarbība ar CERT.LV
- Pieaugušo izglītošanas portāls www.esidross.lv
- www.atveries.lv – brīvā programmatūra

Jauns “kolēģis” - datorologs

- Radies uz E-prasmju nedēļu
- Piedalījās ES Dārza svētkos
- Twitera konts @datorologs



E-prasmju nedēļa – 2012.gada marts

CERT.LV

ES Dārza svētki Vērmaņdārzā 12.maijā

CERT.LV

esi drošs

Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā

Meklēt...

Mājās | Darbā | Publiskās vietās | Ieteikumi | Par drošību | Pasākumi | Notikumi pasaulē

Tēmas

- Ap un par drošību (22)
- Darbā (16)
- Ieteikumu lāde (22)
- Mājās (24)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (6)
- Publiskās vietās (16)

Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija
- LV CSIRT iniciatīva
- Net-Safe Latvia Drošāka interneta centrs

Publikāciju kalendārs

aprīlis 2012

P	O	T	C	P	S	Sv
						1
2	3	4	5	6	7	8

Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!

Kāds uzņēmējs no Rīgas šodien līdz baltkvēlei nomocījis Datorologu, kurš, cenšoties izārstēt datoru, atradis tajā 110 dažādas bīstamības pakāpes vīrusus....

AKTUĀLIE RAKSTI

2012. gada 23. februāris 1

2012. gada 15. februāris 0

CERT.LV | NIC

Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta **ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā**. Mājas lapu uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tajā informācijas tehnoloģiju speciālisti no LV-CSIRT iniciatīvas grupas sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!
- Pārbaudi sava datora veselību pie Datorologa!

CERT.LV

esi drošs

Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā

Meklēt...

Mājās | Darbā | Publiskās vietās | Ieteikumi | Pasākumi | Notikumi pasaulē | Par drošību | Raksti

Tēmas

- Ap un par drošību (5)
- Darbā (7)
- Ieteikumu lāde (9)
- Mājās (15)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (1)
- Publiskās vietās (7)

Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija

VIDEO: Kā justies droši elektroniskā vidē?

Jūties droši elektroniskā vidē from EsiDrossLV on Vimeo. CERT.LV piedāvā jums noskatīties Latvijas Universitātes Informācijas sistēmu drošības pasniedzējas Ilzes Murānes...

Uzmanību! Saskaņā ar CERT.LV datiem, Jūsu dators ar IP adresi [redacted] ir inficēts ar datorvīrusu! Vairāk informācijas.

CERT.LV NIC

Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta **ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā.**

DNS Changer pārbaude – dns-ok.lv

Jūsu dators NAV inficēts ar DNS Changer

Kas ir DNS Changer?

DNS Changer ir ļaundabīga programmatūra, kas, ieperinoties jūsu datorā, apmaina jūsu izmantoto domēna vārdu serveri pret savu IP adresi. Tā rezultātā visi DNS pieprasījumi, ko jūsu dators sūta, tiek novirzīti uz ļaundabīgās programmas izstrādātāju kontrolētiem serveriem. Tie savukārt saņemtos pieprasījumus atrast mājas lapu novirza nevis uz lapu, kuru vēlaties atvērt, bet gan uz lapu ar sev vēlamo saturu. Piemēram, ja vēlaties veikt apmaksu, ievadot kartes datus, ļaundari jūs nosūtīs uz lapu, kurā kartes dati tiks ar pateicību pieņemti.

Otrkārt, šī ļaundabīgā programmatūra cenšas piekļūt upura maršrutētājam, kam uzstādīts DHCP serveris (piemēram, mājas bezvadu maršrutētājs). Programmatūra mēģina pieslēgties maršrutētājam, lietojot noklusētos ražotāja uzstādījumus. Ja piekļuve notiek sekmīgi, tā nomaina DNS serverus uz savējiem – viltus. Šīs izmaiņas ietekmē visus maršrutētāja lietotājus (datorus), pat tos, kas paši nav inficēti.

Kā notiek pārbaude?

Mirklī, kad verat lapu dns-ok.lv, jūsu dators vai maršrutētājs sūta pieprasījumu DNS serverim, kurš atrod, uz kādas IP adreses mājas lapa izvietota. Šobrīd visi ļaundabīgās programmas izstrādātāju uzstādītie viltus serveri ir apzināti. Tāpēc mēs varam pārbaudīt, vai DNS serveris, kuru izmantojat, ir šo ļaundabīgo serveru sarakstā. Ja ir, tad ir skaidrs, ka dators vai maršrutētājs ir inficēts.

Viltus DNS serveru IP adreses:

85.255.112.0 - 85.255.127.255
7.210.0.0 - 67.210.15.255
93.188.160.0 - 93.188.167.255
77.67.83.0 - 77.67.83.255
213.109.64.0 - 213.109.79.255
64.28.176.0 - 64.28.191.255

Nākotne

Nākotne

- Latvijas izvēlētais ceļš – drošība caur sadarbību
- IT drošības līmeni valstī var paaugstināt tikai kopīgiem spēkiem
- IT drošībai jākļūst par katra ikdienu
- Lietotāji jāturpina izglītot un ieinteresēt IT drošībā

CERT.LV attīstības perspektīvas

- Ministrijas maiņa no 2013.gada?
- Vidēja termiņa plānošana
- Svarīgi turpināt visu iesākto
- Izaugsme

Paldies par uzmanību!

http://www.cert.lv/

cert@cert.lv

baiba.kaskina@cert.lv

Semināra programma

13:30-14:00 “Situācija Latvijā IT drošības jomā un CERT.LV attīstības perspektīvas” – Baiba Kaškina, CERT.LV vadītāja

14:00-14:30 „Tīmekļa vietņu drošība” - Ēriks Dobelis, ISACA Latvijas nodaļas biedrs

14:30-15:00 „Bezvadu tīklu drošība” – Varis Teivāns, CERT.LV vadītāja vietnieks

15:00-15:30 pārtraukums

15:30 – 16:00 „Praktisks piemērs – risku novērtēšana un mazināšanas pasākumi” – Sintija Deruma, ISACA Latvijas nodaļas biedrs

16:00 – 16:30 „Rīcība ārkārtas situācijā” – Kristaps Miļevskis, LR CSP, Informācijas sistēmas drošības pārvaldnieks

16:30 – 17:00 „7 būtiski jautājumi par IT drošību” – CERT.LV un LV CSIRT grupas speciālistu sagatavotas atbildes