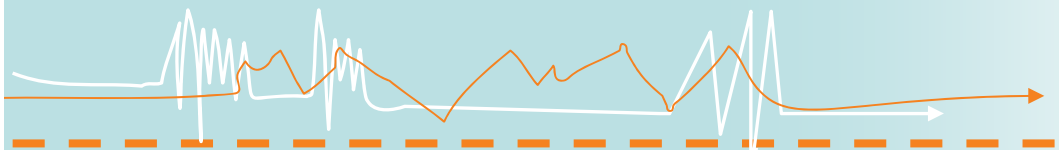
Kas notiek Latvijā – CERT.LV statistikas un jaunākās aktivitātes

ISACA Latvijas nodaļas un CERT.LV konference
8.11.2012, Rīga, LU

Baiba Kaškina, CERT.LV

Saturs

- Par CERT.LV
- Statistikas
- Atbildīgs Interneta pakalpojumu sniedzējs
- Drošības ekspertu grupa
- Padomi un palīdzība
- Nākotne



CERT.LV

Par CERT.LV

CERT.LV

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

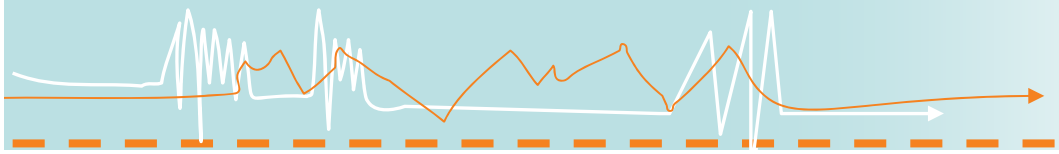
- Misija: “Veicināt IT drošību Latvijā”

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

Kas ir CERT.LV?

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



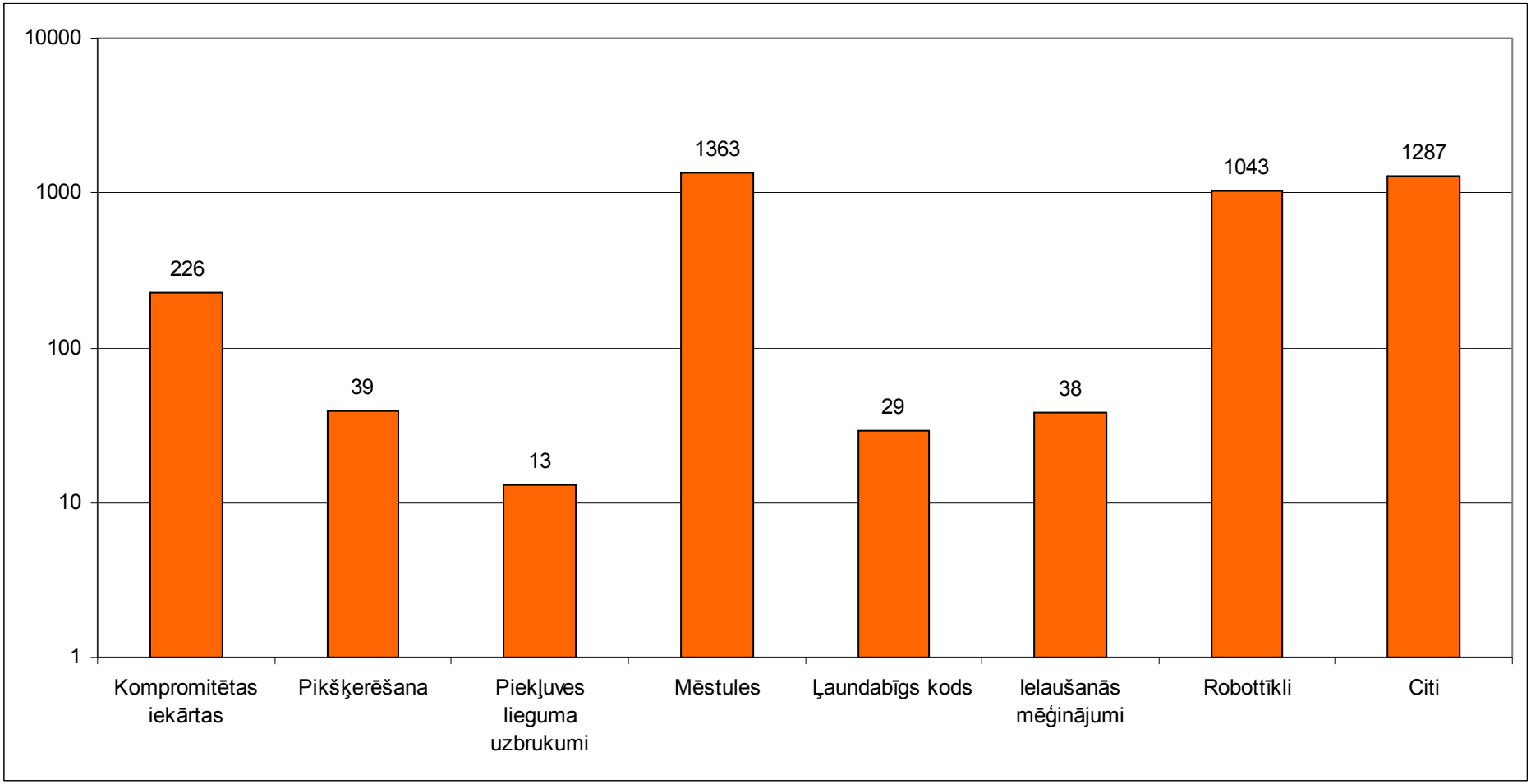
CERT.LV

Statistikas

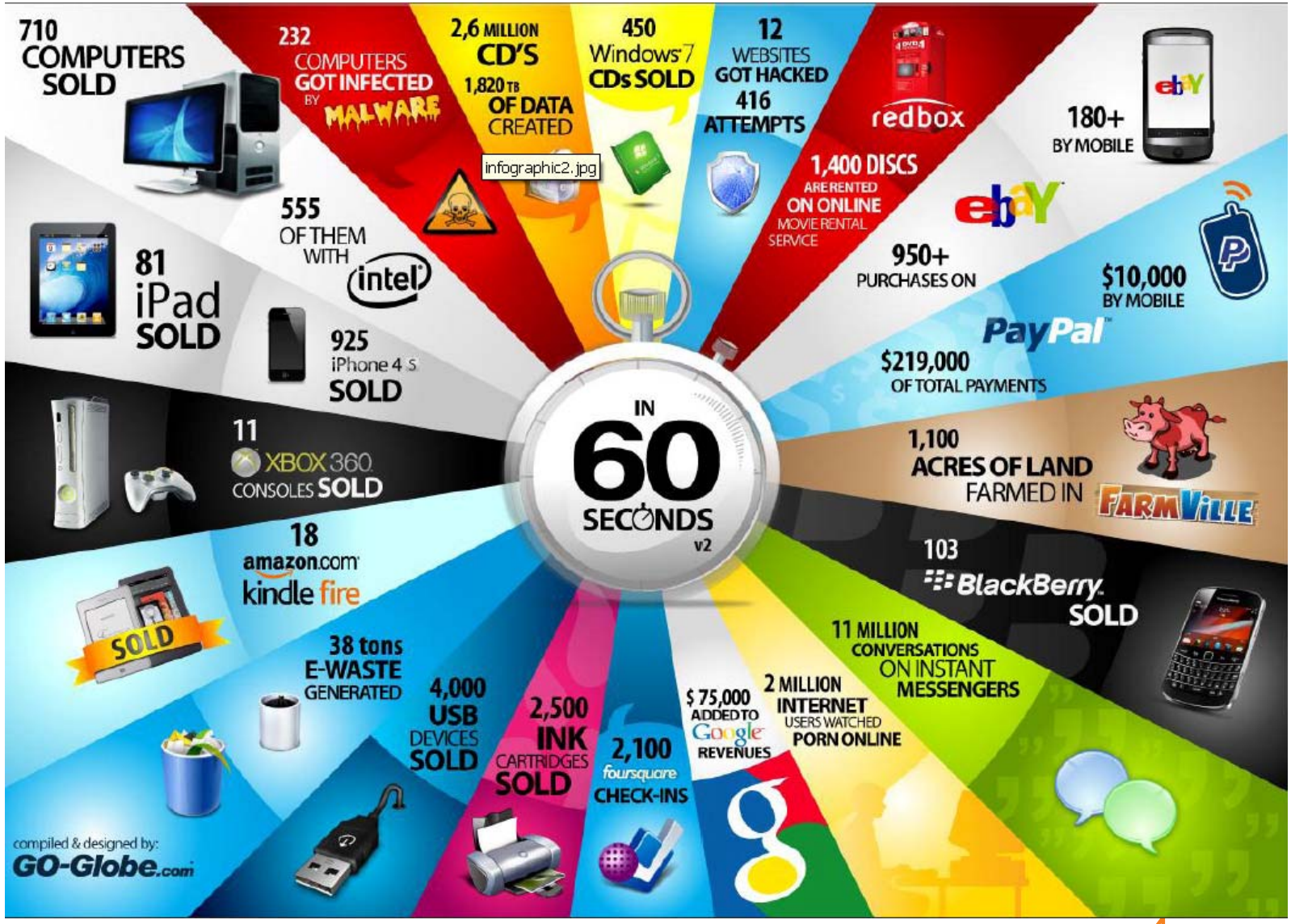
Aktuālā situācija

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

Augstas prioritātes incidenti – 2012.gada janvāris – oktobris - 4039

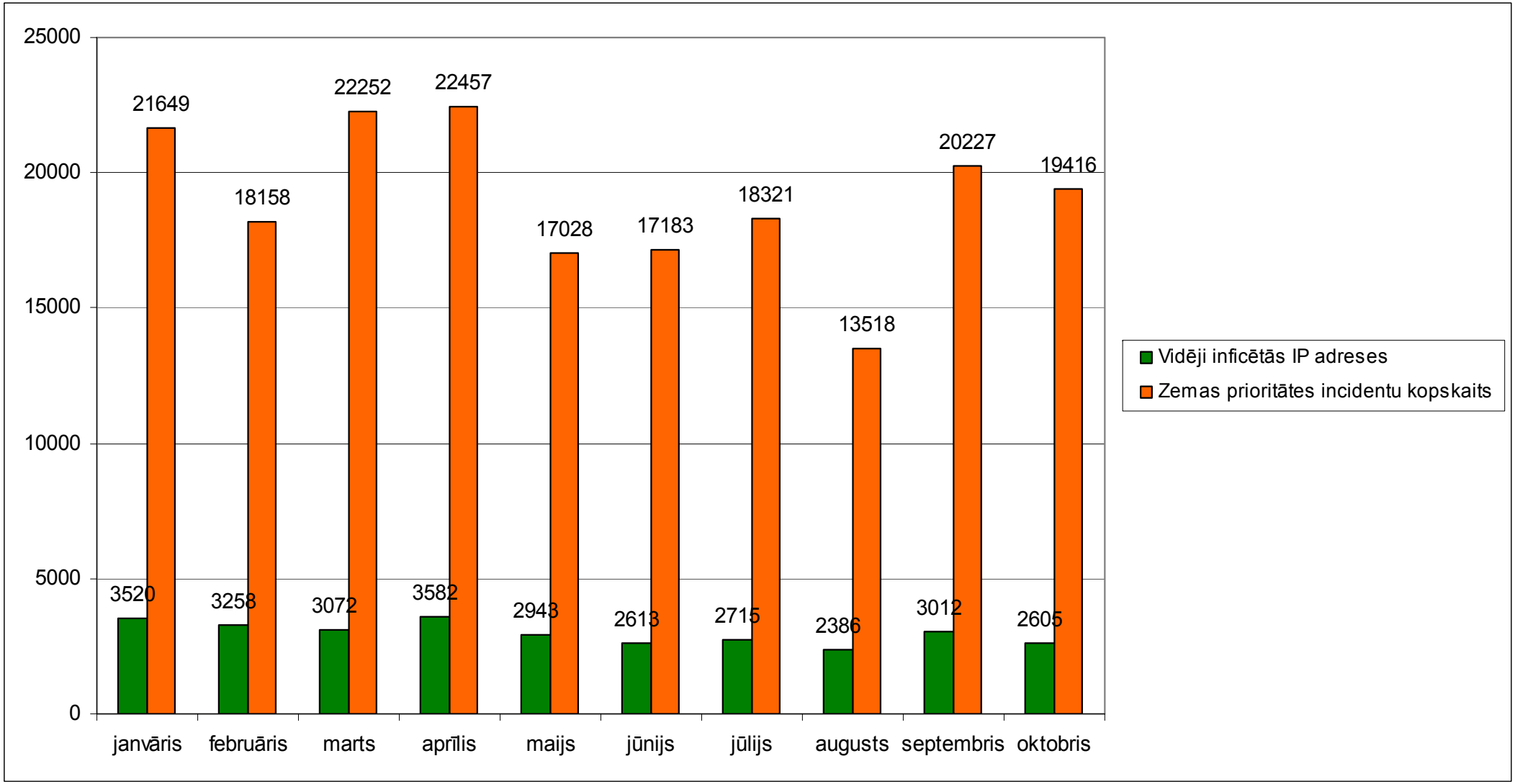


Mūsdienu pasaule 60 sekundēs

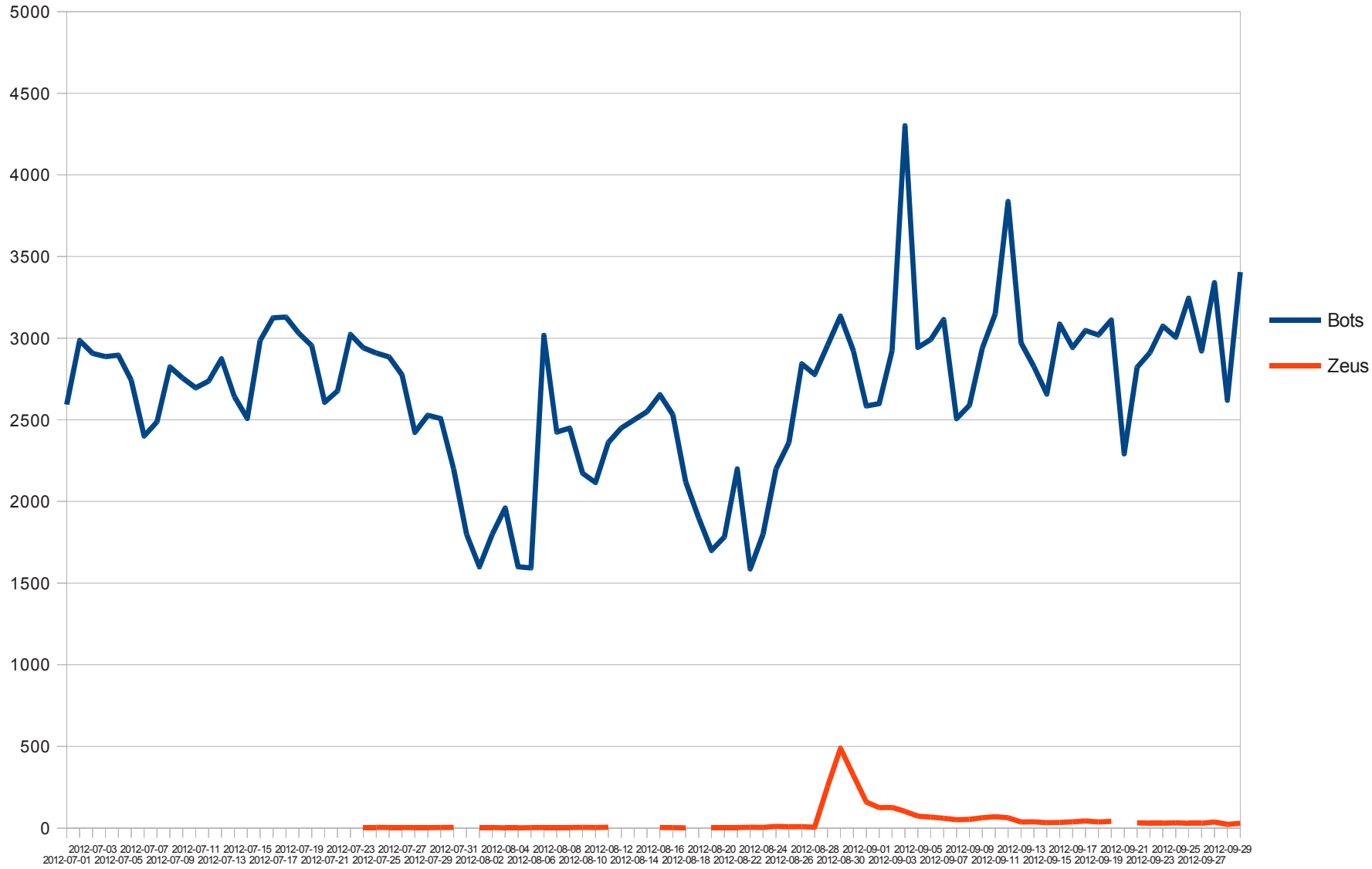


http://www.businessinsider.com/

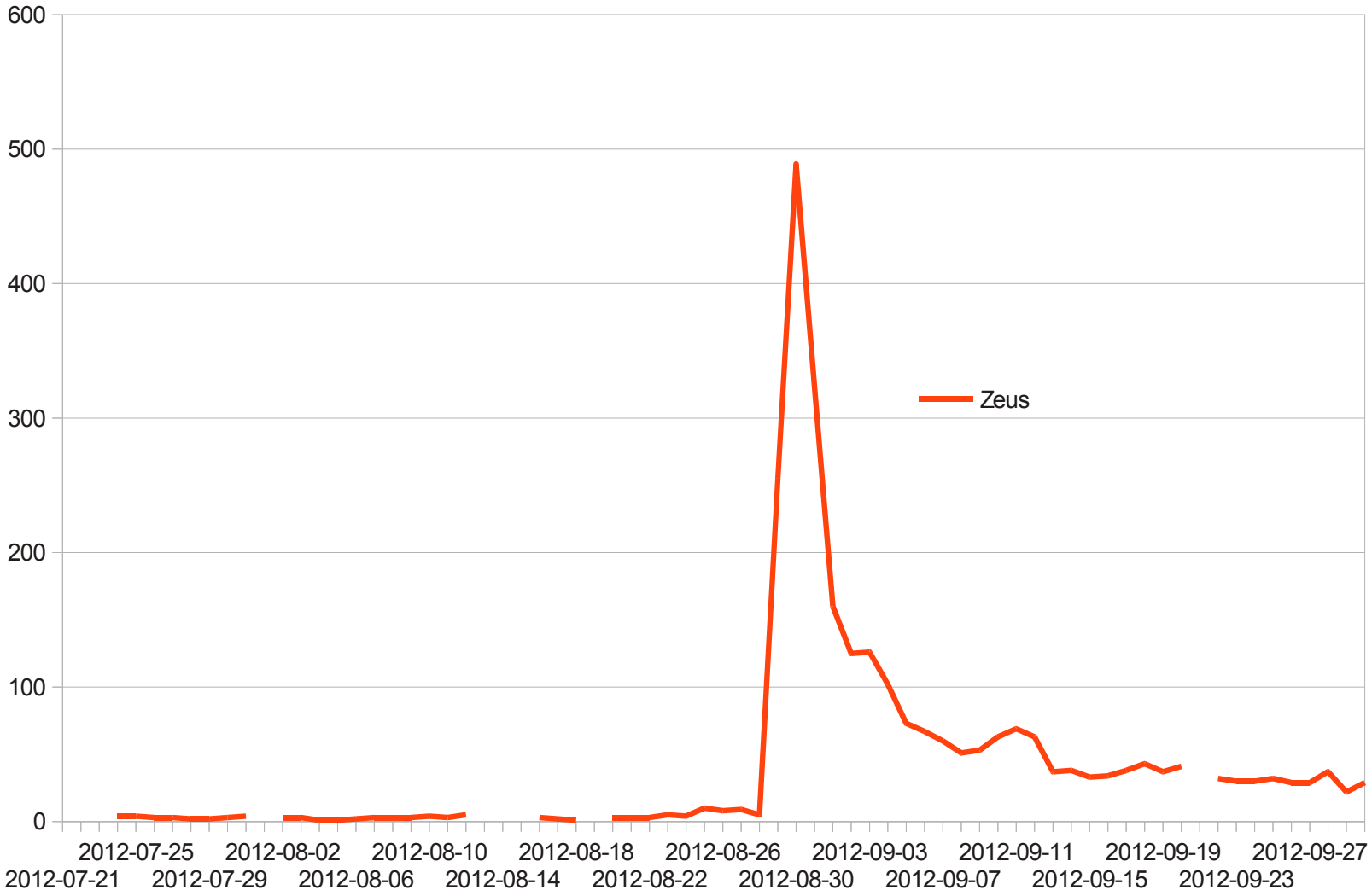
Zemas prioritātes incidentu dinamika 2012.gadā



Inficēto IP adrešu dinamika



Zeus izplatības pieaugums



“Policijas” vīruss

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.

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

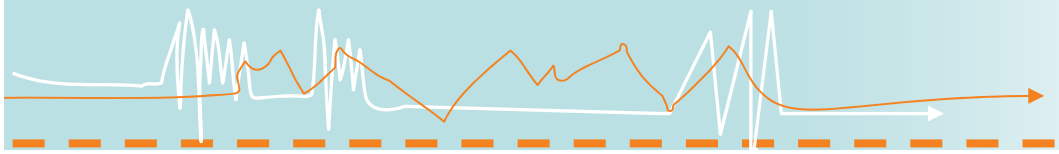
Kur var nopirkt Paysafecard

NARVESEN
plus punkts

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



CERT.LV

Atbildīgs Interneta pakalpojumu sniedzējs

CERT.LV

Atbildīgs interneta pakalpojumu sniedzējs

Sadarbības memorands starp:

- Latvijas Interneta asociācijas *Net-Safe Latvia* Drošāka interneta centru
- Informācijas tehnoloģiju drošības incidentu novēršanas institūciju *CERT.LV*
- Elektronisko sakaru pakalpojumu komersantu / Interneta pakalpojumu sniedzēju (IPS)

Mērķis, lai Interneta pakalpojumu sniedzējs:

- Iestātos par drošāku interneta vidi Latvijā
- Informētu gala lietotājus gadījumos, kad viņu datori ir inficēti ar kādu datorvīrusu
- Aktīvi iesaistītos cīņā ar kriminalizēto pornogrāfiju saturošu materiālu apriti internetā

Memoranda saturs:

- Centra atbildība un saistības
- CERT.LV atbildība un saistības
- IPS atbildība un saistības attiecībā uz Centru
- IPS atbildība un saistības attiecībā uz CERT.LV

CERT.LV atbildība un saistības:

- Apkopot un nosūtīt reizi dienā informāciju par inficētajām IP adresēm
- Izvietot mājas lapā informāciju par Atbildīgajiem IPS
- Konsultēt klientus par drošības incidentiem

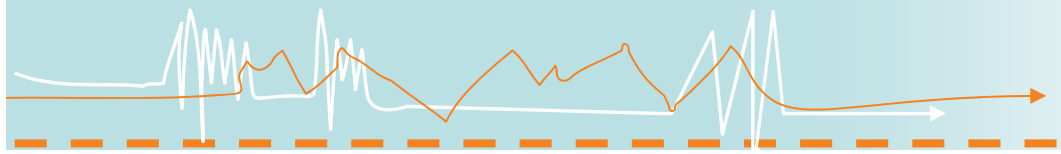
IPS atbildība un saistības attiecībā uz CERT.LV:

- Deleģēt pārstāvi sadarbībai
- Saņemt un apstrādāt inficēto IP adrešu datu bāzi, piecu darba dienu laikā informējot IP adreses lietotāju par inficēto ierīci
- Noteikti ziņojumā jāietver šāda informācija:
  - Inficētā IP adrese un/vai incidenta identifikators, TCP/IP ports, uz kuru norādītajā laikā IP adrese pieslēdzas sensoram;
  - Datorvīrusa nosaukums, ieteikumi, kā problēmu risināt;
  - Norāde, ka informācija saņemta no CERT.LV.
- Informēt klientus, kā saņemt sīkāku informāciju (zvanot vai rakstot CERT.LV)

Atbildīgie interneta pakalpojumu sniedzēji

Kāpēc tas ir svarīgi gala lietotājam?

- CERT.LV nav informācijas par IP adreses gala lietotāju
- Tikai IPS var savlaicīgi informēt gala lietotāju
- Iespēja saņemt kvalitatīvu palīdzību no CERT.LV



CERT.LV

Drošības ekspertu grupa

Drošības ekspertu grupa

Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupa (DEG):

- Dibināta 2012.gada 16.augustā LV CSIRT grupas vietā
- Statūti un Ētikas kodekss
- Noteikumi biedru uzņemšanai
- Sanāksmes reizi mēnesī
- Šobrīd 28 dalībnieki

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
- www.botfrei.de – datoru pārbaudīšana

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 (23)
- Darbā (16)
- Ieteikumu lāde (23)
- 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

maijs 2012

P	O	T	C	P	S	Sv
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

« Apr

Populārākie krāpšanas veidi internetā

Būtu jau labi, ja īstajā brīdī vienmēr varētu bez šaubīšanās pateikt šos vārdus. Vienkārši saprast, ka kāds cenšas Jūs apkrāpt...

AKTUĀLIE RAKSTI

2012. gada 27. februāris 2

Kā atpazīt pikšķerēšanu?

Jau iepriekšējos rakstos par pikšķerēšanu ("Pikšķerēšana jeb, kā atdot savu naudu katram gribētājam" un "3 padomi – kā pasargāt sevi...

2012. gada 23. februāris 2

Kas jāzina, lai droši lietotu „draugiem.lv"?

Šodien vairs neviens nerunā par sociālo tīklu un portālu augošo popularitāti pasaulē. Tas jau ir noticis fakts! Pasaule ir "socializējusies"...

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

- Populārākie krāpšanas veidi internetā
- Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!
- Pārbaudi sava datora veselību pie Datorologa!
- Kā atpazīt pikšķerēšanu?
- Kas jāzina, lai droši lietotu „draugiem.lv"?

Jaunākie komentāri

Tēmas

- Ap un par drošību (39)
- Darbā (22)
- Ieteikumu lāde (37)
- Mājās (32)
- Notikumi pasaulē (2)
- Pasākumi un notikumi (7)
- Publiskās vietās (22)
- Raksti (1)

Saišu lenta

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

Publikāciju kalendārs

oktobris 2012						
P	O	T	C	P	S	Sv
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

CERT.LV brīdinājums

Jūsu IP adrese: 194.8.3.35 ir inficēta

Incidenta datums: 2012-10-24 11:04:30
Datorvīrusa nosaukums: zeus-p2p (Labā prakse)

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 Drošības ekspertu grupas (DEG) sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Robotu tīkls jeb „zombiju armija"
- Bloķētu datoru glābšana un portatīvie antivīrusi
- Rīks IDRE (Informācijas Drošības Risku Eksperts)

Tēmas

- Ap un par drošību (39)
- Darbā (22)
- Ieteikumu lāde (37)
- Mājās (32)
- Notikumi pasaulē (2)
- Pasākumi un notikumi (7)
- Publiskās vietās (22)
- Raksti (1)

Saišu lenta

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

Publikāciju kalendārs

oktobris 2012						
P	O	T	C	P	S	Sv
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

CERT.LV brīdinājums

Jūsu IP adrese: 194.8.3.35 ir inficēta

Incidenta datums: 2012-10-24 11:04:30
Datorvīrusa nosaukums: zeus-p2p (Labā prakse)

Labā prakse:
Redzama datorvīrusa "Zeus" http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS:Win32/Zbot.gen!AF aktivitāte. Lūdzu atjauniniet sava datora antivīrusu programmatūru un veiciet pilnu datora pārbaudi. Vai arī datora pārbaudei variet izmantot kādu no šīm antivīrusu programmām: https://www.botfrei.de/en/decleaner.html vai http://www.f-secure.com/en/web/labs_global/removal/easy-clean vai arī specializētu Zeus datorvīrusa likvidēšanas rīku no Kaspersky: http://support.kaspersky.com/downloads/utils/zbotkiller.zip

---

Lai jūsu dators (vai datortīkls) būtu drošībā, iesakām atslēgt inficēto datoru no datortīkla (Internet) un vērsties pie datorspeciālista.

Lai iztīrītu datoru no datorvīrusa veiciet šādas darbības:

1. Jāveic pilna skanēšana ar atjauninātu Antivīrusu programmatūru; Iesakām izmantot kādu no šiem bezmaksas rīkiem: **BOTFREI**, **F-SECURE**
2. Ja nav iespējams pieslēgties, lai atjauninātu Antivīrusu programmatūru (vai jūsu Antivīrusu programmatūra neko neatrod), dators jāielādē un jāizārstē no citas vides - CD, DVD vai USB diska, to iepriekš sagatavojot uz cita, neinficēta datora. CD sagatavošanai iesakām izmantot, piemēram: **KASPERSKY RESCUEDISK** **F-SECURE RESCUE-CD**
3. Dažos gadījumos pēc infekcijas likvidēšanas, iespējams, ka kādi faili būs bojāti un tie būs jāatjauno no datora rezerves kopijas.

Lai turpmāk jūsu dators būtu labāt pasargāts, iesakām ņemt vērā šeit aprakstīto:

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 Drošības ekspertu grupas (DEG) sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Robotu tīkls jeb „zombiju armija"
- Bloķētu datoru glābšana un portatīvie antivīrusi
- Rīks IDRE (Informācijas Drošības Risku Eksperts)
- Paroļu nebūšanas jeb nomaini savu paroli. Tagad.


CERT.LV
INFORMĀCIJAS TEHNOLOĢIJU
DROŠĪBAS INCIDENTU
NOVĒRŠANAS INSTITŪCIJA


enisa
European Network
and Information
Security Agency

Nākotne

Nākotne

- Latvijas izvēlētais ceļš – drošība caur sadarbību
- IT drošības līmeni valstī var paaugstināt tikai kopīgiem spēkiem
- Vairāk Atbildīgo IPS!
- IT drošībai jākļūst par katra ikdienu
- Lietotāji jāturpina izglītot un ieinteresēt IT drošībā
- Jāveicina akadēmiskie pētījumi IT drošības jomā
- Jāveicina un jāorganizē kvalitatīvas diskusijas par drošības jautājumiem

Tuvākie pasākumi

- Valmieras “hackfest” – 1-2.decembris
- Tehniskais seminārs – “Esi drošs” 4.decembris
- CERT.LV tehniskās IT drošības mācības – 16-17.janvāris, 2013

Paldies par uzmanību!

http://www.cert.lv/
baiba.kaskina@cert.lv
https://twitter.com/certlv