

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

Par CERT.LV



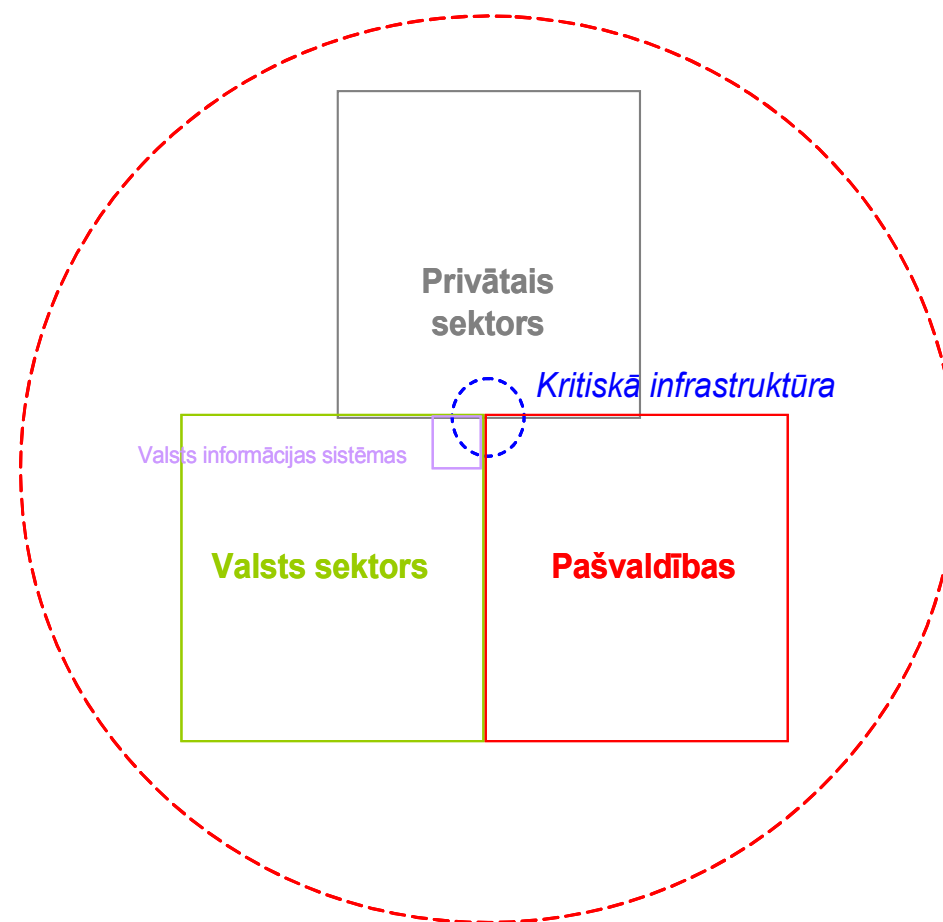
CERT.LV

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

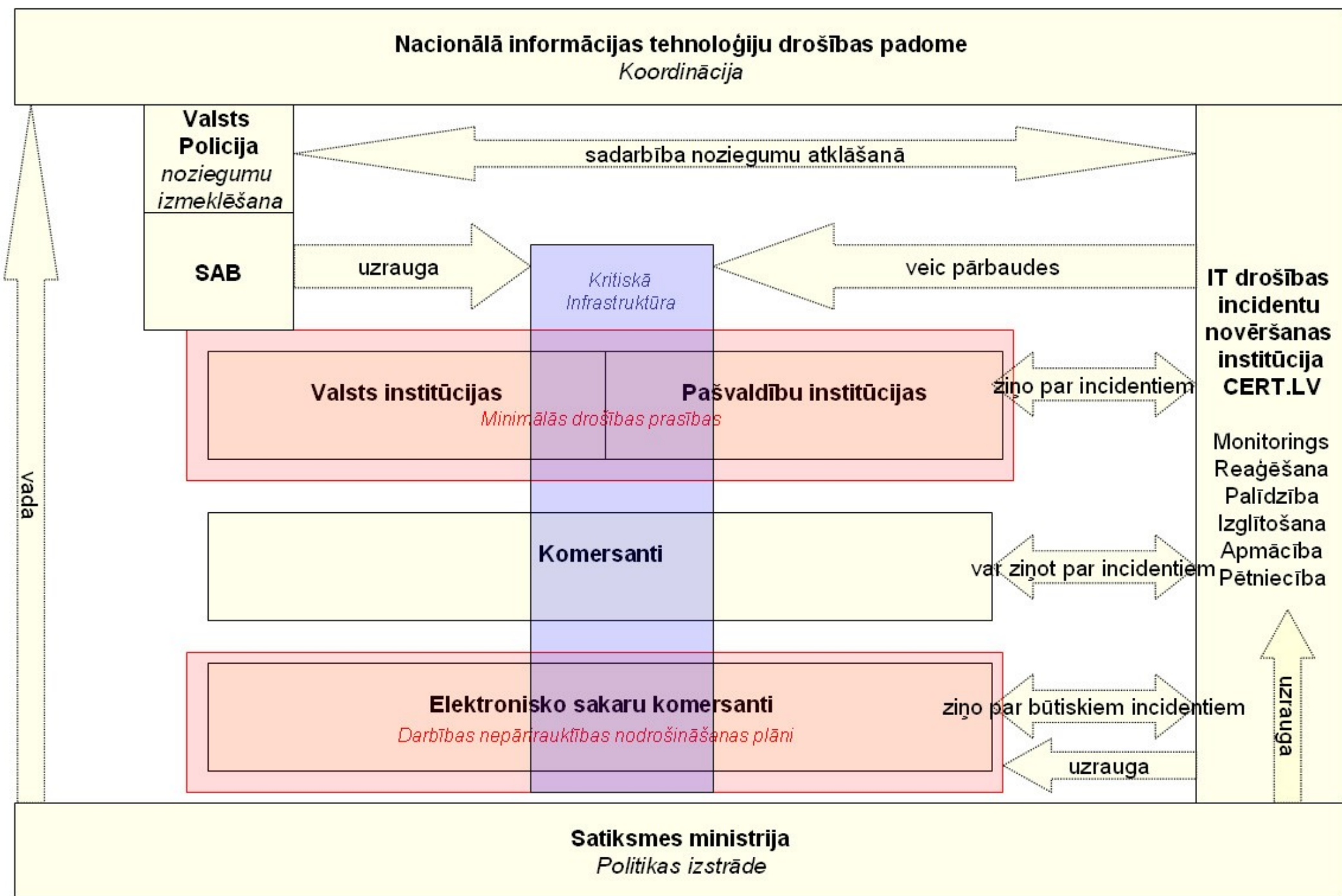
CERT.LV

- 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

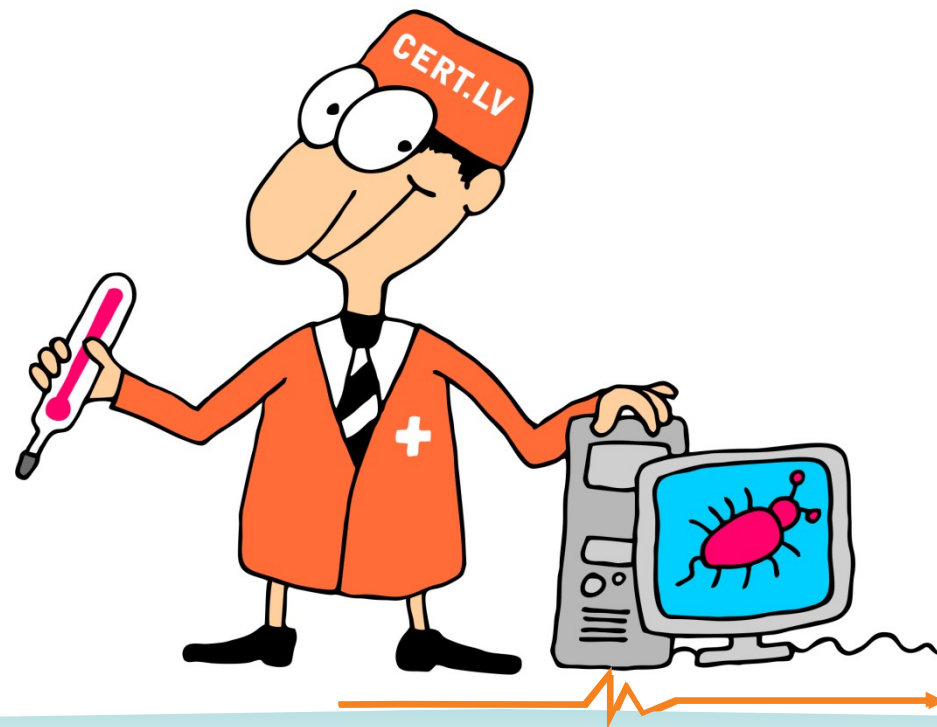


Latvijas IT drošības sistēmas atainojums – būtiskākie elementi



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)



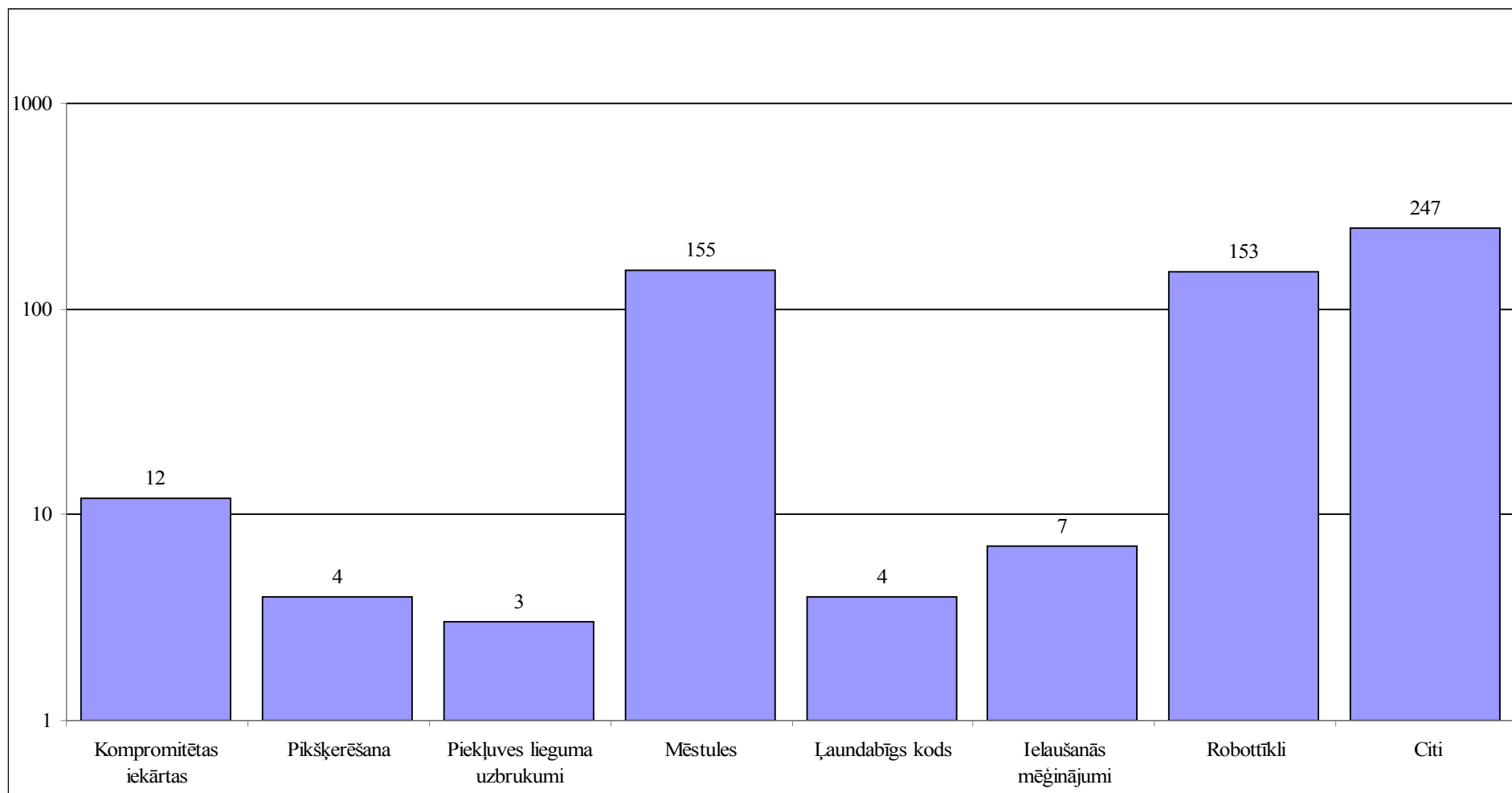
Mūsdienu pasaule 60 sekundēs (2)



Aktuālā situācija

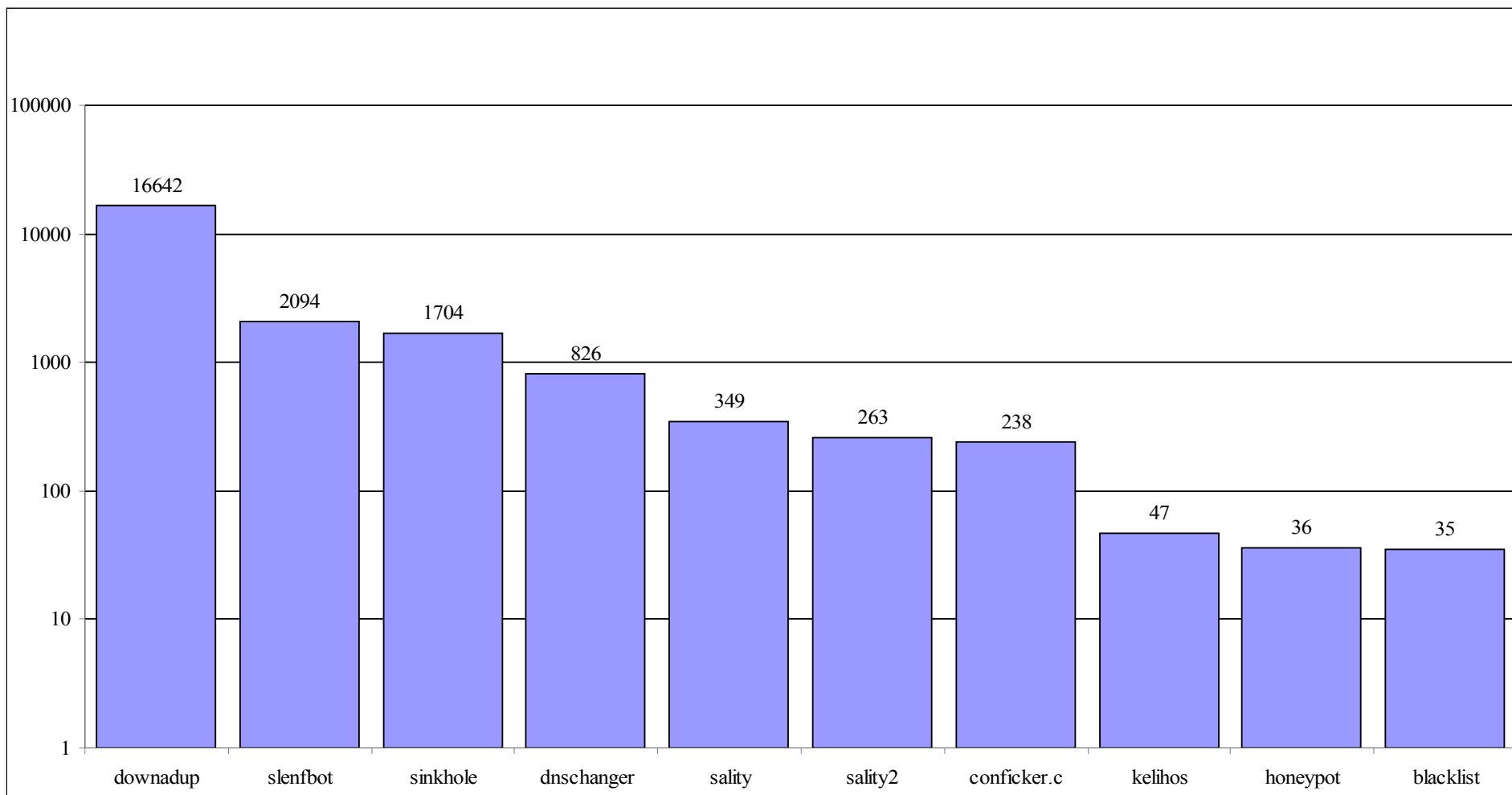
- Milzīgs skaits incidentu ziņojumu katru dienu
- Augstas un zemas prioritātes incidenti
- Sadarbība ar IPS
 - “Kvalitātes zīme” – kopā ar LIA
 - Lattelecom, Latnet Serviss, LMT, Baltkom, IZZI, Telia, Ilva, CSDD, Telecentrs

Augstas prioritātes incidenti – aprīlis 2012 - 585

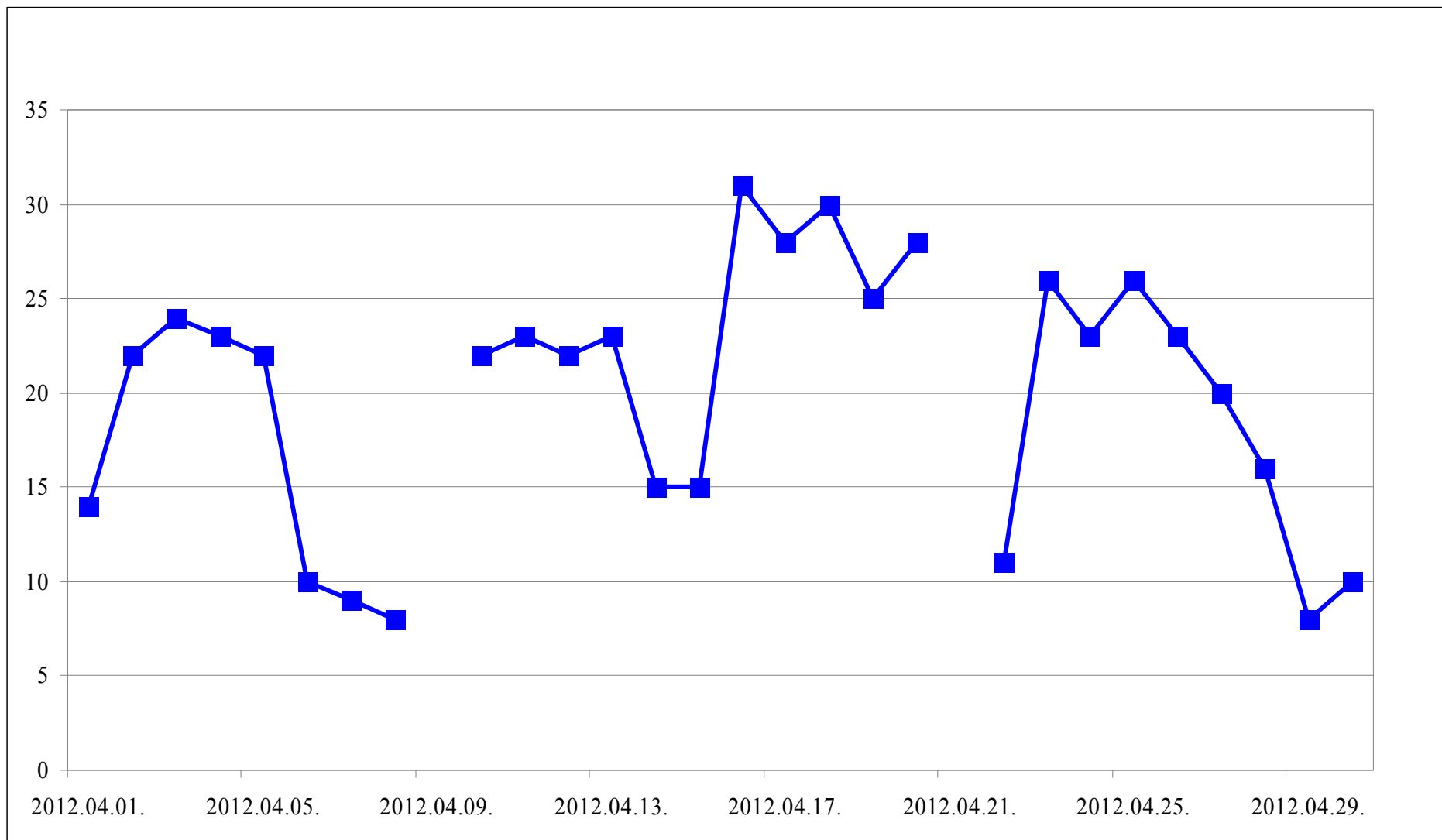


Zemas prioritātes incidenti – aprīlis 2012 – 22457

Infekciju TOP10



Inficētās IP adreses Valsts & pašvaldību iestādēs



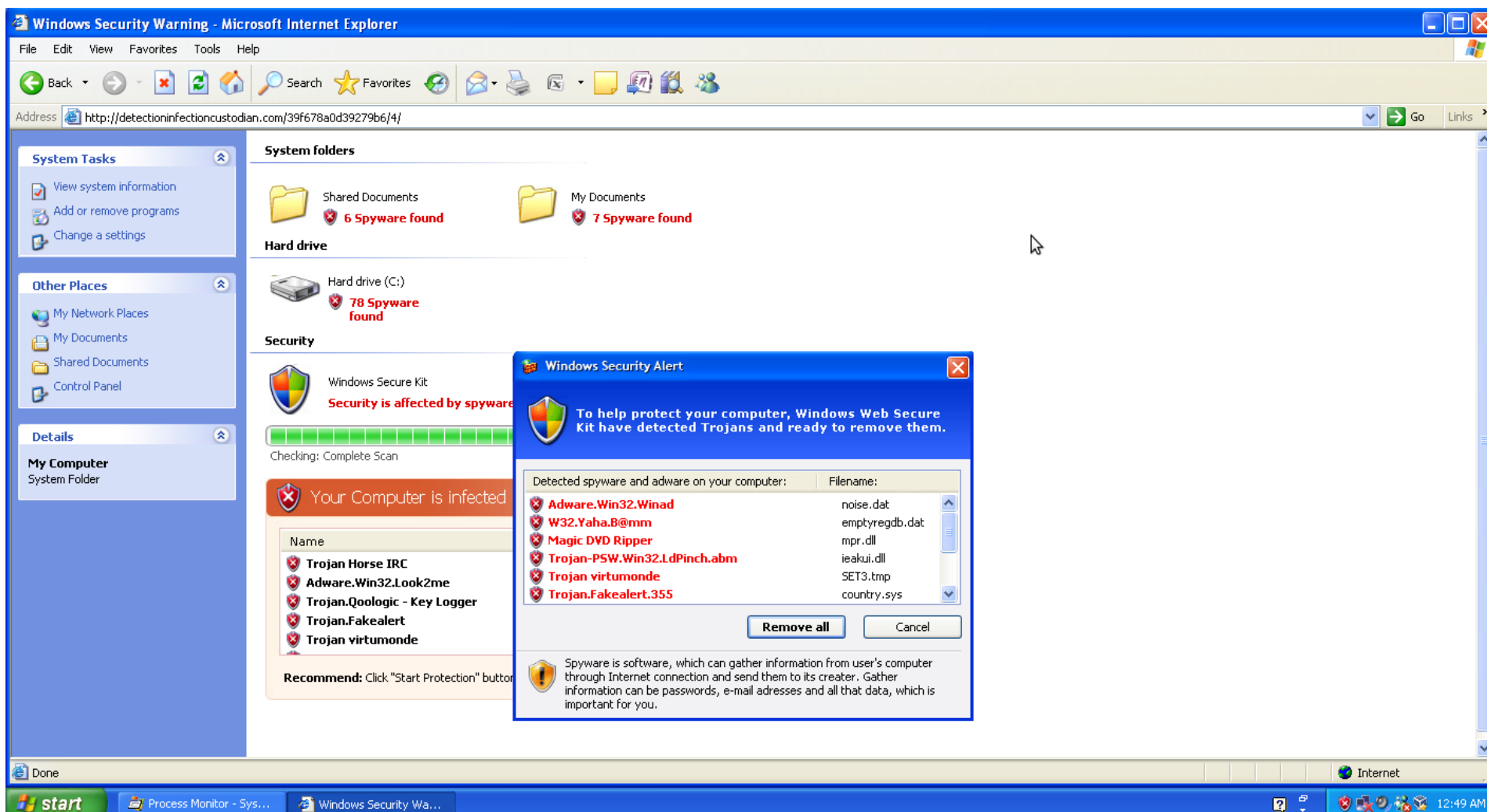
Delfi incident

Piektdiena, 20. aprīlis (2012) 19:55

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



Delfi incident



The screenshot shows a Windows XP desktop with a Microsoft Internet Explorer browser window open. The browser address bar shows a URL from a detection site. The Windows Security Center interface is visible, indicating that the system is infected with spyware. A 'Windows Security Alert' dialog box is open, displaying a list of detected threats and their filenames.

Windows Security Alert

To help protect your computer, Windows Web Security Kit have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
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

Buttons: Remove all, Cancel

Recommend: Click "Start Protection" button

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

Your Computer is infected

- Trojan Horse IRC
- Adware.Win32.Look2me
- Trojan.Qoollogic - Key Logger
- Trojan.Fakealert
- Trojan virtumonde

Delfi incident

The screenshot shows a Windows XP desktop environment. The desktop background is a green landscape with a blue sky. The taskbar at the bottom shows the Start button, Windows Antivirus Care, and the system tray with the time 4:49 AM. A web browser window titled "Online Reg., Inc. [US]" is open, displaying a credit card registration form. The browser's address bar shows "https://onlineregister.com/". The form includes the following fields and options:

- Cardholder Name or Name on Card *:** Text input field.
- Address:** Text input field.
- Country:** Dropdown menu with "United States" selected.
- State:** Dropdown menu with "Outside USA" selected.
- City:** Text input field.
- Card Number *:** Text input field.
- Expiration Date *:** Two dropdown menus for "Month/MM" (01) and "Year/YY" (12).
- CVC2/CVV2 *:** Text input field.
- Phone Number:** Text input field with instructions: "With country and area code. Please fill in the telephone number using the following pattern: +X (XXX) XXX-XX-XX or X-XXX-XXX-XX-XX. Please make sure that you've inserted telephone number correctly."
- Subscription term *:** Radio button options: "6 Month \$74.95 - \$49.95", "1 Year \$82.95 - \$59.95", and "Lifetime \$119.95 - \$79.95" (marked as "Best offer"). A checkbox for "Lifetime support - \$19.95" is checked.
- Total:** 99.90 USD
- Buy Now:** Button

Logos for MasterCard, VISA, and Verified by VISA are visible at the top of the form. A "30 DAY MONEY BACK GUARANTEE" badge is also present. The desktop icons include My Documents, My Computer, My Network Places, Recycle Bin, Adobe Reader, baltkrievi, 7z920, index, and MANAS PAROLES.

DNB bank incident

The screenshot shows the DNB Internet bank login interface. The browser address bar displays the URL `http://sderiz.rr.nu/ib.dnb.lv/login/rid_login.php`. The page features the DNB logo and a navigation menu on the left with options like 'Ieiet', 'Cenrādis', and 'Lietotāja instrukcija'. The central login area contains fields for 'Ieejas vārds' (username: 'demo'), 'Ieejas parole' (password), and 'Atslēga/Kods (03)' (security code), with an 'IEIET' button. A 'Kontakti' sidebar on the right provides contact information. A 'COMFIDES' SSL certificate logo is visible. At the bottom, a promotional banner for 'Izņem naudu veikalā' (Withdraw cash in-store) is shown with product prices and a 'Vairāk šeit' button. The footer includes the DNB logo and the text 'Copyright © 2012 DNB banka'.

DNB Internet bank

dnb.lv http://sderiz.rr.nu/ib.dnb.lv/login/rid_login.php

Google

ENG | RUS

DNB

INTERNETBANKA

> Ieiet

> Cenrādis

> Lietotāja instrukcija

> Mājas lapa

▼ Aktuāli

> **DNB Internetbanka sāk darboties diennakts režīmā**

> **Izmaiņas bankas noteikumos no 26.03.2012**

Ieejas vārds (Lietotāja numurs)

Ieejas parole

Atslēga/Kods (03)

> Kontakti

Tālrunis: **1880**,
(+371) 6717 1880

E-pasts
info@dnb.lv

COMFIDES
ABOUT SSL CERTIFICATES

Nevaru ieiet internetbankā

Izņem naudu veikalā

Minimālā izmaksas summa - 1 santims, maksimālā - 5

Vairāk šeit

DNB

Copyright © 2012 DNB banka

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

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☆

reply reply list forward archive junk

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

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: [Reset Install](#)

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 8
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 06:51:49

Tasks Statistic | Bots Monitoring | Full Statistic | Create task for Loader

Update Bot | VIRTEST | Plugins | FTP backconnect

SOCKS 5 | RDP | Settings

912 6098

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)	

Draudi

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

Padomi un palīdzība



CERT.LV piedāvā

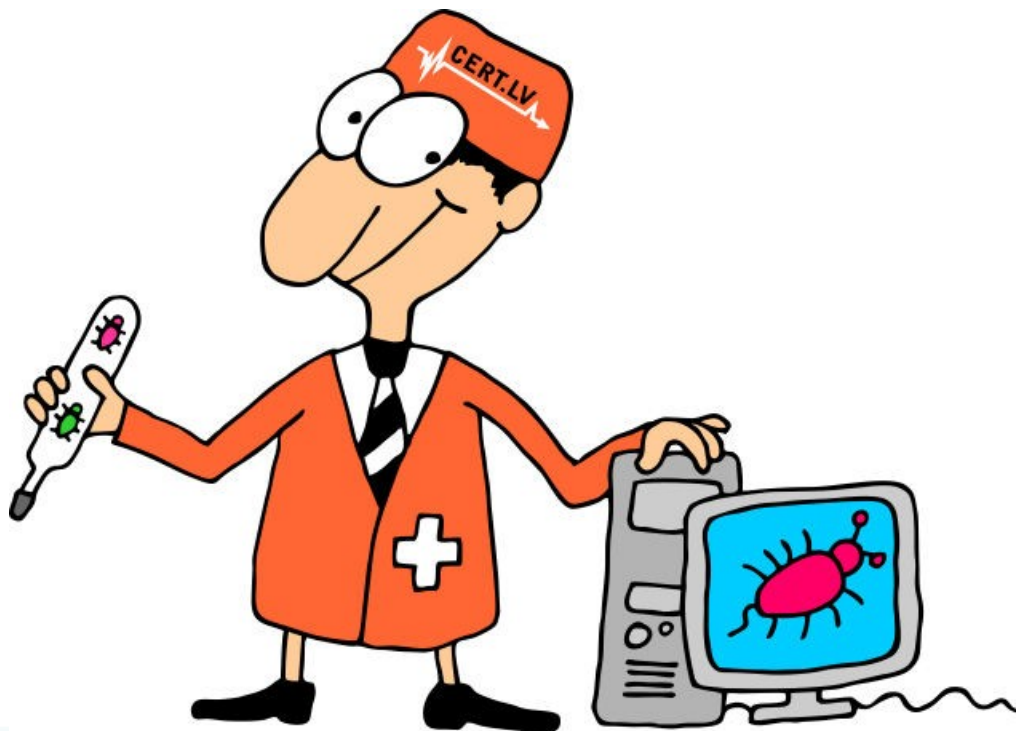
- Palīdzību incidentu risināšanā
- Piemēru darbinieku apmācības programmai
- Piemērus IT drošības dokumentiem
- Informāciju par inficētām IP adresēm un incidentiem
- Reģionālos seminārus

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 kots @datorologs



E-prasmju nedēļa – 2012.gada marts



ES Dārza svētki Vērmaņdārzā 12.maijā





*Mēs atbildam par savu drošību
informācijas tehnoloģiju laikmetā*

Meklēt...



Mājas 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



Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta ikvienam, kurš rūpējas par savu 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 savu datora veselību pie Datorologa!



*Mēs atbildam par savu drošību
informācijas tehnoloģiju laikmetā*

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 lents

- 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 **193.10.10.10** ir inficēts ar datorvīrusu! [Vairāk informācijas.](#)



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 vēlamu 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?

Mirkļi, 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 jāklūst 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