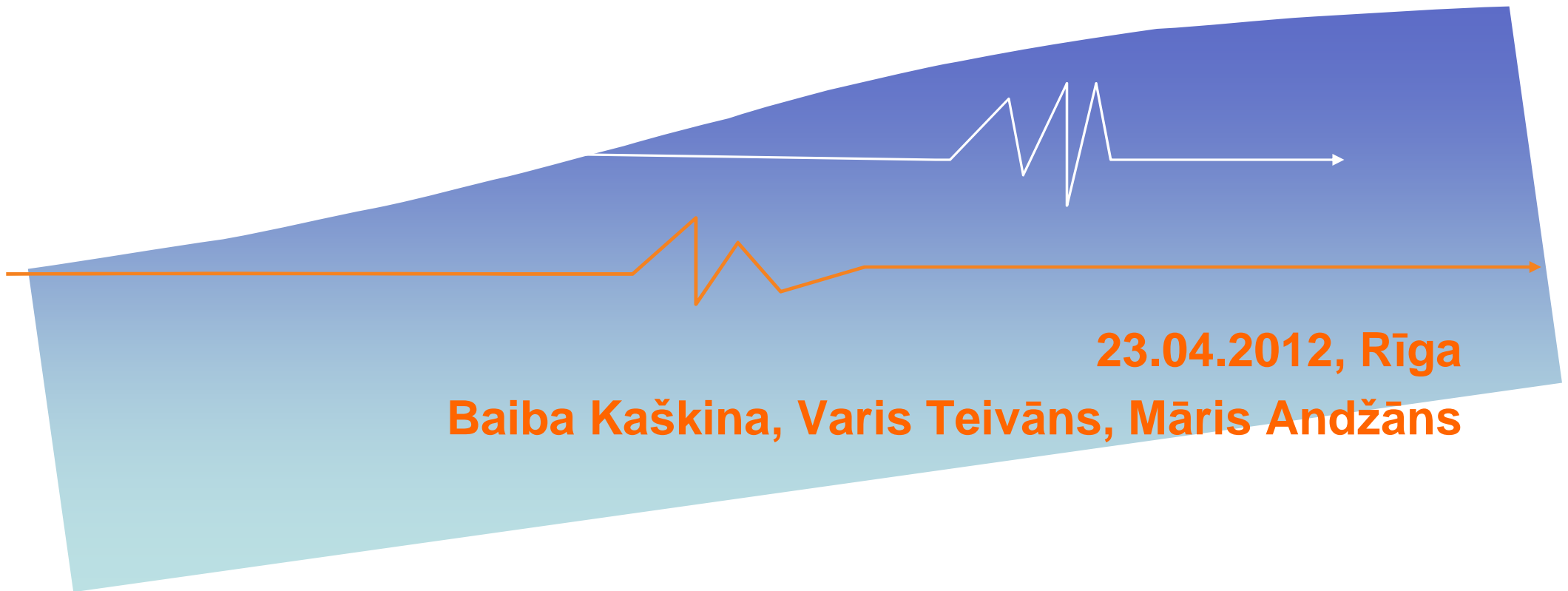
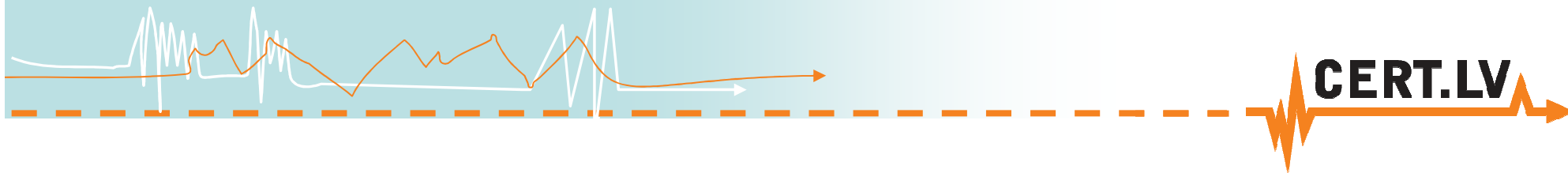


# *Situācija IT drošības jomā Latvijā*



**23.04.2012, Rīga**

**Baiba Kaškina, Varis Teivāns, Māris Andžāns**



**Par CERT.LV**



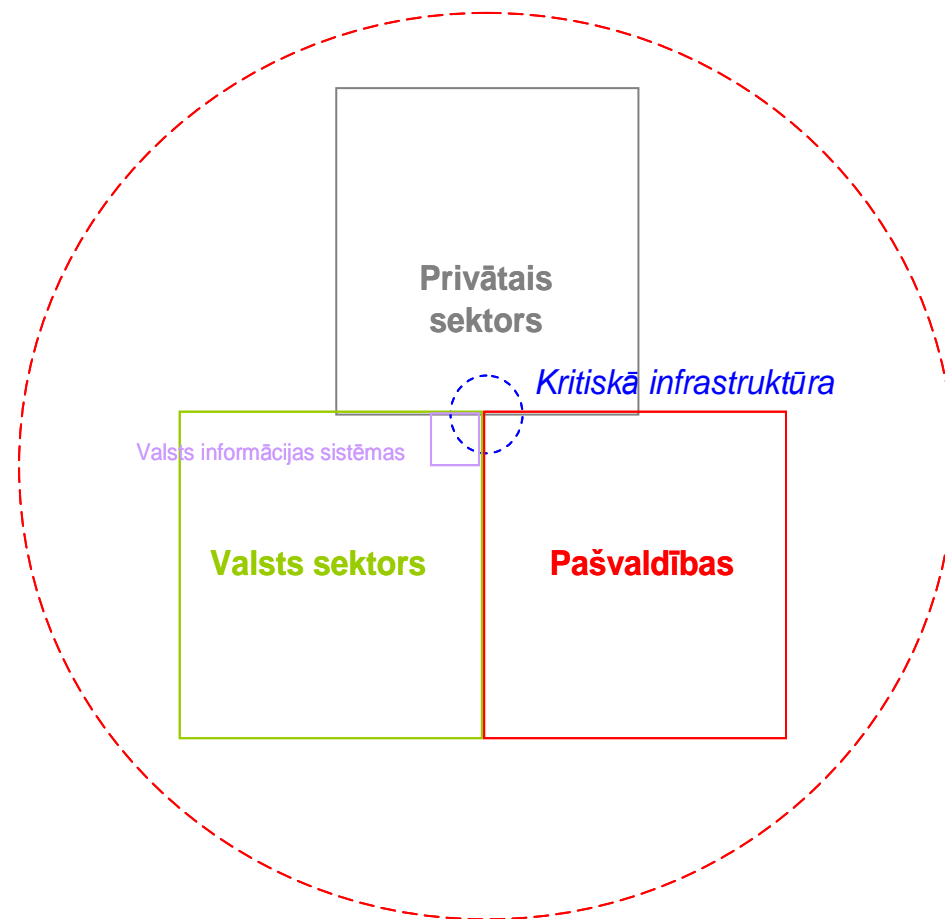
## CERT.LV

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
- Misija: “Veicināt IT drošību Latvijā”

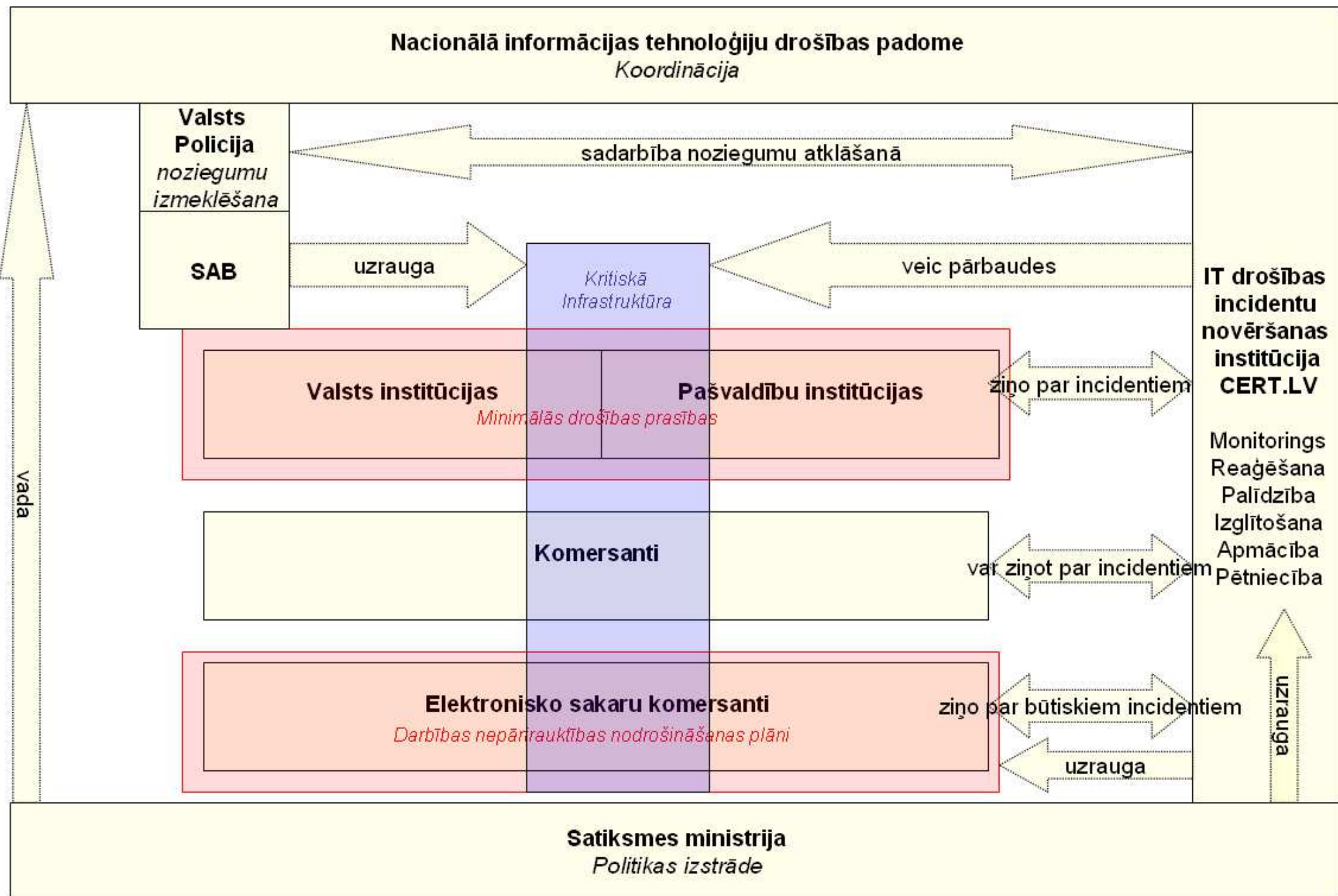
## CERT.LV

- 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 atainojums – būtiskākie elementi

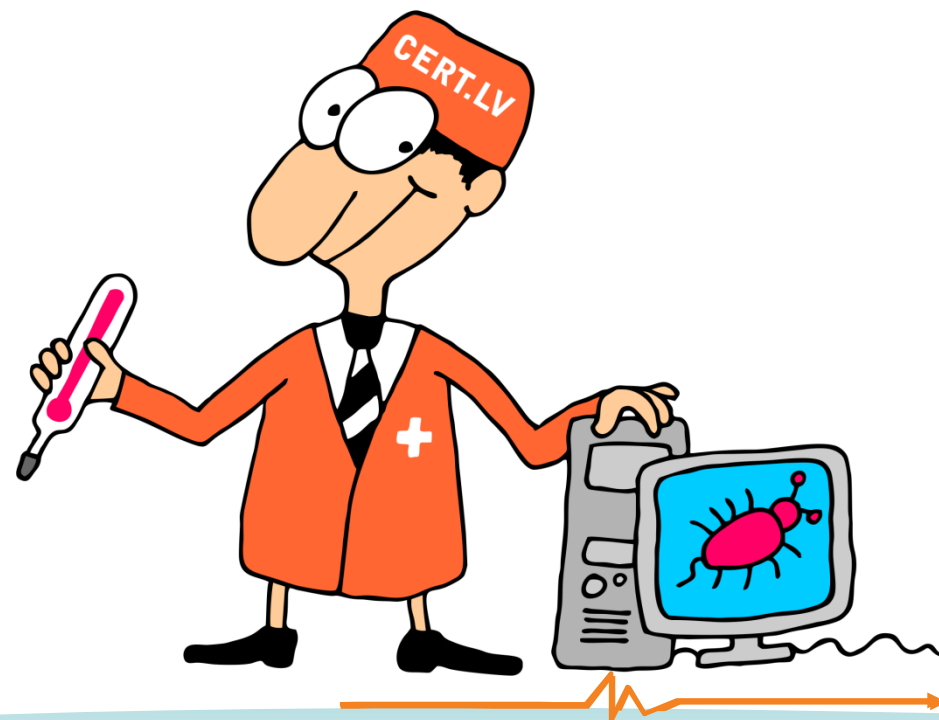


## CERT.LV sadarbības

- Valsts un pašvaldību iestādes
- IT Kritiskā infrastruktūra
- Privātais sektors
  - Elektronisko sakaru komersanti
  - Finanšu sektors
- Nevalstiskās organizācijas
- NBS
- Starptautiskie partneri
  - NATO, ENISA
  - Citu valstu līdzīgas institūcijas

## Kas ir CERT.LV?

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



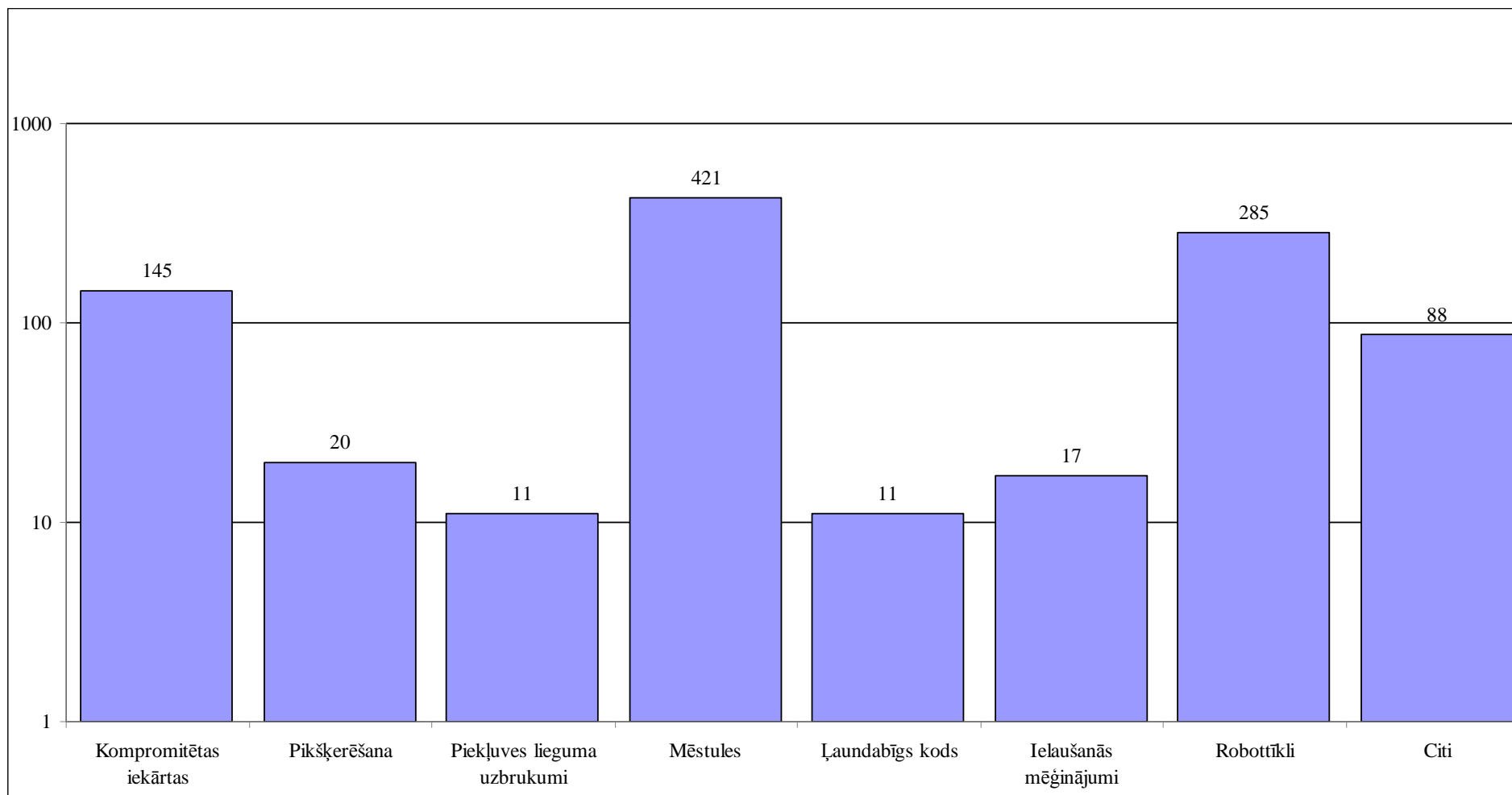


# Aktuālā situācija Latvijā

## Aktuālā situācija

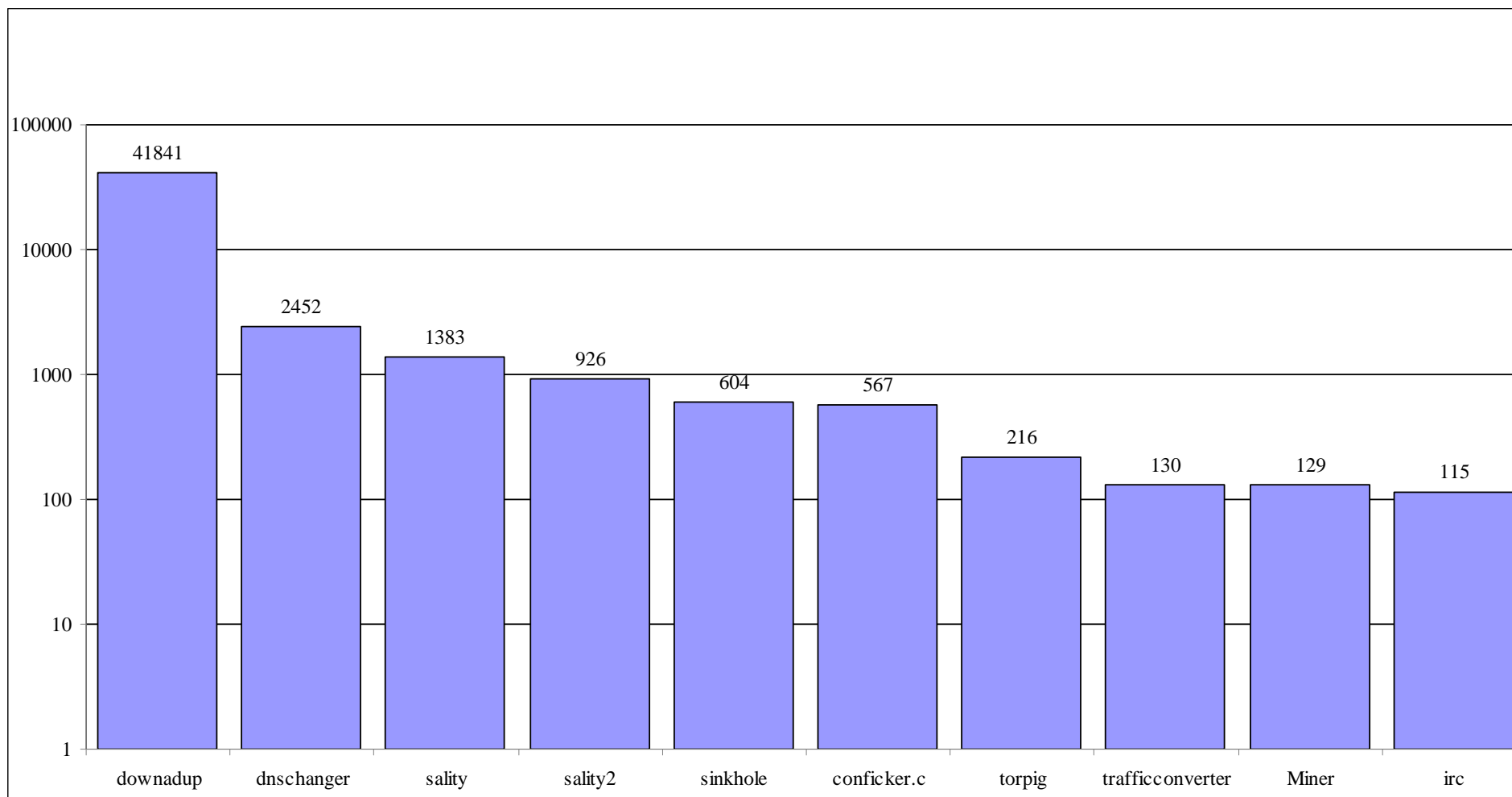
- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS

# Augstas prioritātes incidenti – 1.ceturksnis - 998

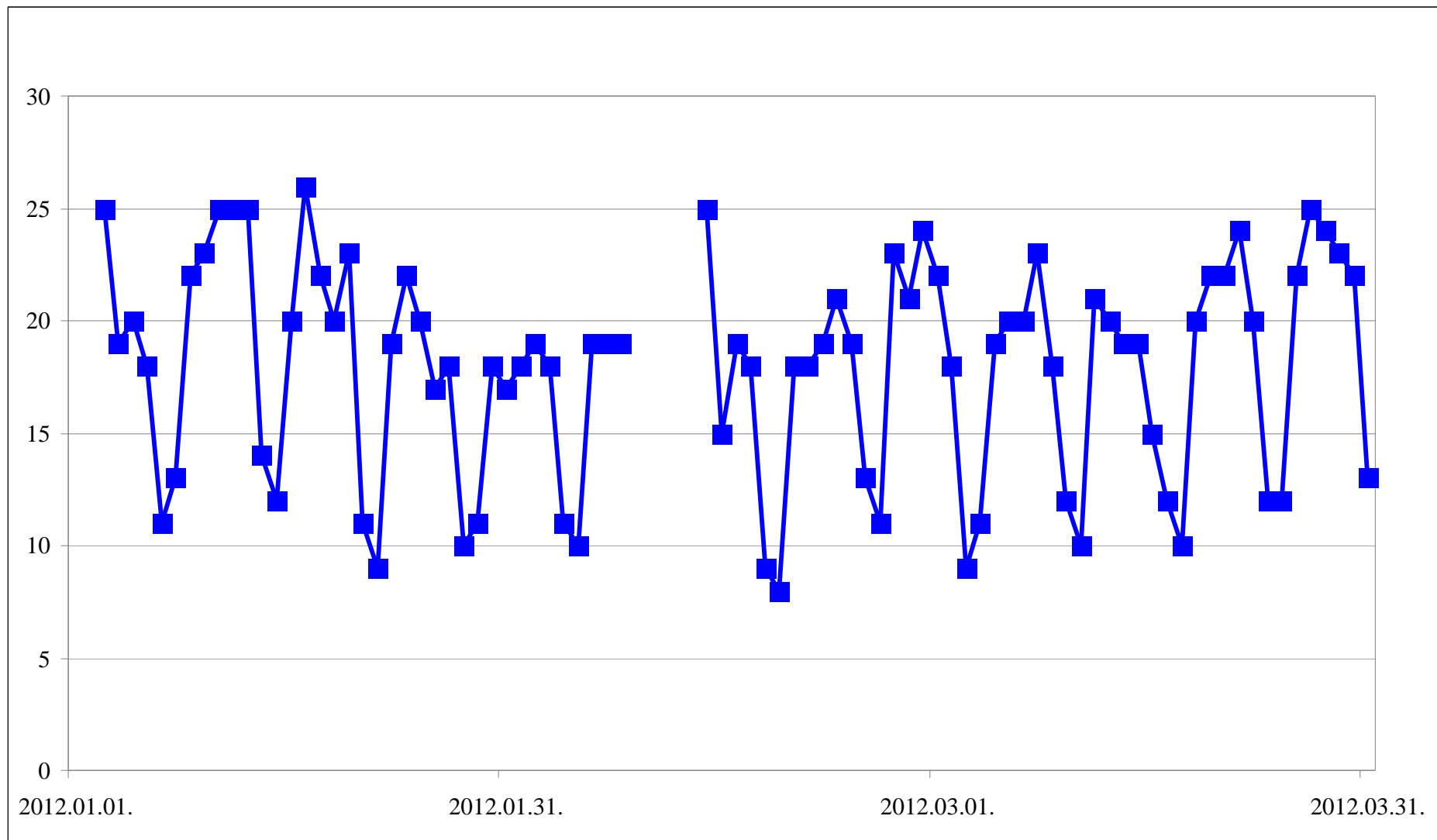


# Zemas prioritātes incidenti – 1.ceturksnis – 48841

## Infekciju TOP10



## Inficētās IP adreses Valsts & pašvaldību iestādēs



## Aktuālā situācija

- Robotu tīklos esošo datoru skaits joprojām liels
- Inficēšanās caur pārlūkprogrammām
- Serveru uzlaušanas, pikšķerēšana, piekļuves liegšanas uzbrukumi
- Uzbrukumi sociāli jutīgos brīžos
- Ļaundabīgās programmatūras izplatīšana

# Latvenergo incidents

## Latvian Electricity Grid Hacked !! So claims a Chinese Group

May 4, 2011 CIIP [Go to comments](#) [Leave a comment](#)

A recent post in the [full disclosure list \(FDL\)](#) claims that a Latvian Power Plant called (Latvenergo RIGAS HES-2) has been hacked. the post is strikingly similar in its approach to the recent FPL SCADA incident/Hoax.

Similarities:

- The FPL post was sent to the FDL at 8:22 (-7) PDT
- The RIGAS post was sent to the FDL at 8:48 (-7) PDT
- The FPL email that the hacker BGR sent me was sent from a Yahoo account, this time they used Rocketmail.com (owned by Yahoo)
- Both started by posting real IPs owned by reportedly the victims
- Both posted Images/screen shots hosted at Imageshack.us
- Both pasted the Cisco router configuration files along with the passwords

The screen shots were taken from a windows PC that also shows a lotus notes mailbox named (Leva Vaica).

I would assume from the pop up below that this is an Asus Laptop and not a desktop, since the EPU-4 Engine is a mother board with integrated graphics mostly used in Asus Laptops for power saving.

### Email Subscription

Enter your email address to follow this blog and receive notifications of new posts by email.

Sign me up!

### CIIP Events Calendar

- Meridian International CIIP Conference 2011 - Qatar
- Information Security in the Energy Sector - Qatar
- SCADA Security Scientific Symposium [S4] ( 20-21 January) - Miami Beach ,FL.
- Meridian 2009 (CIIP) (<http://www.meridian2009.org>)
- SCADA & Control Systems Security Summit - IQPC ([www.scadasecuritysummit.com](http://www.scadasecuritysummit.com))

### George Mason CIP Reports (Monthly)

- Invitation to attend X-SCM: The New Science of Extreme Supply Chain Management Conference
- Washington DC's Preeminent Government & Business Continuity Thought Leadership Event is Back!
- The CIP Report: March 2012 - Critical Manufacturing Sector

### Okamalo Security Watch

- End of Year Security Reports, The Complete List
- GSM Security, 2011
- Ad Networks Drive-by Download attack

Scripts Currently Forbidden | <SCRIPT>: 35 | <OBJECT>: 0

Options...

## LETA incidents



Šī ir Google <http://www.leta.lv> kešatmiņa. Šis ir lapas momentuzņēmums, kāda tā ir parādījies 27 apr 2011 08:33:19 GMT. [Pašreizējā lapa](#) laika gaitā, iespējams, ir mainījies. [Plašāka informācija](#)

Šie vaicājumi parādās tikai saitēs, kas norāda uz šo lapu: **leta lv** [Tikai teksta versija](#)

Dārgie koleģi, pirms publicēt apšaubamu speciālistu viedokļus par nelielu serveru hostingu kompānijam un diskutēt par kompetenci, ieteiktu tomēr pārskatīt šo nomelnojošo ziņu saturu, un parstat publicēt šos aizvainojošos reklamrakstus. Ka redzat- nekas nav drošs un neuzlauzams- JA vajag, tapec nevajag lekt augstāk par savu d. Paldies par uzmanību. Hakeris. [Atsauce](#)



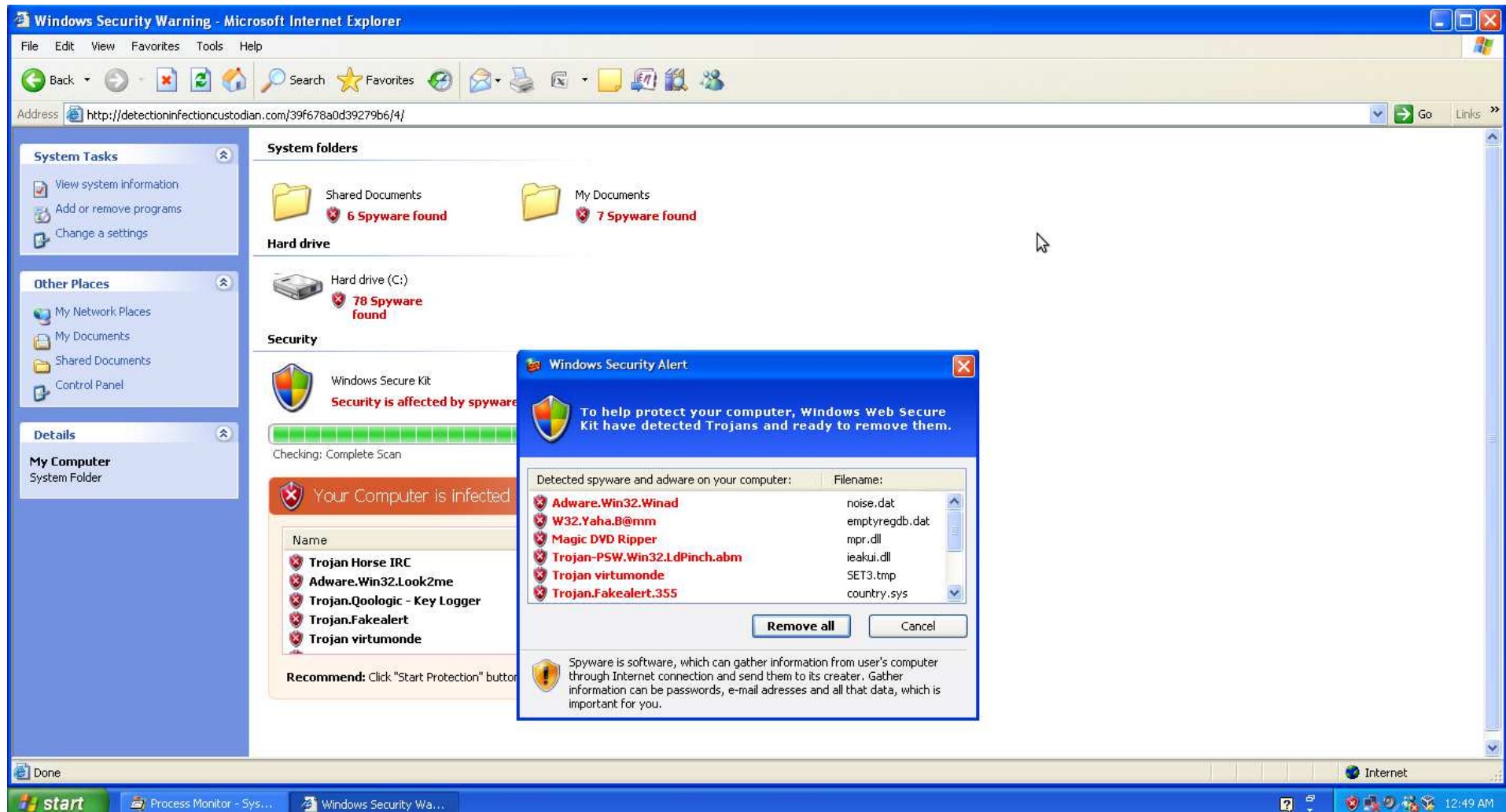
## Delfi incidents

Piektdiena, 20. aprīlis (2012) 19:55

### **Riskē "saņert" datorvīrusu, ja pieļausi gramatiskas kļūdas portāla nosaukumā**



# Delfi incidents



The screenshot shows a Windows Security Warning window in Microsoft Internet Explorer. The address bar displays a URL from detectioninfectioncustodian.com. The main content area shows a system scan progress bar and a list of detected threats. A 'Windows Security Alert' dialog box is overlaid on the screen, listing detected spyware and adware with their filenames. The taskbar at the bottom shows the Start button, Process Monitor, and the Windows Security Warning window.

**System folders:**

- Shared Documents: 6 Spyware found
- My Documents: 7 Spyware found

**Hard drive:**

- Hard drive (C:): 78 Spyware found

**Security:**

Windows Secure Kit  
 Security is affected by spyware

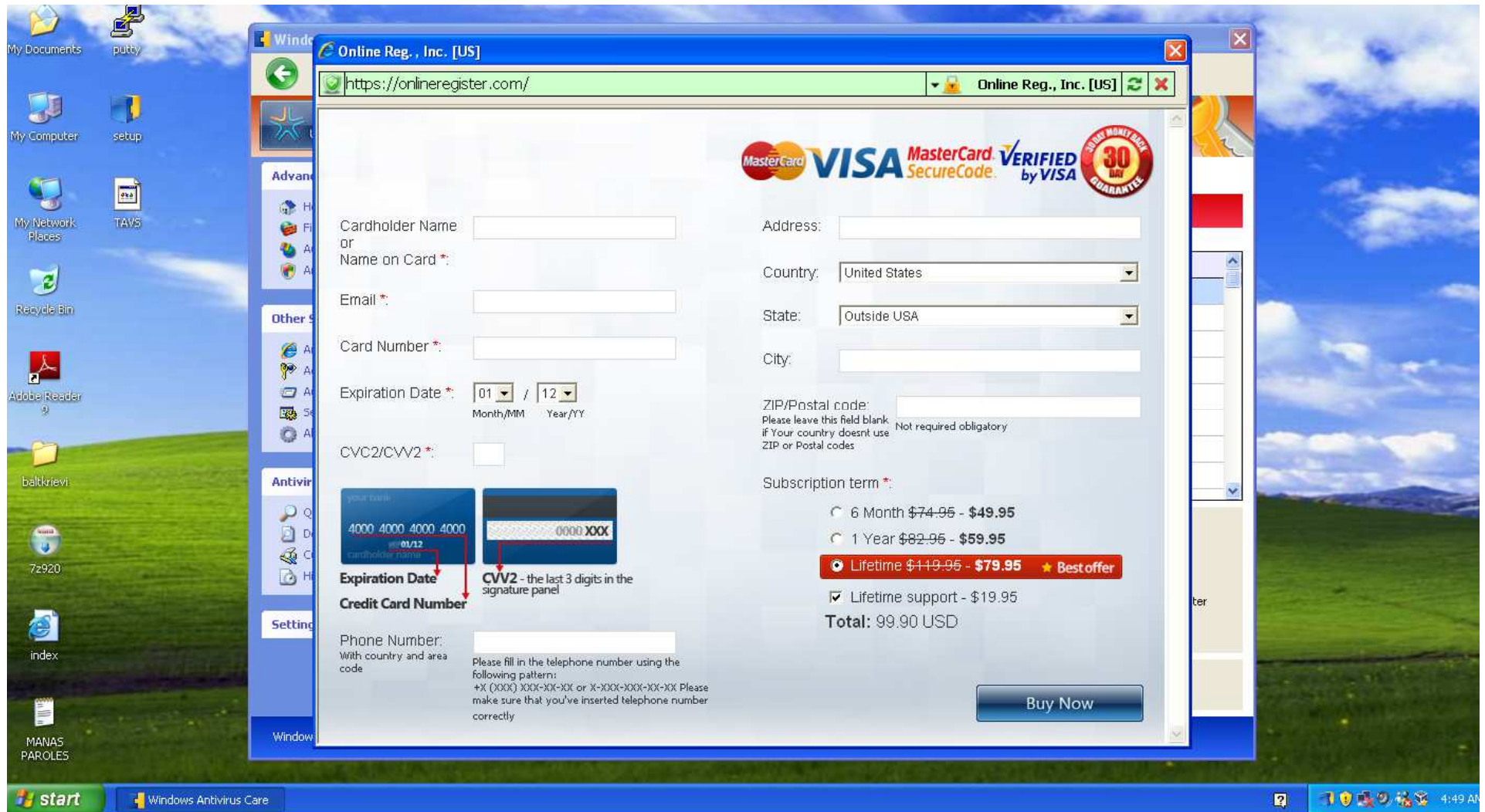
Checking: Complete Scan

**Your Computer is Infected**

Name	Filename
Trojan Horse IRC	
Adware.Win32.Look2me	
Trojan.Qoologic - Key Logger	
Trojan.Fakealert	
Trojan virtumonde	
Adware.Win32.Winad	noise.dat
W32.Yaha.B@mm	emptyregdb.dat
Magic DVD Ripper	mpr.dll
Trojan-PSW.Win32.LdPinch.abm	ieakui.dll
Trojan virtumonde	SET3.tmp
Trojan.Fakealert.355	country.sys

**Recommend:** Click "Start Protection" button

# Delfi incidents



# Neatliekamās medicīniskās palīdzības dienesta incidents

**Mirror saved on:** 2011-10-22 17:00:38

**Notified by:** Over-X

**Domain:** [http://www.nmpd.gov.lv/in\\_site/templates/output/output.tpl](http://www.nmpd.gov.lv/in_site/templates/output/output.tpl)

**IP address:** 92.240.65.137

**System:** Linux

**Web server:** Apache

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-10-22 17:00:38


Hacked By Over-X THNX TO : indoushka & jago-dz & ked ans

# Valsts Administrācijas skolas incidents

Mirror saved on: 2011-03-09 01:41:02

**Notified by:** iskorpitx

**Domain:** <http://www.vas.gov.lv/templates/beeZ/index.php>

**IP address:** 92.240.65.137 

**System:** Linux

**Web server:** Apache

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-03-09 01:41:02

\_shell\_atildi\_

by iskorpitx

O BiR KRAL


hackerler vurur lamerler inler!!

# Rīgas pašvaldības policijas incidents

Mirror saved on: 2011-12-22 18:54:10

Notified by: LatinHackTeam

Domain: <http://rpp.riga.lv>

IP address: 213.175.125.78 

System: FreeBSD

Web server: Apache

[Notifier stats](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-12-22 18:54:10

- [Ceļu policijas pārvalde](#)
- [Ūdenslīdēju, glābēju un civilās aizsardzības nodaļa](#)

- [Arhīvs](#)
  - [Informācija medijiem](#)

Reklāmkarogs

[Reklāmkarogs](#)

[Reklāmkarogs](#)

[Reklāmkarogs](#)

h4x0r3d by LatinHackTeam

**h4x0r3d by LatinHackTeam**

**follow us at @infekt1 @LatinHackTeam**

# Sadarbība ar finanšu sektoru

- Pikšķerēšanas incidenti
- Identitātes zādzības
- Pieredzes apmaiņa

# DNB bankas incidents

Ziņas | Situācija | Adresāri | Kontakti

**nra.lv** Sestdiena, 14.aprīlis **+11°C** 7 m/s DR uz plkst.14  
 Vārda dienas: Gudrīte, Strauja Saule lec 06:18, riet 20:31

Sākums Rīgā **Latvijā** Pasaulē Ekonomika Sports Izklaide Viedokļi Foto

Latvijā - Kriminālziņas | 20.jūlijs 2011, 13:25  
 Portāls nra.lv

Drukāt Komentēt Rakstīt redakcijai

## DnB Nord Banka brīdina par viltus e-pasta vēstulēm

DnB NORD Banka brīdina, ka bankas klienti, kā arī ar banku nesaistīti cilvēki ir saņēmuši viltus e-pastus, kas nosūtīti it kā DnB NORD vārdā. Banka aicina neveikt nekādas darbības e-pastā norādītajā interneta vietnē un šo e-pastu dzēst.

Cilvēkiem izsūtīti viltus e-pasti ar saiti uz interneta vietni, kurā tiek prasīts ievadīt internetbankas lietotāja datus – ieejas vārdu, paroli un kodus. Interneta vietne, uz kuru ved saite no viltus e-pasta, pēc sava vizuālā noformējuma ir ļoti līdzīga īstajai internetbankas iNORD ieejas lapai.

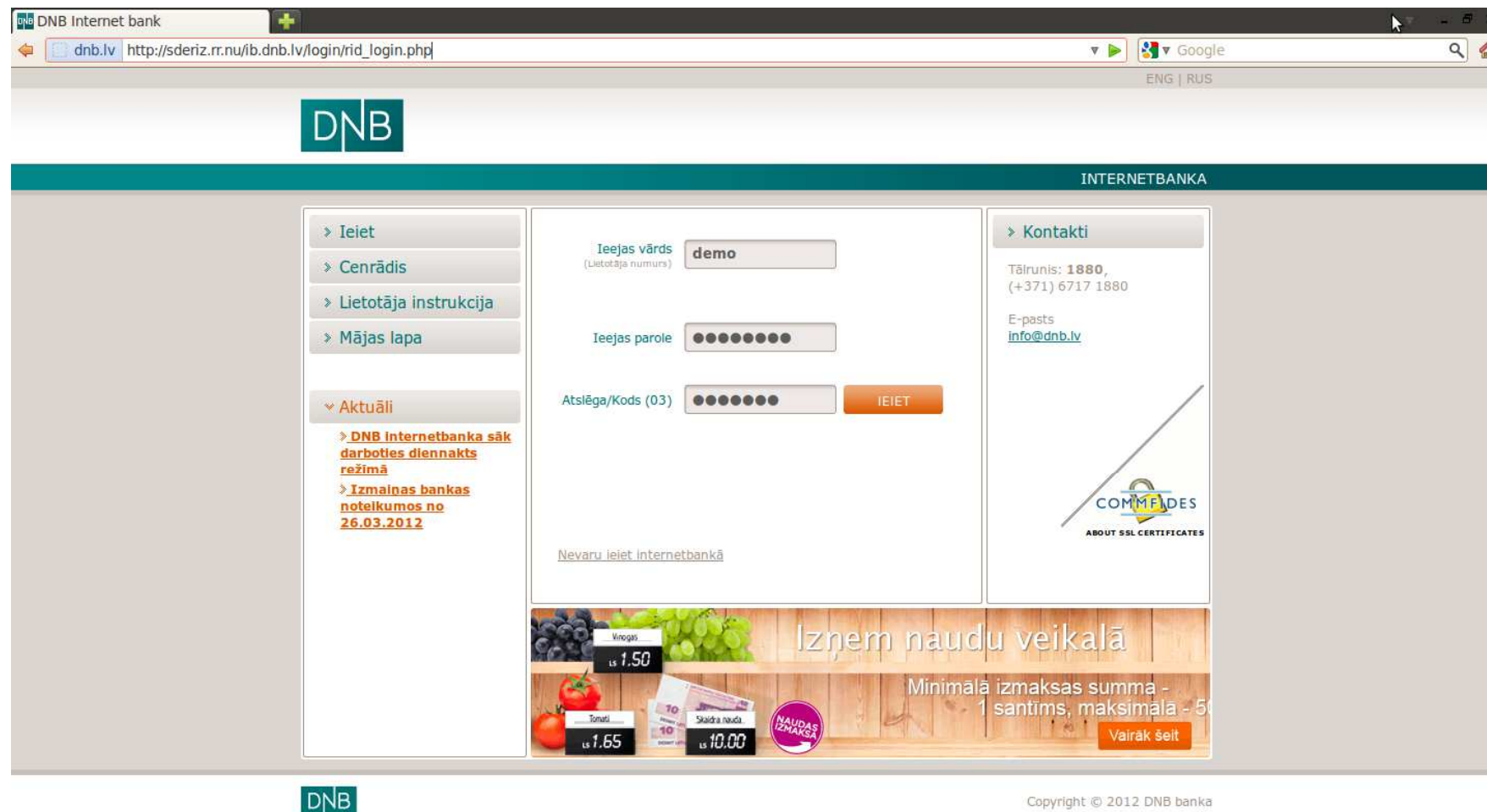
Banka uzsver, ka nekad nesūta šāda veida e-pastus un nelūdz no klienta datus, kas nepieciešami internetbankas lietošanai (paroles un kodus). DnB NORD Banka atgādina, ka iekļūt internetbankā iNORD var no bankas mājas lapas [www.dnbnord.lv](http://www.dnbnord.lv) vai arī, lietojot tiešo adresi <https://www.inord.lv>.

Šis krāpšanas veids pasaulē ir pazīstams ar apzīmējumu „phishing”. Krāpnieki, izsūtot šādus e-pastus, mēģina maldināt cilvēkus un ļaunprātīgi izvilināt konfidenciālu informāciju no banku klientiem.

Ja bankas klientiem rodas šaubas par kādu savu darījumu, no bankas saņemtu e-pastu, vēstuli vai zvanu, DnB NORD Banka lūdz nekavējoties sazināties ar banku (e-pasts: [info@dnbnord.lv](mailto:info@dnbnord.lv), tālr. 1880). DnB NORD Banka rūpējas par savu klientu drošību, tādēļ jebkura sīkāka informācija par



# DNB bankas incidents



The screenshot shows the DNB Internet bank login page. The browser address bar displays the URL `http://sderiz.rr.nu/ib.dnb.lv/login/rid_login.php`. The page features a login form with the following fields:

- Ieejas vārds (Lietotāja numurs):
- Ieejas parole:
- Atslēga/Kods (03):

An orange **IEIET** button is located to the right of the third field. Below the login form, a link reads [Nevaru ieiet internetbankā](#).

On the left side, there is a navigation menu with links: [Ieiet](#), [Cenrādis](#), [Lietotāja instrukcija](#), [Mājas lapa](#), and **Aktuāli**. Under **Aktuāli**, there are two news items:

- [DNB Internetbanka sāk darboties diennakts režīmā](#)
- [Izmaiņas bankas noteikumos no 26.03.2012](#)

On the right side, there is a **Kontakti** section with the following information:

- Tālrunis: **1880**, (+371) 6717 1880
- E-pasts: [info@dnb.lv](mailto:info@dnb.lv)

Below the contact information is a logo for **COMFIDES** with the text **ABOUT SSL CERTIFICATES**.

At the bottom of the page, there is a promotional banner for a store with the text **Izņem naudu veikalā**. It includes images of groceries (grapes, tomatoes) and banknotes (10, 10.00). The banner also states: **Minimālā izmaksas summa - 1 santims, maksimālā - 5**. A **Vairāk šeit** button is also present.

The footer contains the DNB logo and the text **Copyright © 2012 DNB banka**.

# Uzbrucēja saskarne – Zeus robotu tīkls

**CP :: Summary statistics**

**Information:**  
 Current user:  
 GMT date: 30.01.2011  
 GMT time: 12.51.41

**Statistics:**  
 → Summary  
 OS

**Botnet:**  
 Bots

**Reports:**  
 Search in database  
 Search in files

**System:**  
 Information  
 Users  
 Logout

**Information**  
 Total reports in database: Array  
 Time of first activity: -  
 Total bots: 6098  
 Total active bots in 24 hours: 54.90% - 3348  
 Minimal version of bot: Array  
 Maximal version of bot: Array

Botnet: [All] >>

Actions: [Open installs](#)

Installs (6098)		Online (912)	
Germany	3023	Germany	442
Korea, Republic of	908	Korea, Republic of	157
Unknown	514	Austria	87
Austria	507	Unknown	66
Switzerland	213	Netherlands	26
Peru	123	Switzerland	25
Italy	93	Belgium	17
Netherlands	75	Spain	9
Spain	69	France	7
Chile	50	Italy	7
United States	45	Poland	6
Belgium	44	India	5
Ecuador	35	Taiwan	5
France	31	United States	4
Mexico	27	Peru	3
Argentina	27	Turkey	3
Turkey	23	Thailand	3
Taiwan	22	Slovenia	3
United Kingdom	21	Russian Federation	2
Colombia	21	Slovakia	2
Poland	18	Serbia	2
Thailand	15	Ecuador	2
Russian Federation	13	Chile	2
Czech Republic	12	Argentina	2
Serbia	11	Czech Republic	2
India	10	Hungary	2
Japan	9	Mongolia	1
Iran, Islamic Republic of	9	Iran, Islamic Republic of	1
Slovenia	8	Japan	1
Venezuela	7	Bosnia and Herzegovina	1
Ukraine	7	Jordan	1
Romania	6	China	1

2011 01/30 00:51:48

Tasks Statistic | Bots Monitoring | Full Statistic | Create task for Loader  
 Update Bot | VIRTEST | Plugins | FTP backconnect  
 SOCKS 5 | RDP | Settings

912 G098

**GEO info**

Flag	Country	Online Bots / All Bots	Detail State
	Argentina	(2/ 27)	
	Aruba	(0/ 1)	
	Australia	(0/ 6)	
	Austria	(87/ 507)	
	Belarus	(1/ 2)	
	Belgium	(17/ 44)	
	Bosnia and Herzegovina	(1/ 2)	
	Brazil	(0/ 1)	
	Bulgaria	(0/ 3)	
	Canada	(0/ 6)	
	Chile	(2/ 50)	
	China	(1/ 1)	
	Colombia	(0/ 21)	
	Croatia	(0/ 1)	
	Czech Republic	(2/ 12)	
	Denmark	(1/ 4)	
	Ecuador	(2/ 35)	
	Egypt	(0/ 2)	
	Estonia	(1/ 2)	
	France	(7/ 31)	
	Germany	(441/ 3023)	
	Greece	(1/ 5)	
	Guatemala	(0/ 4)	
	Hungary	(2/ 6)	
	Iceland	(1/ 1)	
	India	(5/ 10)	
	Indonesia	(0/ 1)	
	Iran, Islamic Republic of	(1/ 9)	
	Ireland	(0/ 4)	
	Israel	(1/ 4)	
	Italy	(7/ 93)	

# Starptautiskā sadarbība – uzbrukums Azerbaidžānai

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
<b>Re: [1st-t] Attack!!! Urgent HELP needed!!!</b>	<b>Chad Greene</b>	<b>02:22 AM</b>
<b>Re: [1st-t] Attack!!! Urgent HELP needed!!!</b>	<b>mizamil</b>	<b>06:13 AM</b>
<b>Re: [1st-t] Attack!!! Urgent HELP needed!!!</b>	<b>Khalifa Al Shamsi</b>	<b>08:15 AM</b>
<b>Re: [1st-t] Attack!!! Urgent HELP needed!!!</b>	<b>Rohana Palliyaguru</b>	<b>08:56 AM</b>

from CERT.GOV.AZ <first-team@cert.gov.az>  
 subject **[1st-t] Attack!!! Urgent HELP needed!!!**  
 to 'FIRST Secretariat' <first-sec@first.org>  
 cc first-teams@first.org

04/22/2012  
 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

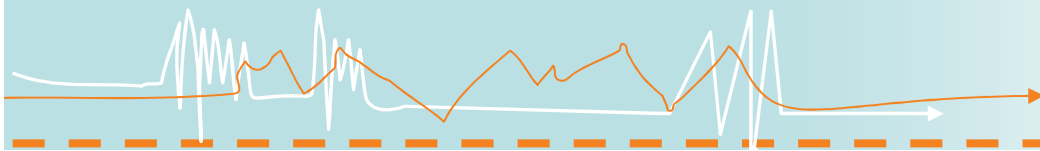
During this attack the following proxy servers were used:

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

# Draudi

- Politiskās situācijas saasinājumi
- Mērķētie uzbrukumi
- Ļaunatūras izplatīšana no uzlauztajām lapām
- Pikšķerēšanas u.c. uzbrukumu ticamības palielināšanās



**CERT.LV**

**Nākotne**



## Turpmākie darbi

- Informācijas tehnoloģiju drošības attīstības stratēģijas projekts
- Informatīvā ziņojuma projekts par Krimināllikumā un Latvijas Administratīvo pārkāpumu kodeksā ietvertā tiesiskā regulējuma pietiekamību attiecībā uz nodarījumiem, kas pastrādāti elektroniskās informācijas telpā un pret informācijas tehnoloģijām
- Saprāšanās memorandu projekti ar starptautiskajām organizācijām un citām valstīm
- Brīvprātīgo informācijas tehnoloģiju speciālistu iesaistīšana

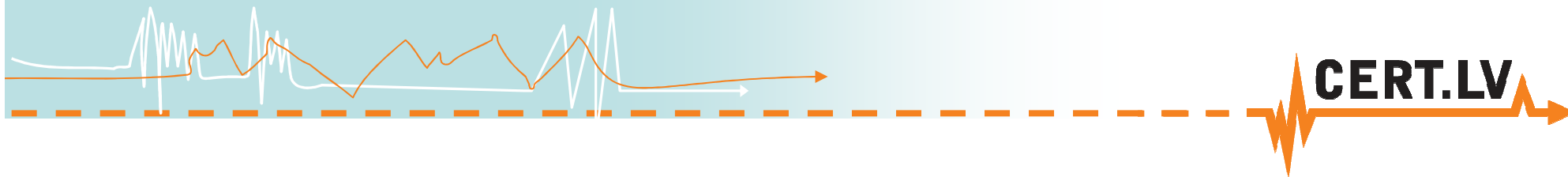
## Nākotne (1)

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

## Nākotne (2)

- Pakļautības maiņa – turpmāk Aizsardzības ministrija
- Svarīgi turpināt visu iesākto un nemainīt galvenos principus





**Paldies par uzmanību!**

**<http://www.cert.lv/>  
[cert@cert.lv](mailto:cert@cert.lv)**

