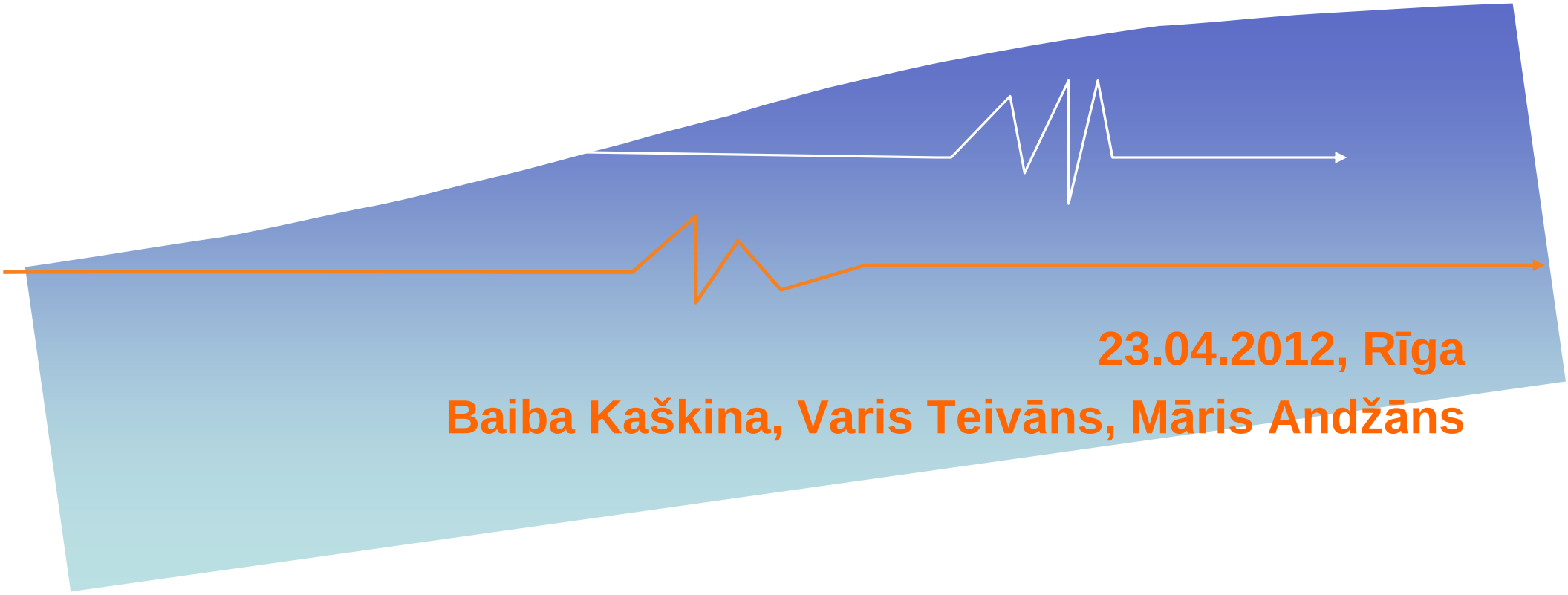
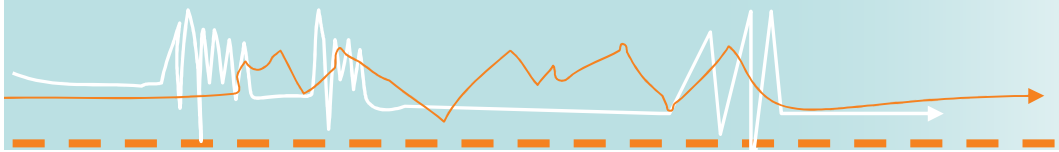
CERT.LV

Situācija IT drošības jomā Latvijā



23.04.2012, Rīga

Baiba Kaškina, Varis Teivāns, Māris Andžāns



CERT.LV

Par CERT.LV

CERT.LV

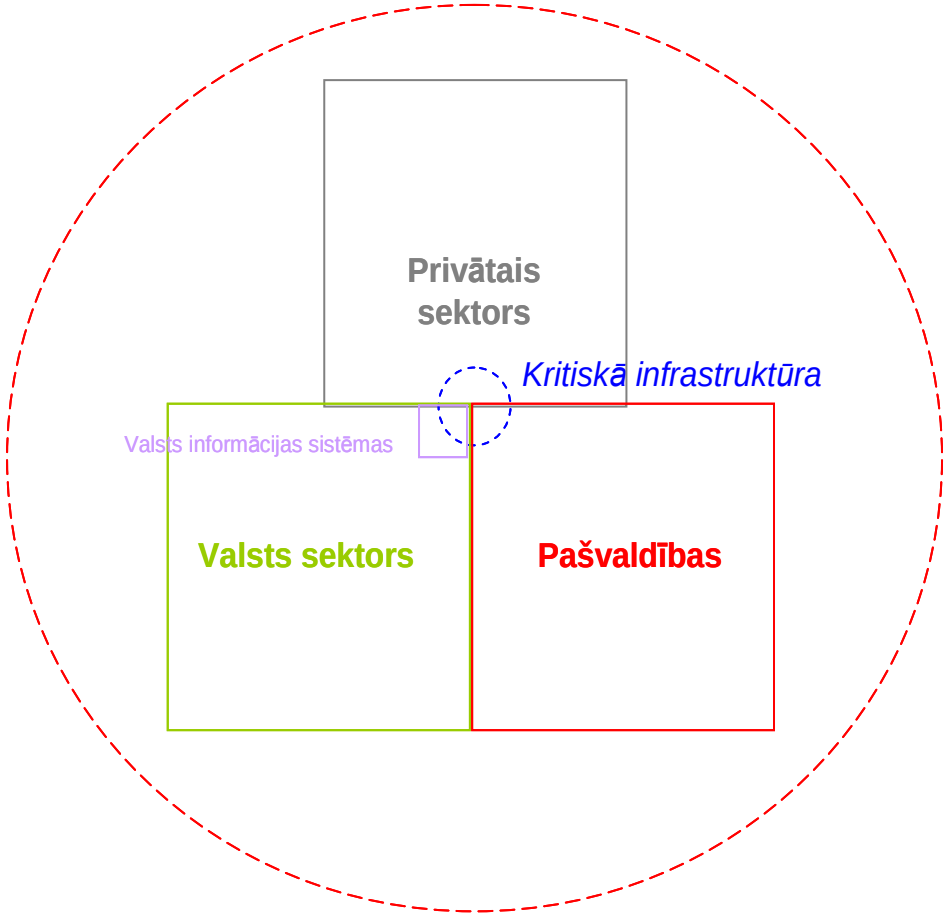
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Misija: “Veicināt IT drošību Latvijā”

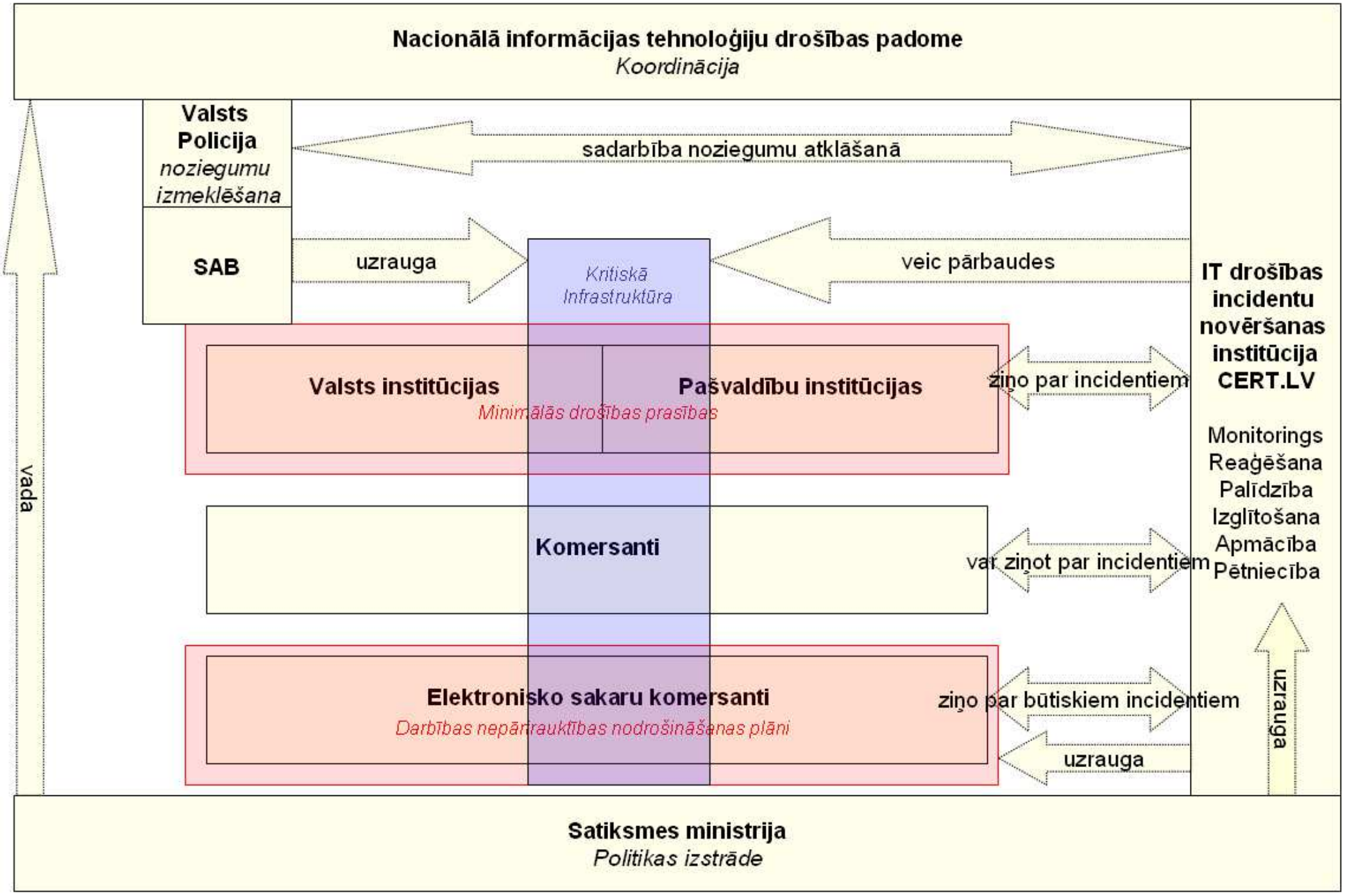
CERT.LV

- 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 atainojums – būtiskākie elementi

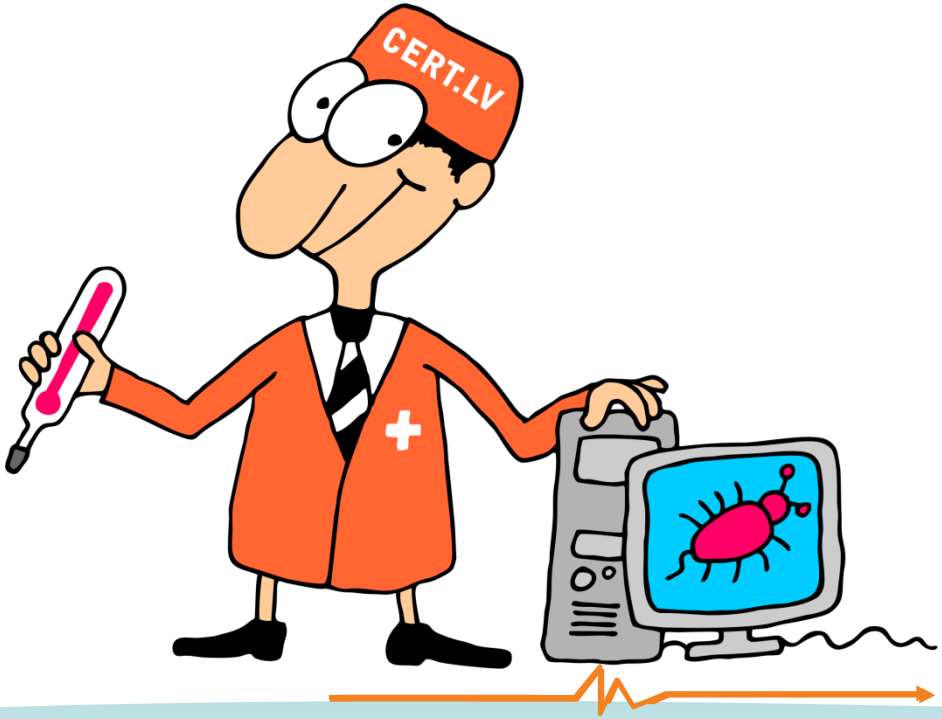


CERT.LV sadarbojas

- 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

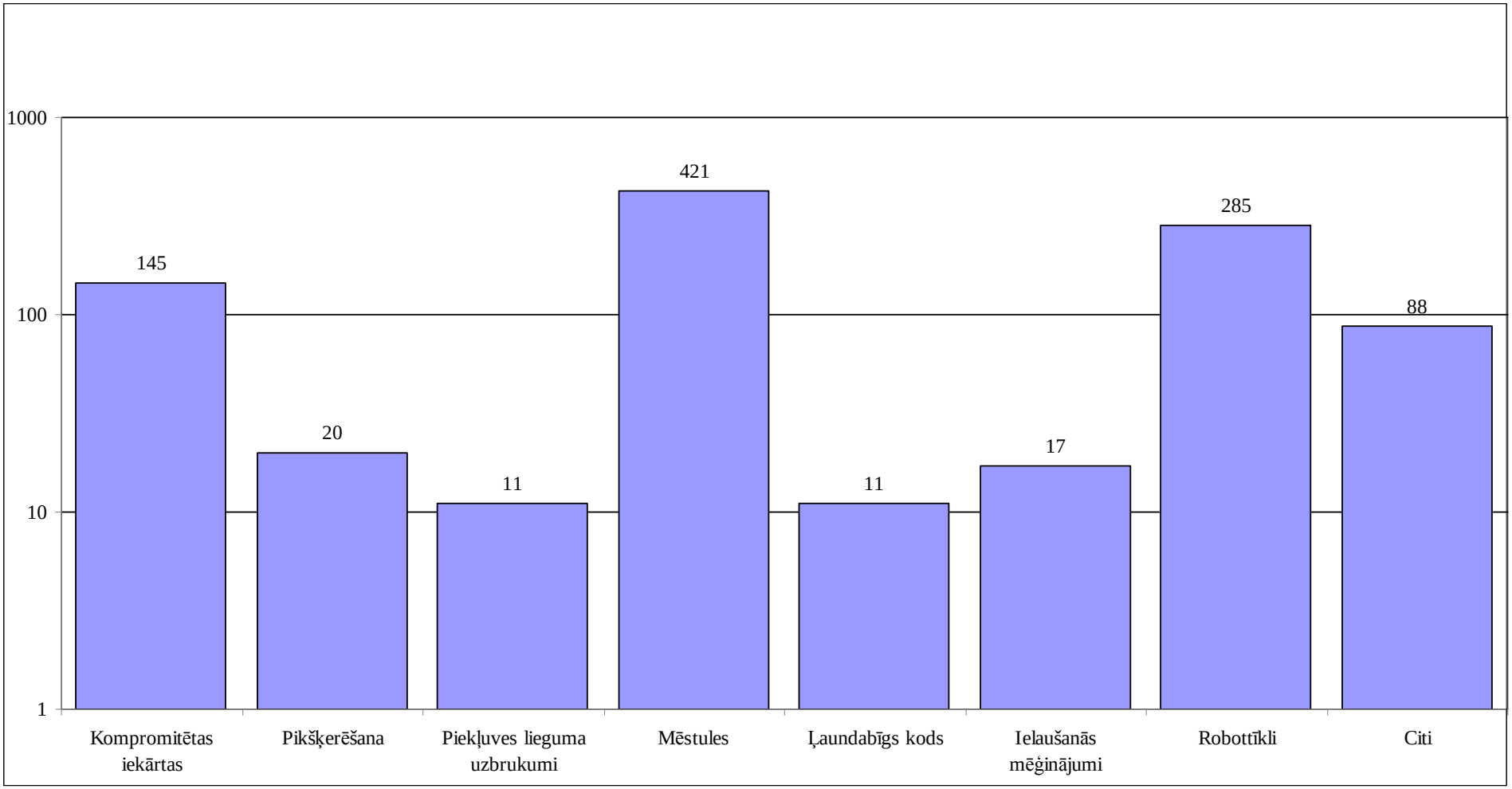


Aktuālā situācija Latvijā

Aktuālā situācija

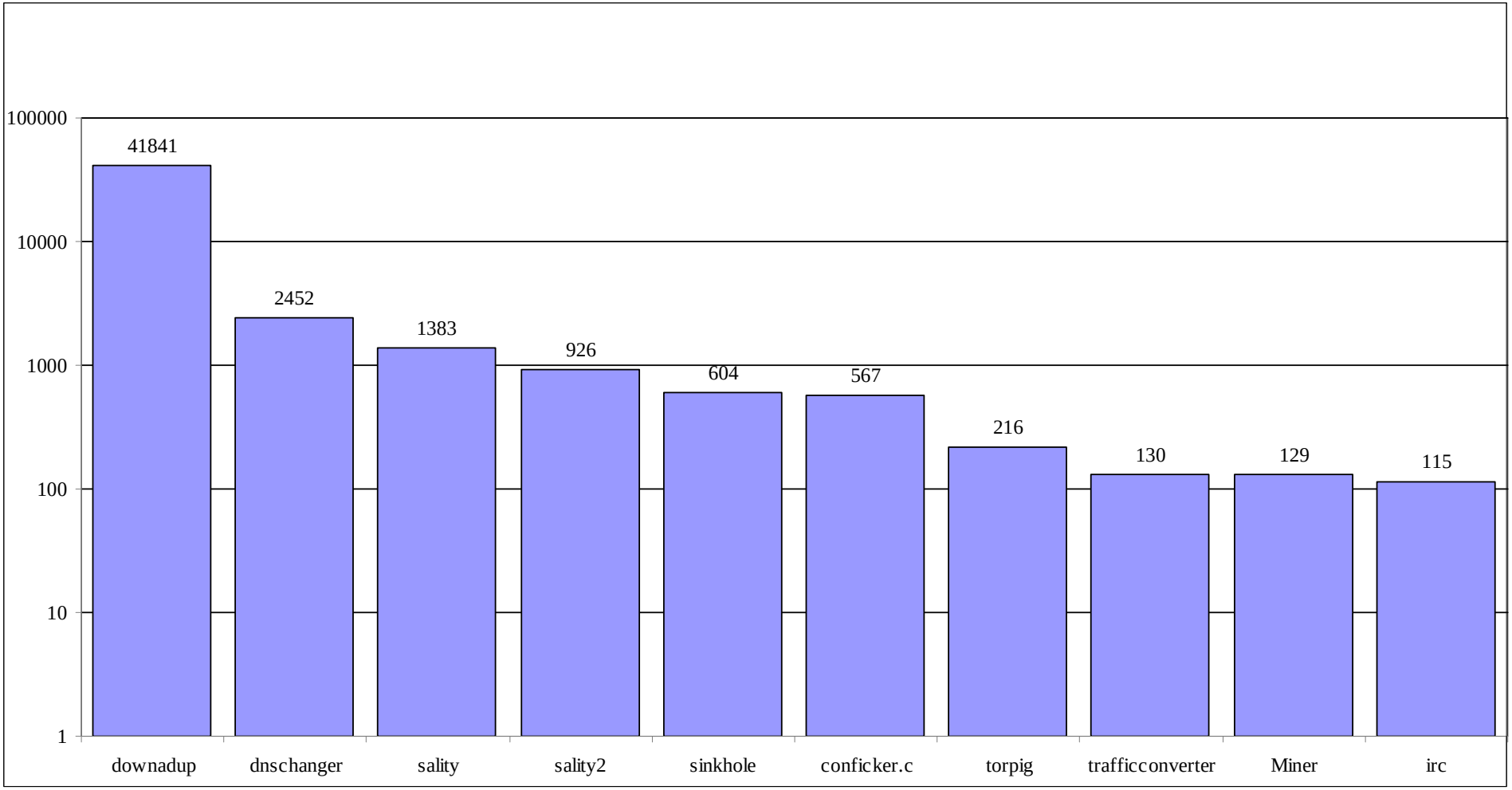
- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS

Augstas prioritātes incidenti – 1.ceturksnis - 998

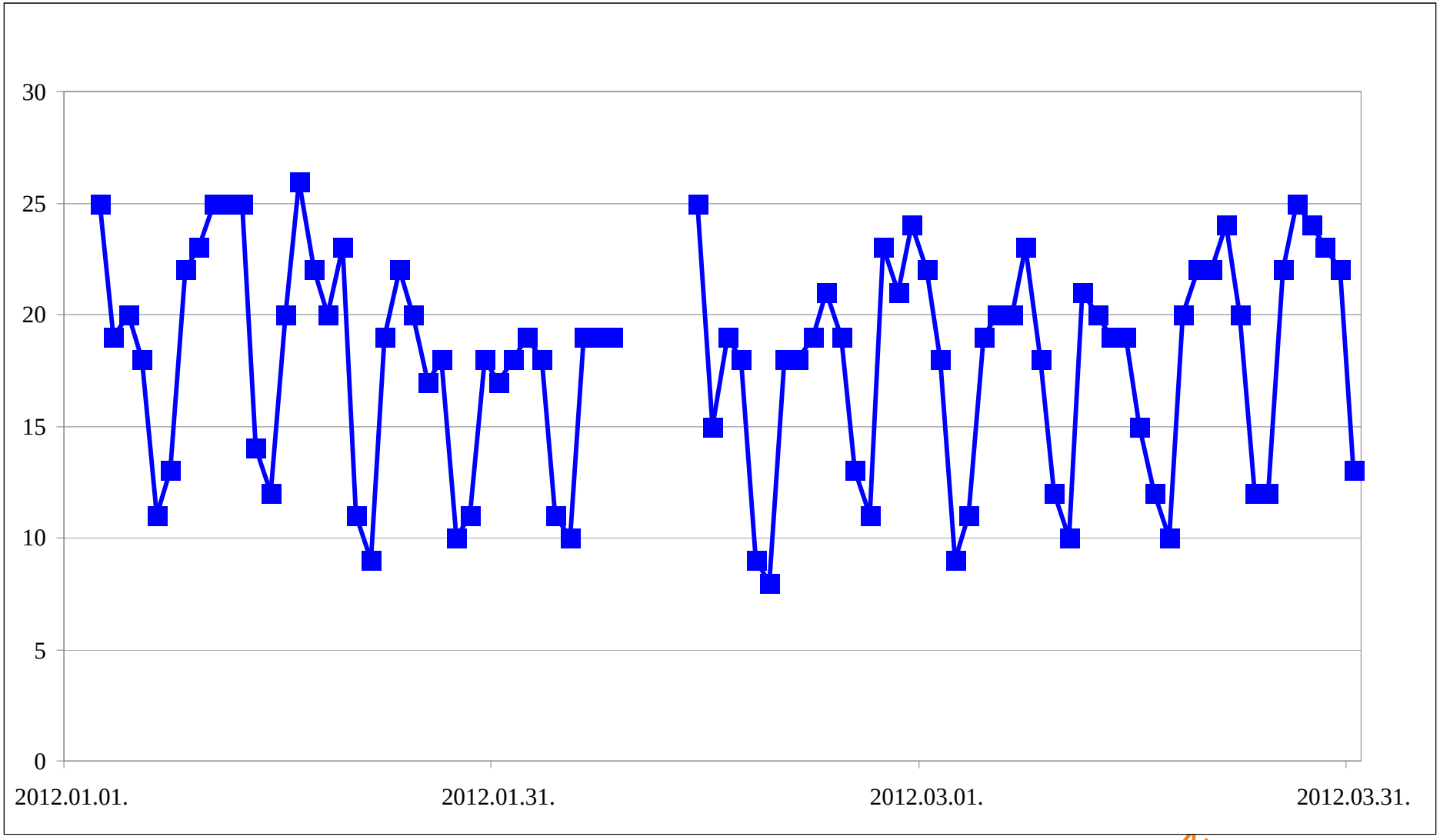


Zemas prioritātes incidenti – 1.ceturksnis – 48841

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 jūtīgos brīžos
- Ļaundabīgās programmatūras izplatīšana

Latvenergo incidents

Latvian Electricity Grid Hacked !! So claims a Chinese Group

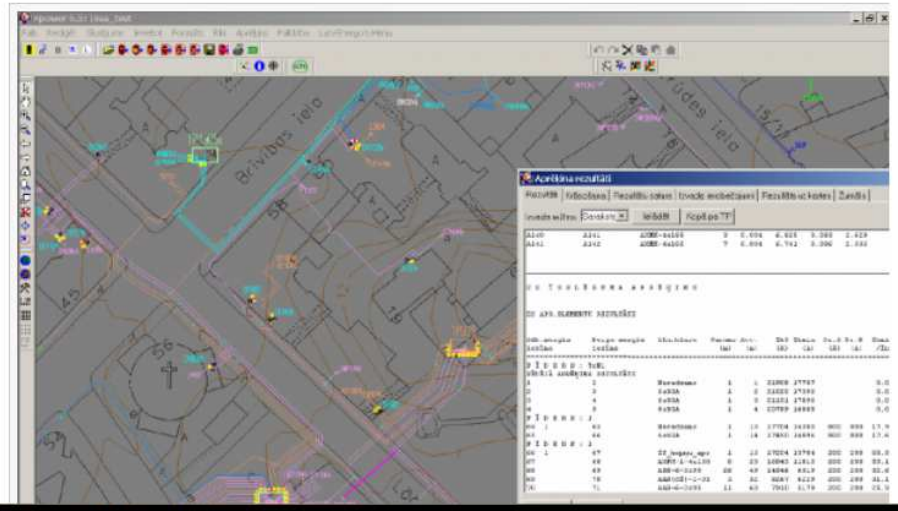
May 4, 2011 CIIP Go to comments Leave a comment

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)

George Mason CIP Reports (Monthly)

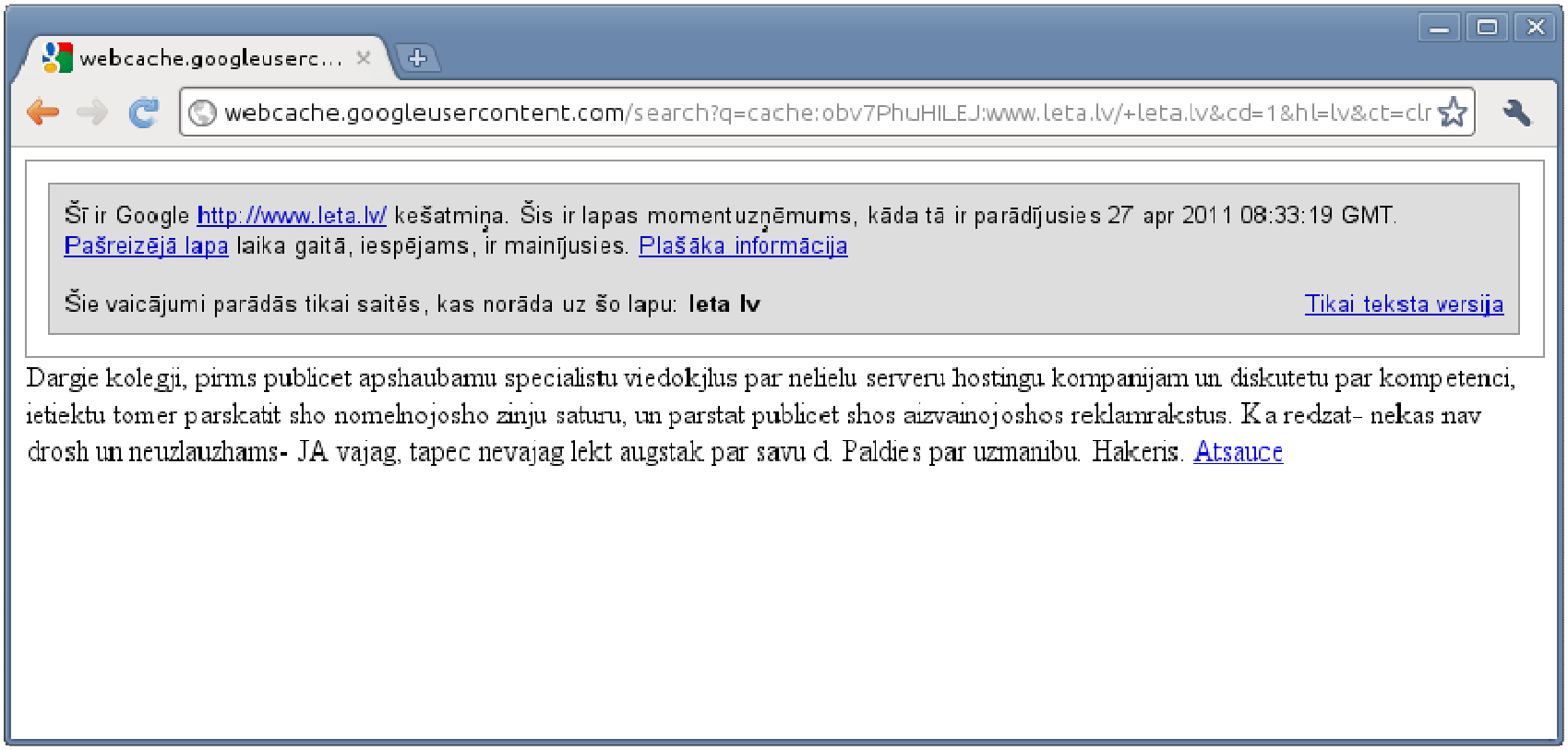
- Invitation to attend X-SCM: The New Science of Extreme Supply Chain Management Conference
- Washington DC's Preeminent Government & Business Continuity Thought Leadership Event is Back!
- The CIP Report: March 2012 - Critical Manufacturing Sector

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

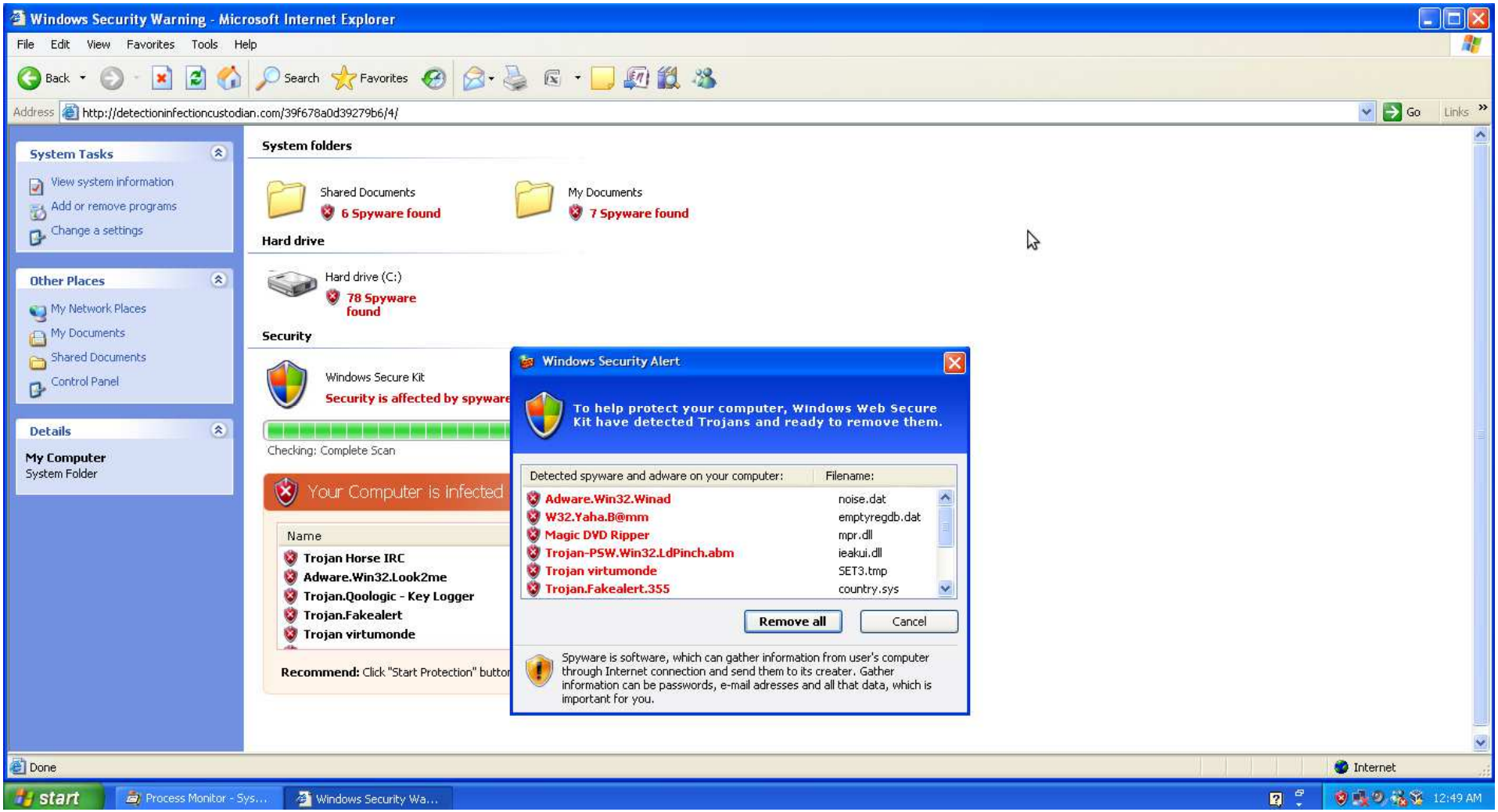


Delfi incidents

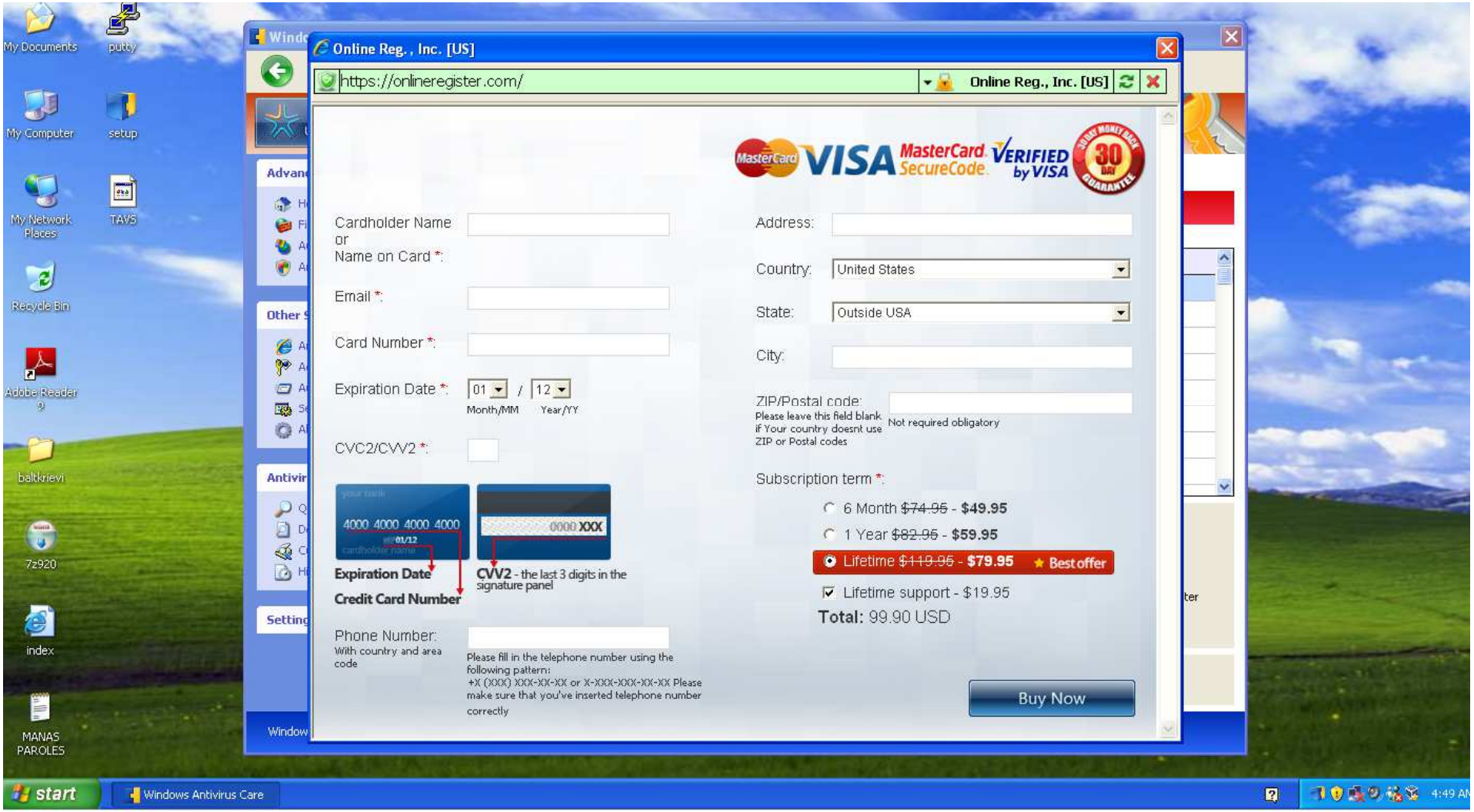
Piektdiena, 20. aprīlis (2012) 19:55

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

Delfi incidents



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
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

nra.lv

Sestdiena, 14.aprīlis
Vārda dienas: Gudrīte, Strauja
+11°C 7 m/s DR uz plkst.14
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.

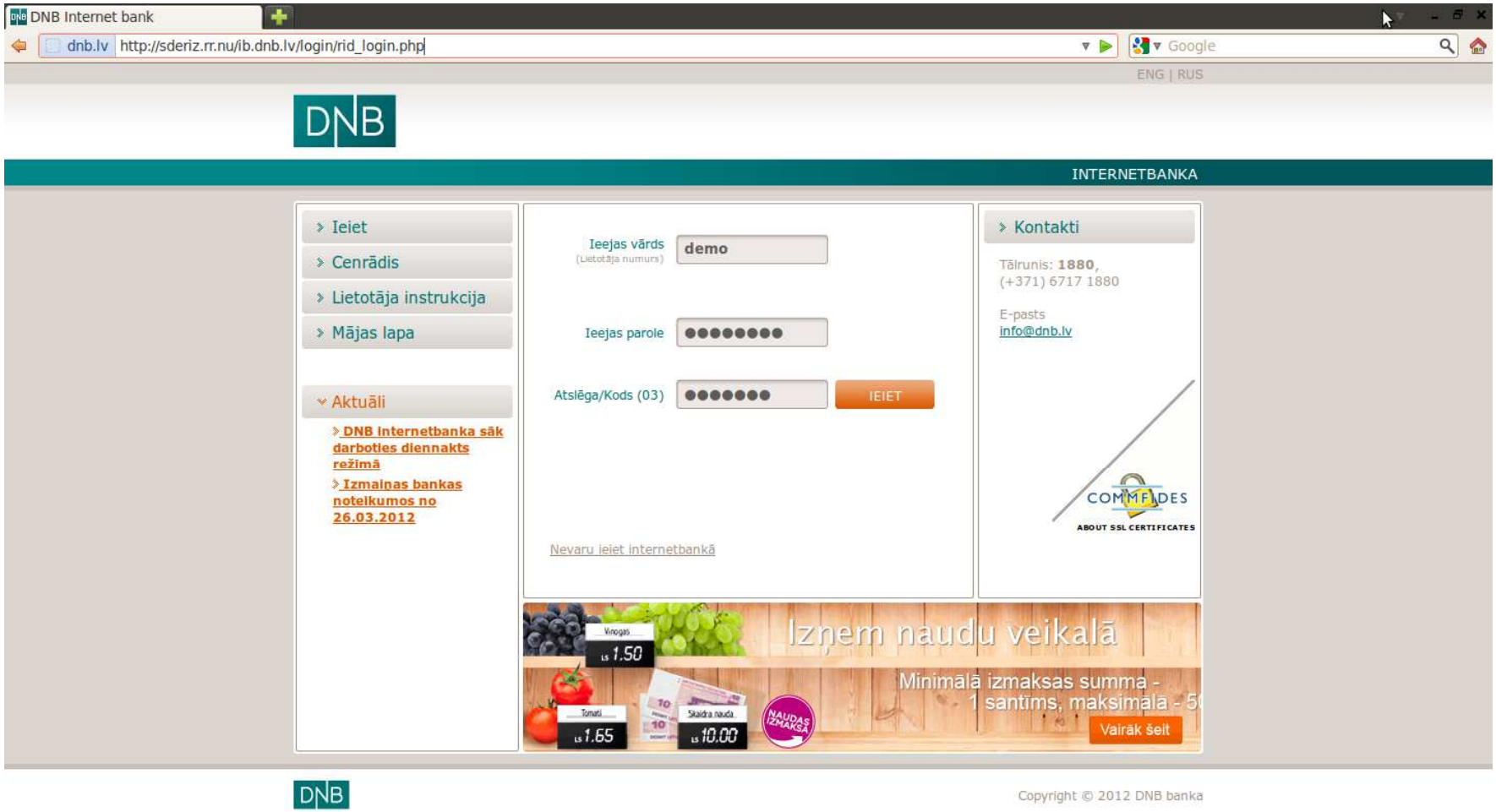
Cilvēkiem izsūtīti viltus e-pasti ar saiti uz interneta vietni, kurā tiek prasīts ievadīt internetbankas lietotāja datus – ieejas vārdu, paroli un kodus. Interneta vietne, uz kuru ved saite no viltus e-pasta, pēc sava vizuālā noformējuma ir ļoti līdzīga īstajai internetbankas iNORD ieejas lapai.

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 vai arī, lietojot tiešo adresi https://www.inord.lv.

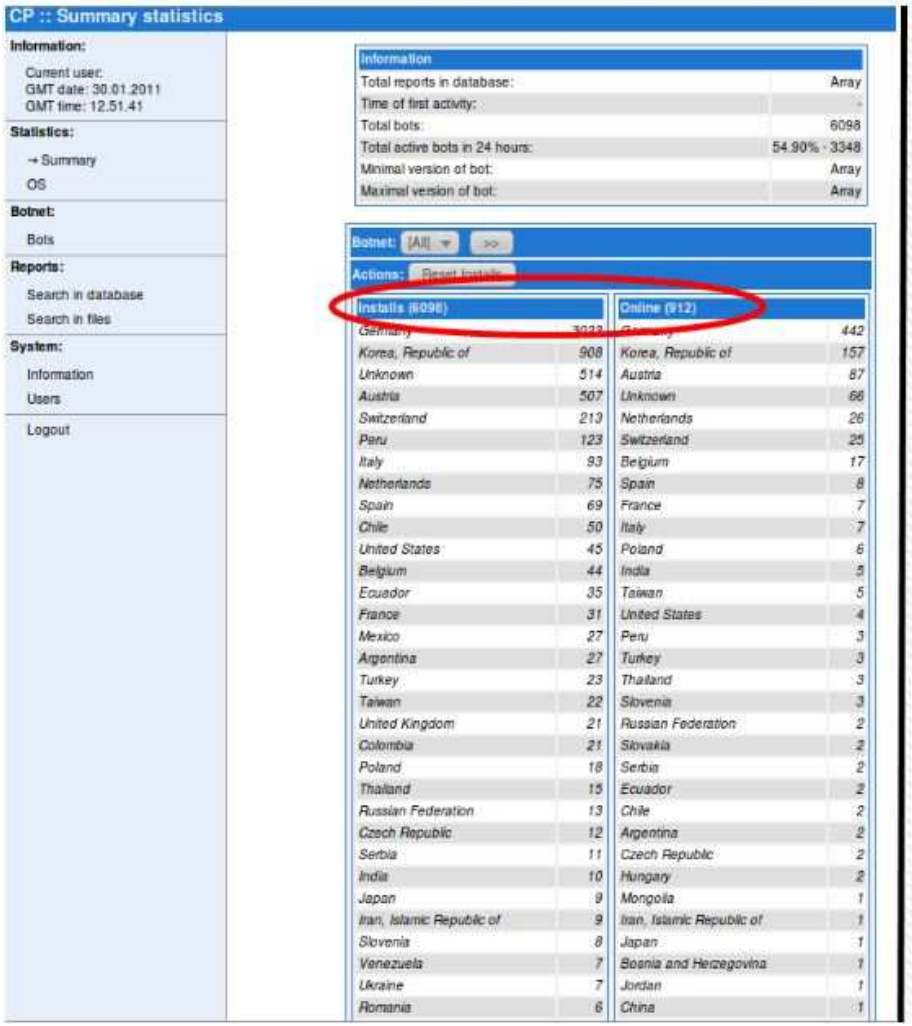
Šis krāpšanas veids pasaulē ir pazīstams ar apzīmējumu „phishing". Krāpnieki, izsūtot šādus e-pastus, mēģina maldināt cilvēkus un ļaunprātīgi izvilināt konfidenciālu informāciju no banku klientiem.

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, tālr. 1880). DnB NORD Banka rūpējas par savu klientu drošību, tādēļ jebkura sīkāka informācija par

DNB bankas incidents



Uzbrucēja saskarne – Zeus robotu tīkls



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
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

Draudi

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

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
- Saprašanās 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 jākļūst 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