“*deny ip any any*”, vai IT drošības incidents piektdienas vakarā

Varis Teivāns, CERT.LV

08.11.2012. Rīga, Latvija

ISACA Latvijas nodaļas un CERT.LV konference

IT drošības incidents

Uzbrukuma motivācija

- DOS/DDOS – servisa atteices uzbrukums
- Deface – publiski pieejama resursa izķēmošana
- Nesankcionēta resursu izmantošana
- Informācijas zādzība / Spiegošana
- *Cybercrime* Bizness – visas incidentu variācijas

Incidenta uztveršanas fāzes

“nejaukais scenārijs”

- Neziņa
- Slinkums
- Panika
- Ignorance / Noliegšana
- Hej! Ar šo taču var pievērst uzmanību :)
- **Definēto procedūru ievērošana, pēc kurām incidents tiek risināts un izvērtēti riski**

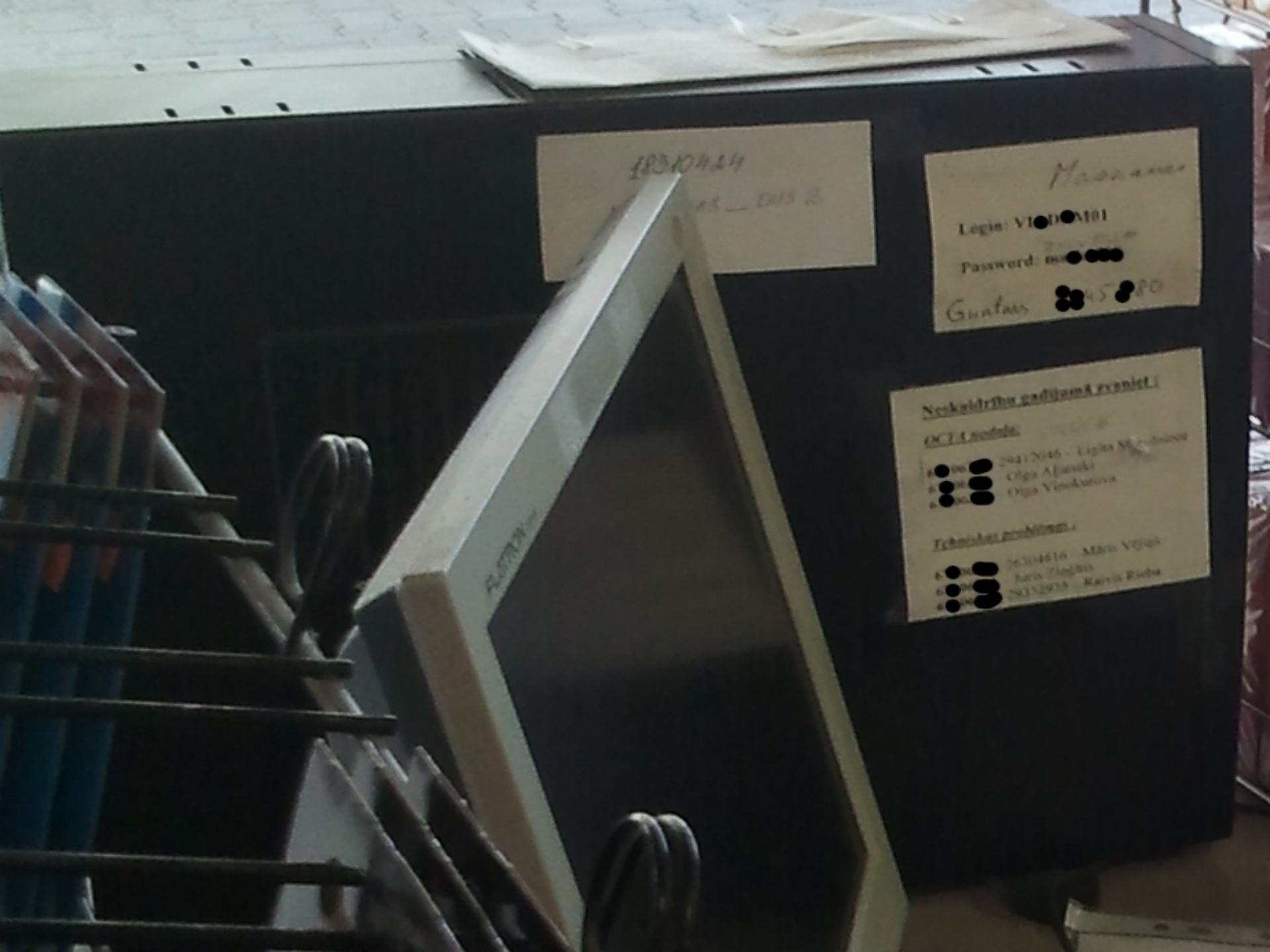
Neziņa

- Par incidentu uzzin no CERT.LV (labākajā gadijumā)
- Nereti ir situācijas, kad informācija jau ir nonākusi līdz publiski pieejamiem resursiem (ziņas, forumi)
- Savu IT resursu iespēju neapzināšanās

Slinkums

- Dažkārt visa drošības politikas izvēle nemanāmi tiek balstīta uz šo netikumu
- Nepiemērota paroļu izvēle, servisu un piekļuves neapzināšana
- Autentifikācijas dati tiek rakstīti uz lapiņām un kaut kur pielīmēti
- Paroļu izvēles politika neeksitē pat lielos, ar IT saistītos uzņēmumos


Contex
durex
Login: VIADAM01
Password: mask1888


Login: VI●●●M01
Password: m●●●●
Neskaidrību gadījumā zvaniet:
OCT4 nodaļa:
Olga Afanasjeva
Olga Vinokurova

Panika

- DDOS uzbrukums – serverim tiek atslēgts tīkls, lai nenotiek kas ļaunāks. No uzbrucēja viedokļa – viegla uzvara
- Firewall/IDS sāk ziņot par SQL injekcijas mēģinājumiem – Serveris tiek izslēgts

Panika

- Firewall/IDS nokonfigurēts celt trauksmi, kad pieslēgumu skaits pārsniedz definētās robežas – serveris tiek izolēts no interneta, taču izrādās, ka pieprasījumi bijuši leģitīmi

Panika

VS

Panika

- Noslodzes balansēšanas iekārta valstiski nozimīgam resursam tiek nokonfigurēta ar neadekvāti zemu slodzes noturi.
- Rezultāts: izveidojas leģitīmu lietotāju DOS. Sākotnēji tas tiek uzskatīts par uzbrukumu, taču situācija ir labojama ar vienu konfigurācijas rindiņu

Ignorance / Noliegšana

- Tiek savlaicīgi ziņots par identificētām kritiskām ievainojamībām – risks tiek pieņemts, problēma netiek risināta
- Bet vēl taču nekas nav noticis...
- Ir gadījumi, kur savādāka sākuma taktika kā "*noliegšana*" netiek pieļauta...

Ignorance / Noliegšana

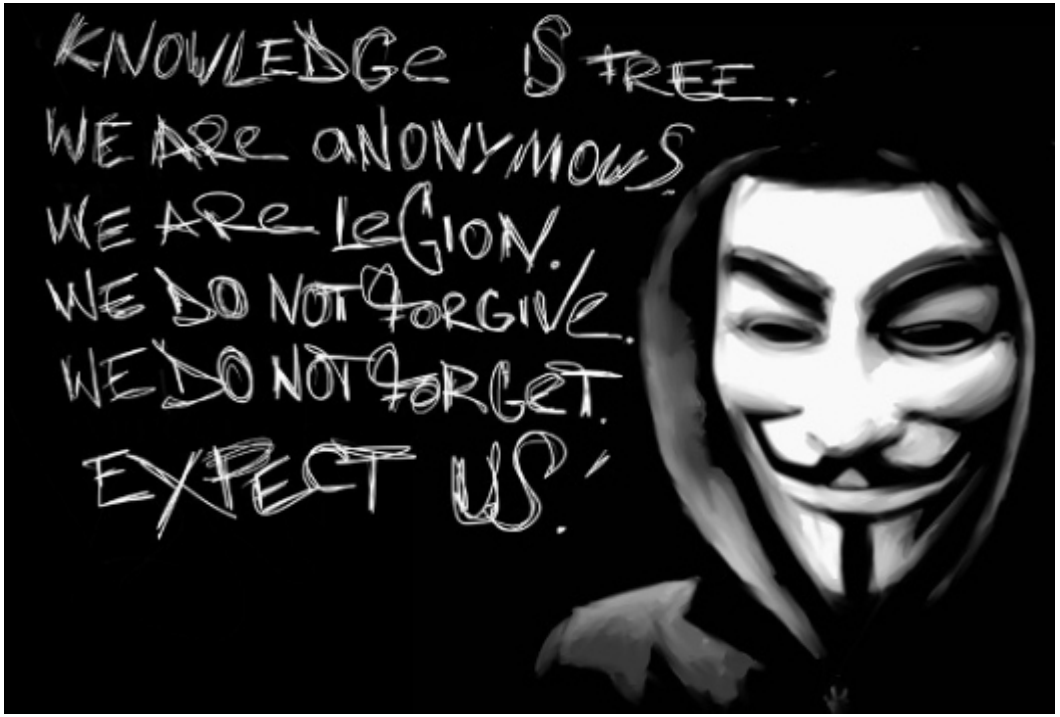
Hej! Ar šo taču var pievērst uzmanību

- Incidentu safabricēšana PR nolūkos – vairāki gadījumi arī Latvijā
- Informācijas kropļošanās ceļojot starp resursiem

Hej! Ar šo taču var pievērst uzmanību

- Anonymous tēla izmantošana kā PR instruments

Liela daļa uzbrukumu nav nekādā veidā saistīti ar Anonymous



Ko darīt, ja tiek konstatēts notiekošs IT drošības uzbrukums?

Drošības perimetrs

- **Incidenta risināšanas procedūra**
- Jāapzin savi resursi un iformācijas avoti
- Jāsaprot kam uzbrūk un kādas ir pirmās, acīmredzamās pazīmes
- Jāzin kontaktpersona pie sava IPS

Uzbrukums tīkla servisam

- Programmatūras atjauninājumiem ir iemesls... Tos vajadzētu pielietot
- Piekļuves kontroles mehānismi?
  - **VoIP** – Latvijā katru gadu vairāki uzbrukumu gadījumi. Zaudējumi katrā incidentā no vairākiem desmitiem līdz simtiem latu
  - **NAS** – pieejami no visa interneta

Uzbrukums WEB servisam

- Noturīgas tendences - OWASP TOP 10
- SQL injekcija - viena no biežāk izmantotajām ievainojamībām web servisiem

Uzbrukums WEB servisam. Ko darīt panikas brīdī?

- DB uzbrukuma brīdī tikai *read* režīmā
- DB lietotāja tiesības:
  - FS *read* / FS *write*
    - File, insert, update, create table...
  - SELECT … INTO DUMPFILE
- Ar sql injekciju var nolasīt, ierakstīt failus
- web servera lietotāja tiesības *read* režīmā un tikai savā direktorijā

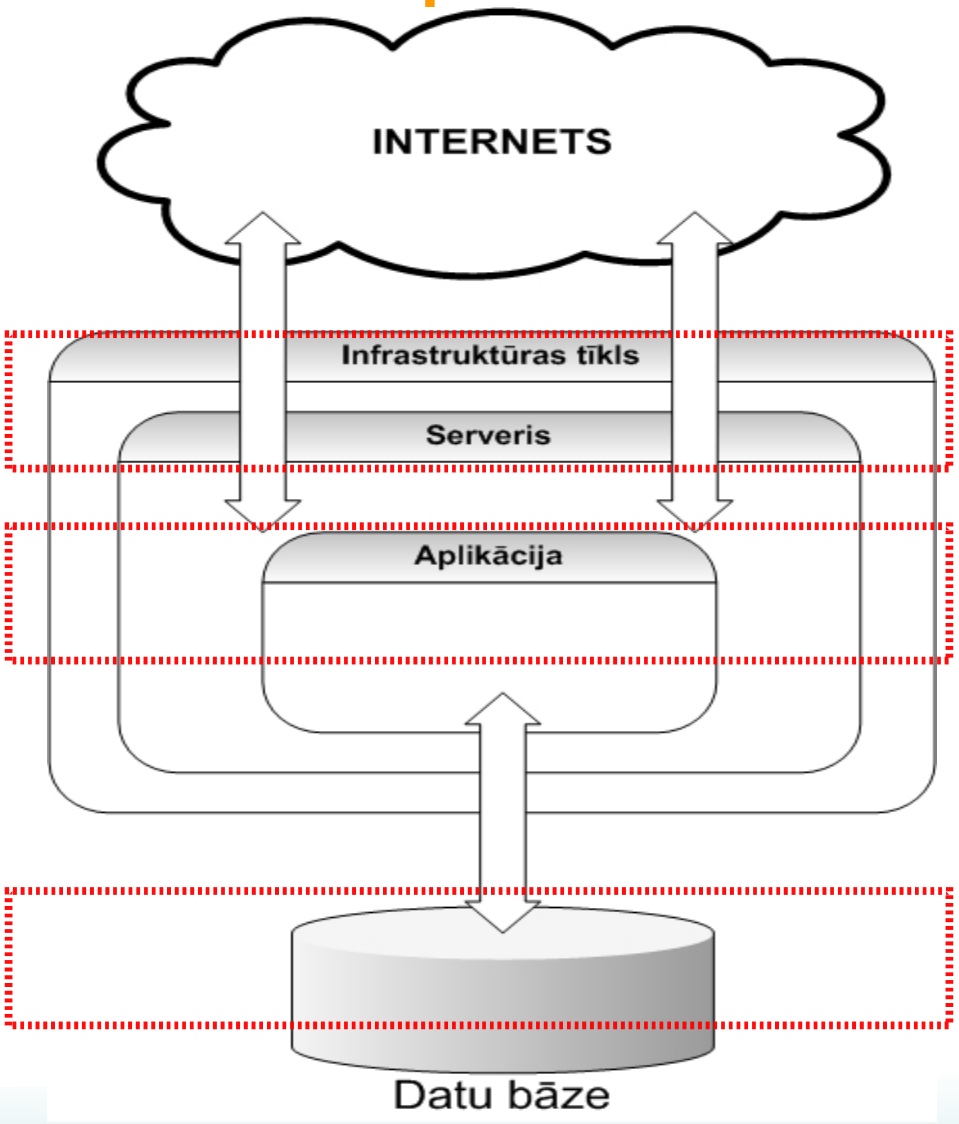
Uzbrukums WEB servisam. Ko darīt panikas brīdī?

- Jāpārliecinās, lai lietotāja .htaccess nepārkāpj globālos uzstādījumus
- Lai nestrādā symlink ar kura palīdzību varētu izkļūt no kokrētā lietotāja direktorijas
- HTTP POST žurnalēšana
- Jābūt gatavam ievākt datu plūsmas pcap
- SRC IP spoof prevencija – kolektīva atbildība IPS - IPS
- Memory dump / process memory dump

Kur veikt aizsardzības pasākumus?

- Primāri vajadzētu koncentrēties uz nepilnību novēršanu aplikācijas līmenī. Par to jādomā visā izstrādes procesā
- Lai Firewall/IDS/IPS, WAF (mod_security) nekalpo kā primārais vairogs “caurai” sistēmai

Drošības perimetrs



WAF, IDS/IPS, NetFlow, FW, pcap – tshark proto fields, regex., SIEM

Droša programmatūras koda izveide.

SQL modifikācija

PENTEST

- Vai no tā ir jābaidās? - Nē
- Vai ir jāizvairās veikt testus uz *production* sistēmas – Nē. It sevišķi, ja tas ir ik vienam tīklā sasniedzams serviss.
- Uzbrukumu mēģinājumus un ievainojamību testus veiks arī bez Jūsu piekrišanas vai zināšanas

Mēs prasām jaunākās tehnoloģijas, bet vai protam izmantot esošās?


Cilvēki gaida rindā pēc jauna viedtelefona

- Viedtālruņu programmatūras izstrādē tiek atkārtotas gadiem vecas kļūdas
- Blackhole exploit kit lielāko daļu upuru inficē izmantojot vairāk kā gadu vecas ievainojamības
- SQL injekcijas – tiek izmantotas jau kopš 2005. gada un joprojām turpinās

Nikjju Mass injection campaign (180k+ pages compromised)

april 17, 2012 by daniel cid · 16 comments

Our research team have been tracking a new mass SQL injection campaign that started early this month. So far more than 180,000 URLs have been compromised. We will keep posting updates as we get them.

Massive SQL Injection Attack Hits A Million Pages

LizaMoon attacks may have waned but code injection is still rife with a million pages infected in a new wave

On October 20, 2011 by Eric Doyle 1

A massive blitz of SQL injection attacks has been unleashed against Websites based on Microsoft ASP.Net. It is reported that up to a million Web pages have been infected so far.

The attack, discovered by online security firm Armorize, seems to be related to the LizaMoon attacks last April. The certificates used are registered under the same name as those used in the previous attack. There was also an apparently unrelated attack that infected six million sites in early August.

Barclays: 97 percent of data breaches still due to SQL injection

Barclays calls for better information security management to protect against attacks

By Sophie Curtis | Techworld | Published: 15:35, 19 January 2012

SQL injection attacks have been around for more than ten years, and security professionals are more than capable of protecting against them; yet 97 percent of data breaches worldwide are still due to an SQL injection somewhere along the line, according to Neira Jones, head of payment security for Barclaycard.

4 dažādi Sony incidenti – visi SQL

Sony hack reveals password security is even worse than feared

Most conformed to *very* predictable patterns

By **John Leyden** • **Get more from this author**

Posted in Security, 8th June 2011 10:07 GMT

SQL inject

An analysis of password re-use from data spilled via the Sony and Gawker hack reveals that consumer password security is even more lax than we might have feared.

A million Sony users' password/username IDs and 250,000 Gawker login credentials, each stored in plain text, were exposed via separate hacks. In each case hackers posted a subset of these passwords as a torrent.

MIT incidents - SQL

Internet

Hackers Use MIT Server to Hack 100,000 Sites

Jason Mick (Blog) - November 7, 2011 2:42 PM

Print

2 comment(s) - last by Ammohunt.. on Nov 8 at 10:24 PM

SQL inject

SECURITY

MySQL.com Hacked to Serve Malware

SQL inject

400,000 apmeklētāju dienā

#root tika pārdots cybercrime izsolēs par 3000$

- Apache servisa ievainojamības – vairākus gadus vecas – izplatība milzīga.

- PHP, Ruby, Java, etc., *izņemot Perl* - HASH table DOS. Ievainojamības vairākus gadus vecas – izplatība milzīga. Jaudīgi serveri nogāžami ar vienu piezīmju datoru.

- Joprojām apbrīnojams daudzums ar WiFi AP, kas lieto WEP, vai pilnībā atvērtus AP. Reāli testa rezultāti Rīgā. Simtiem atvērtu piekļuves punktu.

Paroļu izvēle redzama vairākos lielos incidentos

- Linkedin
- Vairāki paroļu zādzības incidenti pie kuriem strādajis CERT.LV
  - Vairāk kā 1 milj. unikālu lietotāju datu
- WiFi paroles nav labākā situācijā

Ranking	Password Phrase	Number of Times Appeared
1	link	941
2	1234	435
3	work	294
4	god	214
5	job	205
6	12345	179
7	angel	176
8	:the	143
9	ilove	133
10	sex	119
11	jesus	95
12	connect	91
13	Fu**	85
14	monkey	78
15	123456	76

Top Nr.	Biežums	Parole
1	673	'123456'
2	404	'1q2w3e4r5t'
3	385	'123456789'
4	308	'12345'
5	265	'qwertyuiop'
6	254	'1qaz2wsx'
7	228	'123456a'
8	226	'123'
9	226	'zxcvbnm'
10	223	'k.
11	216	'stalker'
12	198	'1234qwer'
13	191	'1234'
14	188	'qwertyuiop'
15	187	'123456789a'
16	172	'qwe123'
17	170	'qwerty'
18	167	'1234567'
19	152	'qwerty'
20	152	'samsung'
21	143	'159753'
22	138	'ghbdtn'
23	137	'nikita'

DNS cache poisoning (Kaminsky attack)

- Ievainojamība atklāta 2008. gadā
- 2012. gadā izplatība joprojām milzīga
  - NIC.LV un CERT.LV kopīgi veiktais pētījums

DNS cache poisoning (Kaminsky attack)

- NIC.LV un CERT.LV kopīgi veiktais pētījums
  - Analizēti ~4500 DNS pieprasījumu avoti
  - 13% identificēti kā potenciāli ievainojami
  - 177 DNS serveriem atļauti rekursīvie pieprasījumi no visas pasaules
  - Daļa ievainojamo serveru bija IPS DNS serveri, kurus lieto tūkstošiem klientu

DNS cache poisoning (Kaminsky attack)

- Risinājums ir sen pieejams
  - DNS serveru programmatūras atjaunināšana
  - DNSSEC
  - No Latvijā apzinātajiem serveriem lielākā daļa ievainojamības ir izlabojuši

Apkopojums

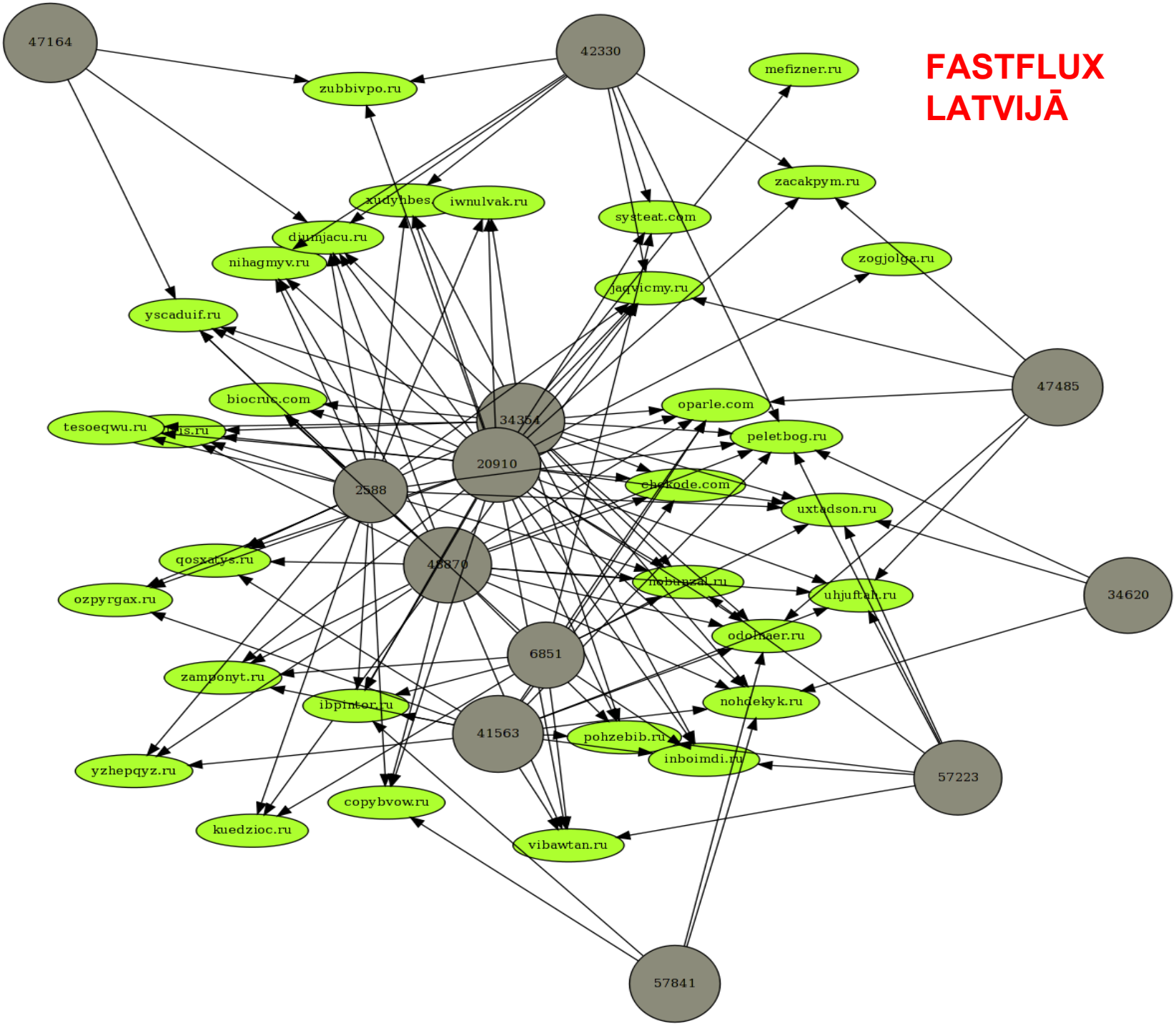
- Ērti un vienkārši – nopirkt drošību, bet...
  - Lielu daļu aizsardzības mehānismu ir iespējams ieviest neieguldot milzīgus līdzekļus
  - Vai var nopirkt drošības stāvokli?
- Liela daļa uzbrukumos izmantotās ievainojamības joprojām ir gadiem vecas
- Vājākais posms - joprojām cilvēks

Apkopojums

- Jāstrādā pie lietotāju izglītošanas un izpratnes veidošanas par to, ka arī IT drošība ir svarīga
- Pieminētos izaicinājumus CERT.LV piedāvā risināt rīkojot praktiskos seminārus, praktiskās un teorētiskās IT drošības mācības, hackfest
  - Dalība - BEZMAKSAS

Apkopojums

- Semināru programma, kas attiecās uz minētajām tēmām:
  - NETFLOW / NFSEN
  - Risku pārvaldība
  - SEM / SIEM ar OSSEC
  - IT uzbrukumu vizualizācija
  - MS server security policy & templates


FASTFLUX
LATVIJĀ
47164
42330
mefizner.ru
zubbivpo.ru
zacakpym.ru
xudyhbes.
iwnulvak.ru
systeat.com
djuvmjacu.ru
nihagmyv.ru
zogjolga.ru
jaqvicmy.ru
yscaduif.ru
47485
biocruc.com
oparle.com
tesoeqwu.ru
34364
peletbog.ru
20910
2588
chekode.com
uxtadson.ru
qosxafys.ru
45870
nobunzal.ru
34620
ozpyrgax.ru
uhjuftah.ru
odohner.ru
6851
zamponyt.ru
nohdekyk.ru
ibpintor.ru
41563
pohzebib.ru
yzhepqyz.ru
inboimdi.ru
57223
copybvow.ru
kuedzioc.ru
vibawtan.ru
57841

Paldies par uzmanību

http://ww.cert.lv/
cert@cert.lv
varis.teivans@cert.lv