

mysphere1

# Rozvoj systémů pro detekci průniků v síti WEBnet

Projekt FR Cesnet



Radoslav Bodó <[bodik@civ.zcu.cz](mailto:bodik@civ.zcu.cz)>

Aleš Padrta <[apadrta@civ.zcu.cz](mailto:apadrta@civ.zcu.cz)>

# Agenda

- O projektu
- Zkoušené nástroje
- Výstupy projektu
- Závěr



# O projektu

- FR Cesnet č. 230/2007
- CIV, ZČU Plzeň
- Motivace
  - WIRT chtěl nástroj pro detekci napadených PC
  - Začít incidentům předcházet
- Cíle
  - Naučit se problematiku
  - Zlepšit stávající nástroje
  - Zvýšit bezpečnost sítě WEBnet



# Řešení projektu

- Výchozí stav
  - snort, nepenthes
  - Bez reportingu, procesní reakce, znalostí
- Cílový stav
  - Získat znalosti (literatura, konference)
  - Prostředky (Xen server)
  - Provozně 2 – 3 systémy
    - Nids: snort, labrea, nepenthes, honeytrap, pehunter
    - Wids: php hop, GGH
  - Reporting a reakce
  - Výměna získaných dat





# Metody (N)IDS

- Analýza provozu
  - Vyhodnocování toků
    - Statistické modely (baseline)
    - Vyhledávání vzorů
  - Inspekce paketů
  - Logy (HIDS)
- Honeypoty
  - S nízkou interakcí – emulátory
  - S vysokou interakcí – *tvrzené stroje*

# LaBrea

- Tarpit honeypot (cesnet-cirt)
- Reakce na lavinu CodeRed
- Pokus o zpomalení
  - LaBrea užívá možností TCP pro řízení toku
    - Nedokončí spojení
    - Ohlašuje nemožnost přijímat (zero window)
  - Pozdrží exekuci viru – zaměstnává škodiče
- Log > Reporting



# LaBrea

- Reporting
- labrea\_report.pl
- Geolokace
  - Net::Whois::Iana
  - Vypnuto

```
DEBUG: query whois for 216.191.75.193
DEBUG: query whois for 24.80.177.41
DEBUG: query whois for 131.193.39.207
DEBUG: query whois for 217.133.229.193
DEBUG: query whois for 222.133.128.205
DEBUG: query whois for 125.123.145.196
DEBUG: query whois for 24.80.194.248
DEBUG: query whois for 70.67.220.123
Total sessions: 9327
```

```
Total attackers in ownnet: 1
    147.231.xx.194 at 147.228.0.0/14: 36 times
```

```
Destination ports listing: 34 in total
```

445:	4566
139:	2094
3306:	654
1080:	383
5405:	266
3128:	252
8800:	252
1433:	252
623:	245
25:	228
111:	88

```
<zkraceno>
```

```
Attackers listing: 138 in total
```

213.215.208.132:	497	IT
70.70.124.224:	496	CA
213.80.23.75:	433	SE
66.151.10.1:	266	US
217.106.133.72:	252	RU
122.116.113.218:	228	TW
131.193.39.207:	221	US
81.195.104.242:	220	RU
70.70.18.221:	207	CA
70.71.74.29:	196	CA
64.16.34.34:	183	US
209.82.46.121:	179	CA



## Overall

Time frame: 2008-03-19 12:33:27 - 2009-05-09 20:15:31

Last bw at: 2009-05-09 20:15:31 - **1648b/s**

Last tarpit at: 2009-05-09 20:15:02 (**1m ago**) from [79.229.43.213](#) (p4FE52BD5.dip.t-dialin.net)

Legend: **Port rise** **Port fall** **Well-known port** **Registered port** Dynamic/private/local port

## Ownnet attackers for 30 days

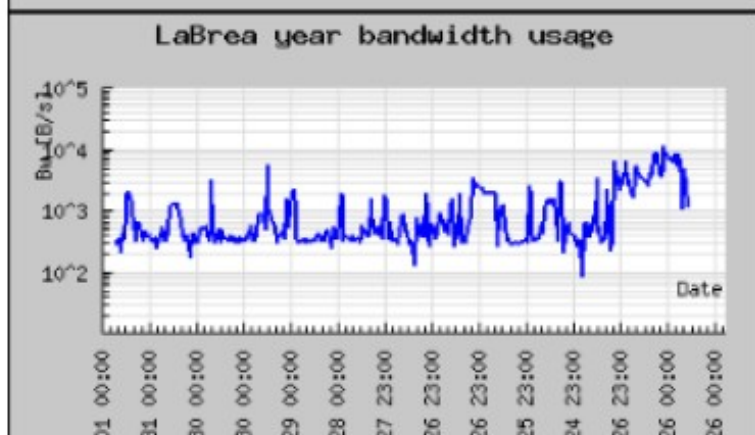
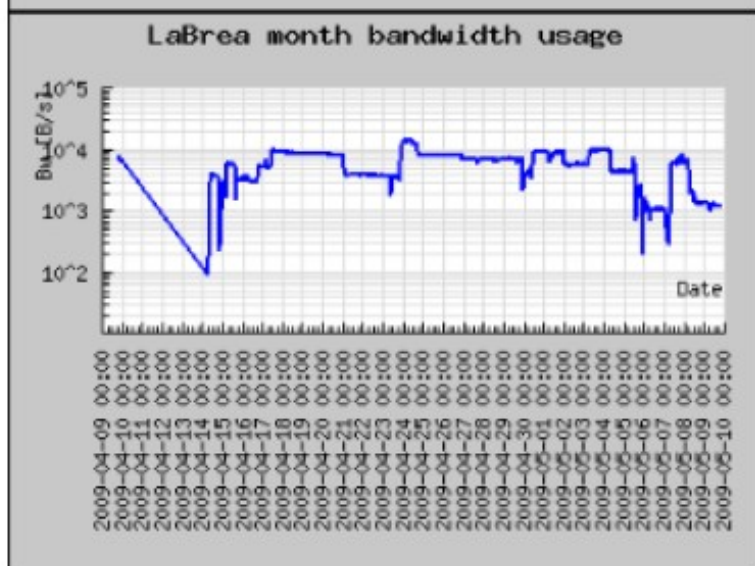
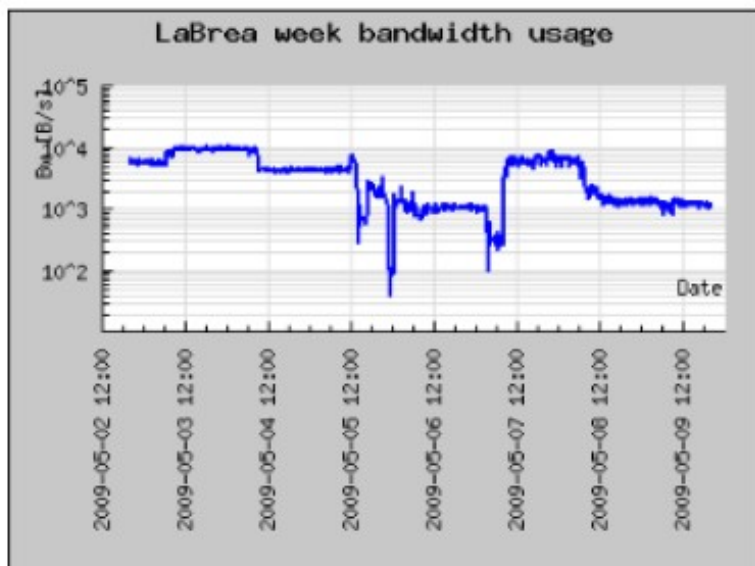
time	held	ips	ipd	psrc	pdst	count	hostname
2009-04-29 11:00:48	0	<a href="#">195.113.1.111</a>	0.166	3145	21705	1	.....vvs-pv.cz
2009-04-27 00:16:29	5	<a href="#">146.102.2.202</a>	0.48	5042	1433	252	.....vse.cz
2009-04-25 12:50:19	0	<a href="#">195.113.5.114</a>	0.128	3027	15854	1	.....cuni.cz
2009-04-16 14:15:23	0	<a href="#">78.128.1.111</a>	0.183	2530	25724	1	1.....e.cuni.cz

## Port trends

trend = count(dpst) - avg(last 72 hours)

pdst/name	count	count72	trendRatio
<b>1433/ms-sql-s</b>	31364	91224	<b>0.344</b>
<b>3306/mysql</b>	3368	3086	<b>1.091</b>
<b>22/ssh</b>	1862	618	<b>3.013</b>
<b>23/telnet</b>	1599	682	<b>2.345</b>
<b>25/smtp</b>	1559	683	<b>2.283</b>
<b>445/microsoft-ds</b>	1232	608	<b>2.026</b>
<b>4899/radmin-port</b>	1094	932	<b>1.174</b>
<b>139/netbios-ssn</b>	526	205	<b>2.566</b>
<b>2967/</b>	502	880	<b>0.57</b>
<b>1080/socks</b>	256	90	<b>2.844</b>
<b>8089/</b>	252	425	<b>0.593</b>
<b>21/ftp</b>	252	169	<b>1.491</b>
<b>3050/gds_db</b>	250	0	<b>250</b>
<b>9090/</b>	250	569	<b>0.439</b>

- Pohled
- | labrea.loadup >

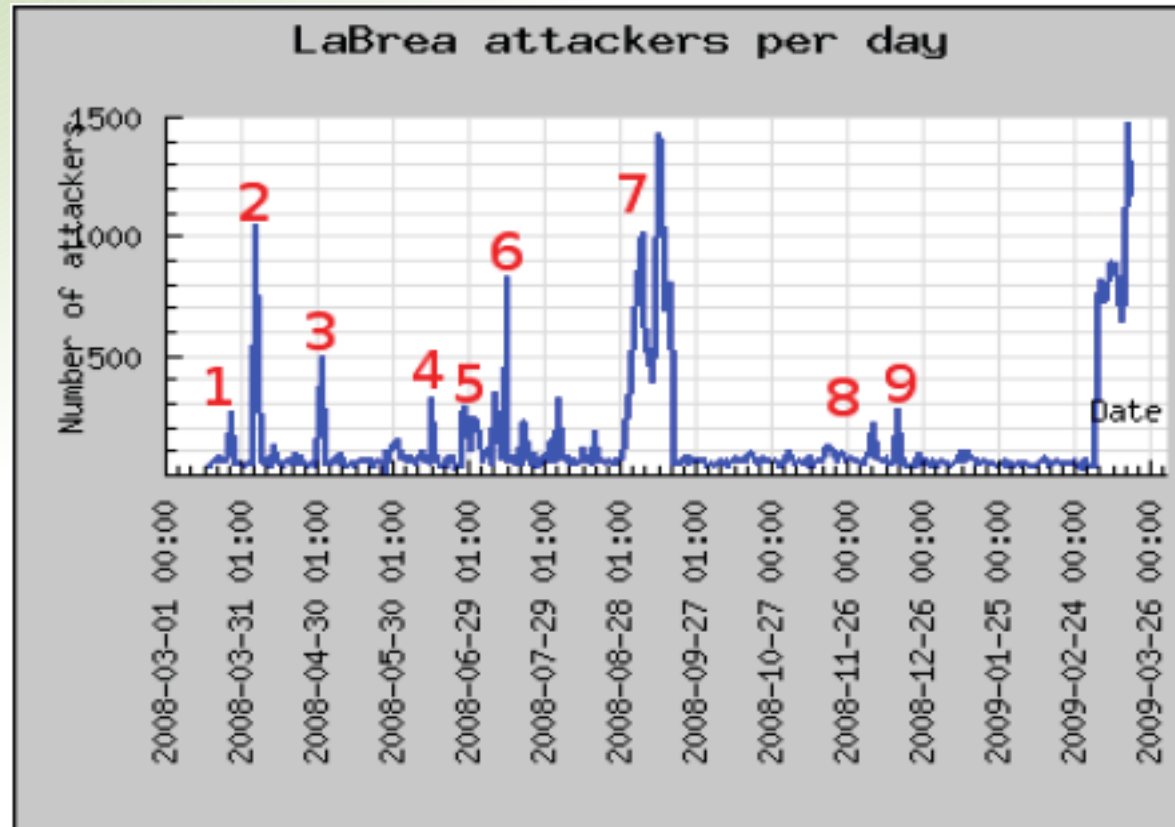




# LaBrea

- Velikost: 253 adres
- Výsledky za období 03/08 – 03/09
- Celkem 37 628 útočníků (146/den)
- WEBnet/Cesnet2 8:8

- Špičky
  - VNC, MS, Web
- Pokračujeme



# Nepenthes (láčkovka)

- Nejen síť
- Emulátor Windows
- Zachycuje nabízený malware
- C++, problematický výstup
  - Debug log
  - Prelude IDS:
    - + IDMEF, Pluginy, HIDS
    - – Python, DB, GUI
    - Not this time
  - SurfIDS:
    - – Pluginy, PostgreSQL
- Zvolili jsme vlastní dočasné řešení





# Nepenthes

- Vlastní modul log-grep
- nepe\_report2.pl
- malware
  - ClamAV
  - Public DB
- <http://www.nothink.org/binaries/malwa>
- <http://www.cyber-ta.org/releases/malw>
- <http://nepenthes.carnivore.it/analysis>

```
Total sessions: 14373
Total events: 60617
EV_SOCKET_TCP_RX: 23151
EV_SOCKET_TCP_CLOSE: 14068
EV_SOCKET_TCP_ACCEPT: 12346
EV_HEXDUMP: 4113
EV_DOWNLOAD: 1734
EV_DIALOGUE_ASSIGN_AND_DONE: 1732
EV_SHELLCODE_DONE: 1732
EV_SLAMMER: 869
EV_SOCKET_UDP_RX: 869
EV_SUBMISSION: 3
```

```
Total attackers in ownnet: 1
147.228.xx.161 at 147.228.0.0/14: 25064 times
```

```
Uniq submissions: 3
SUBMISSION: 5a0e0370ce40bd8aa2c25b2a2e8b347e ftp://1:1058.77.97.100:55083/vPanele.com: 1
-rw-r--r-- 1 nepei nepei 105472 Nov 16 2008 /opt/nepe/var/binaries/5a0e0370ce40bd8aa2c25b2a2e8b347e
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/5a0e0370ce40bd8aa2c25b2a2e8b347e/
5a0e0370ce40bd8aa2c25b2a2e8b347e.virus-labels
```

```
SUBMISSION: 831f4ee0a7d2d1113c80033f8d6ac372 ftp://anonymous:bin079.41.216.217:5554/13938_up.exe: 1
-rw-r--r-- 1 nepei nepei 15872 Mar 4 2008 /opt/nepe/var/binaries/831f4ee0a7d2d1113c80033f8d6ac372
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/831f4ee0a7d2d1113c80033f8d6ac372/
```

```
831f4ee0a7d2d1113c80033f8d6ac372.virus-labels
http://nepenthes.mwcollect.org/analysis:norman:831f4ee0a7d2d1113c80033f8d6ac372
http://www.honeynet.unam.mx/en/malware.pl?hash=831f4ee0a7d2d1113c80033f8d6ac372
```

```
SUBMISSION: e7801a316bb060178914ae9dbfd0078a ftp://1:1089.136.110.154:63219/Tilesys.com: 1
-rw-r--r-- 1 nepei nepei 214016 Nov 16 2008 /opt/nepe/var/binaries/e7801a316bb060178914ae9dbfd0078a
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/e7801a316bb060178914ae9dbfd0078a/
e7801a316bb060178914ae9dbfd0078a.virus-labels
```

```
Uniq hexdumps: 33
HEXDUMP: 0f7b92f524b404314c0b6ccc6c3e76215: 1
-rw-r--r-- 1 nepei nepei 613 Mar 22 19:47 /opt/nepe/var/hexdumps/0f7b92f524b404314c0b6ccc6c3e76215.bin
00000000 50 4f 53 54 20 2f 75 6e 61 75 74 68 65 6e 74 69 |POST /unauthenti|
00000010 63 61 74 65 64 2f 2f 2e 2e 25 30 31 2f 2e 2e 25 |cated//..%01/..%|
00000020 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
00000030 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000040 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000050 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
00000060 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000070 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000080 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
00000090 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
000000a0 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
000000b0 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
000000c0 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
000000d0 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
000000e0 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
000000f0 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000100 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000110 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
00000120 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000130 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
00000140 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e |01/..%01/..%01/.|
00000150 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 |..%01/..%01/..%01|
00000160 2f 2e 2e 25 30 31 2f 2e 2e 25 30 31 2f 2e 2e 25 |/..%01/..%01/..%|
<zkraceno>
```

# Nepenthes

## Overall

Time frame: 2008-03-20 14:29:14 - 2009-05-24 11:33:50

Last attacker at: 2009-05-24 11:33:50 (35m ago) from 147.229.67 ( [REDACTED].cz )

Legend: Port rise Port fall Well-known port Registered port Dynamic/private/local port

## Ownnet attackers for 30 days

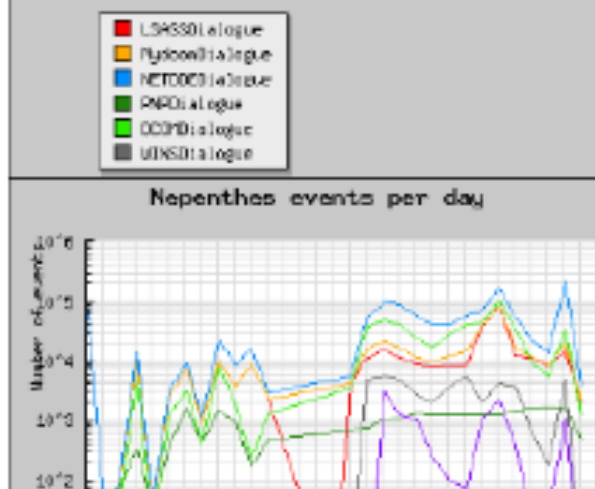
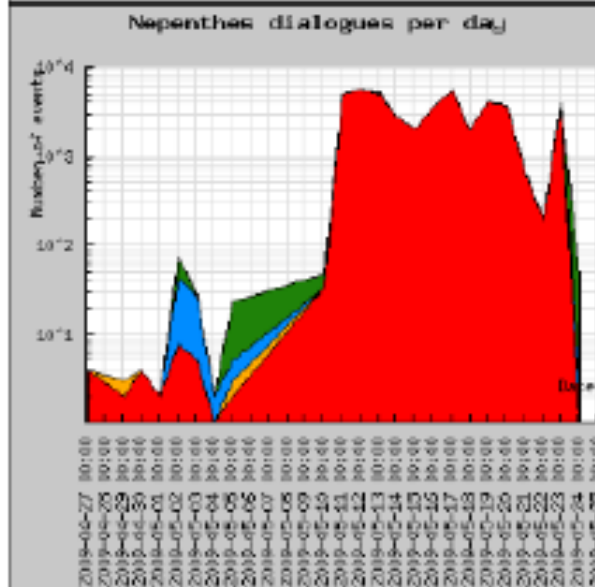
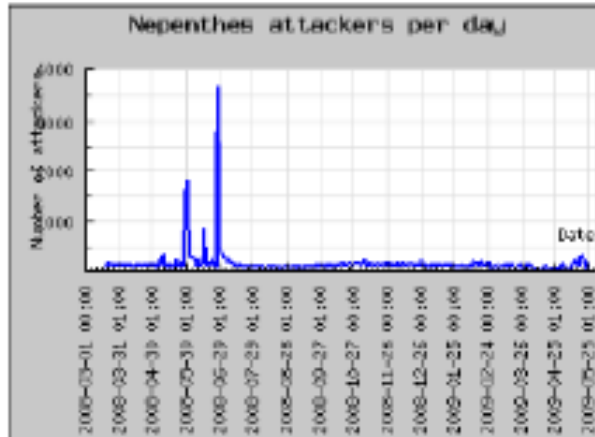
time	held	ips	ipd	psrc	pdst	count	tot_size	hostname
2009-05-20 02:07:33	4771	[REDACTED].215	[REDACTED]	4824	445	208	9152	[REDACTED].cz
2009-05-11 10:14:09	18800	[REDACTED].67	[REDACTED]	1977	445	81574	6719456	[REDACTED].cz
2009-05-04 13:04:30	665	[REDACTED].133	[REDACTED]	58676	3140	37635	734070	[REDACTED].cz
2009-05-04 12:19:45	77	[REDACTED].190	[REDACTED]	1169	21	22	588	[REDACTED].190

## Port trends

trend = count(dpst) - avg(last 72 hours)

pdst/name	count	count72	trendRatio
445/microsoft-ds	60145	77288	0.778
0/	6224	4940	1.265
1434/ms-sql-m	2624	3232	0.812
42/nameserver	2461	0	2461
21173/	1054	0	1054
4493/	963	0	963
18800/	902	0	902
40720/	902	0	902
13504/	901	0	901
13117/	900	0	900
12198/	891	0	891
21856/	887	0	887
39161/	885	0	885
22832/	883	0	883
13665/	877	0	877
3359/	875	0	875
28590/	875	0	875
27408/	870	0	870
39382/	866	0	866
39442/	865	0	865
139/activex-svc	0	3719	0

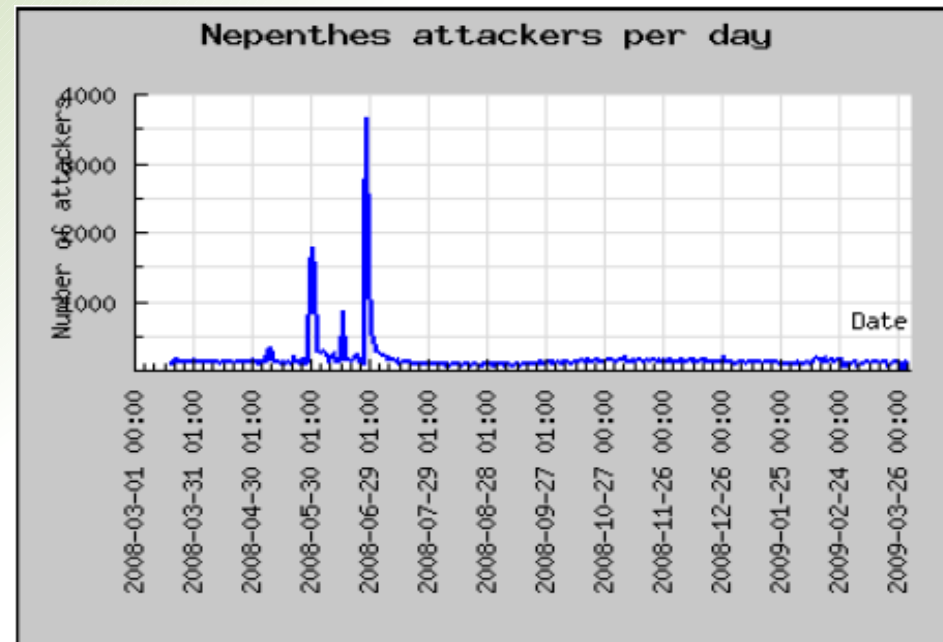
- Pohled
- | nepe.loadup >





# Nepenthes

- Velikost: 150 adres
- Výsledky za období 03/08 – 03/09
- Celkem 28 485 útočníků (156/den)
- WEBnet/Cesnet2 12:4
- Špičky – MS



- Malware
  - Žádný z ownnetu
  - Celkem 450 unikátních vzorků
- Pokračujeme >> dionaea ?

# Webové honeypoty

- Nejen síť a Windows
- Web, atraktivní cíl (WAF)
- PHP HoP, GHH
  - Neudržovány
  - Nepěkné
- HIHAT
  - Vyrobit honeypot z jakékoliv PHP aplikace
  - Logovací preambule
  - Výsledek je vysoce interaktivní



# HIHAT s nízkou interakcí

- Wget mirror předlohy
  - Filtr výkonného kódu
  - Scramble obsahu
  - Logovací preambule
- Registrace v GYM
  - Transparent linking
  - Původní multivirtualhost vyhodnocen jako linkfarma
  - Výsledná velikost – jedna doména, 10 aplikací
  - PHP



- Webové rozhraní, [clean\\_spiders.sh](http://clean_spiders.sh)

	OVERVIEW	SEARCH	DOWNLOADS	MAPPING	STATISTICS	CONFIG
<a href="#">← PREVIOUS ID</a> <a href="#">NEXT ID →</a>	<a href="#">← BACK TO SEARCH RESULTS</a>					
245853 /phpbb/viewtopic.php	189.110.240.166	NV32ts	2009-02-13 16:27:30		SQL	
	no referrer					
<a href="#">-&gt; map</a>						
<p><b>HTTP-GET Information:</b></p> <pre>f = 8 t = 21715\' and 1=2 union select CONCAT(0x27,0x7c,0x5f,0x7c),CONCAT(0x27,0x7c, 7,0x7c,0x5f,0x7c),CONCAT(0x27,0x7c,0x5f,0x7c) f,0x7c),CONCAT(0x27,0x7c,0x5f,0x7c),CONCAT(0x NCAT(0x27,0x7c,0x5f,0x7c),CONCAT(0x27,0x7c,0x 0x7c,0x5f,0x7c),CONCAT(0x27,0x7c,0x5f,0x7c),C 0x7c),CONCAT(0x27,0x7c,0x5f,0x7c),CONCAT(0x27 AT(0x27,0x7c,0x5f,0x7c),CONCAT(0x27,0x7c,0x5f 7c,0x5f,0x7c),CONCAT(0x27,0x7c,0x5f,0x7c),CON 7c),CONCAT(0x27,0x7c,0x5f,0x7c),CONCAT(0x27,C</pre>						
<p><b>HTTP-POST Information:</b></p>						
<p><b>HTTP-SERVER Information:</b></p> <pre>HTTP_USER_AGENT = NV32ts</pre>						
<p><b>Overall</b></p> <p>DESIUD select min(Creation) as mi, max(Creation) as ma from hitat_main_logs Time frame: 2009-07-21 22:00:00 - 2009-10-21 22:00:00 DESIUD select attackerIP, Creation, user_namecamp(Creation) as t, module from hitat_main_logs order by Creation desc limit 1 Last touch at: 2009-10-21 22:21:22 (See also: http://www.demonstrations.org) to phpbb Total count: 266602 Zeroed iper: 40</p> <p><b>Owncnet attackers for 30 days</b></p> <p>DESIUD select * from hitat_main_logs where user_namecamp(Creation)=1256459204 and (ipper BETWEEN 1217064226 AND 1217076991) OR (ipper BETWEEN 1245169205 AND 1245169207) OR (ipper BETWEEN 1245169208 AND 1245169210) OR (ipper BETWEEN 1245169211 AND 1245169213) OR (ipper BETWEEN 1245169214 AND 1245169216) OR (ipper BETWEEN 1245169217 AND 1245169219) OR (ipper BETWEEN 1245169220 AND 1245169222) OR (ipper BETWEEN 1245169223 AND 1245169225) OR (ipper BETWEEN 1245169226 AND 1245169228) OR (ipper BETWEEN 1245169229 AND 1245169231) OR (ipper BETWEEN 1245169232 AND 1245169234) OR (ipper BETWEEN 1245169235 AND 1245169237) OR (ipper BETWEEN 1245169238 AND 1245169240) OR (ipper BETWEEN 1245169241 AND 1245169243) OR (ipper BETWEEN 1245169244 AND 1245169246) OR (ipper BETWEEN 1245169247 AND 1245169249) OR (ipper BETWEEN 1245169250 AND 1245169252) OR (ipper BETWEEN 1245169253 AND 1245169255) OR (ipper BETWEEN 1245169256 AND 1245169258) OR (ipper BETWEEN 1245169259 AND 1245169261) OR (ipper BETWEEN 1245169262 AND 1245169264) OR (ipper BETWEEN 1245169265 AND 1245169267) OR (ipper BETWEEN 1245169268 AND 1245169270) OR (ipper BETWEEN 1245169271 AND 1245169273) OR (ipper BETWEEN 1245169274 AND 1245169276) OR (ipper BETWEEN 1245169277 AND 1245169279) OR (ipper BETWEEN 1245169280 AND 1245169282) OR (ipper BETWEEN 1245169283 AND 1245169285) OR (ipper BETWEEN 1245169286 AND 1245169288) OR (ipper BETWEEN 1245169289 AND 1245169291) OR (ipper BETWEEN 1245169292 AND 1245169294) OR (ipper BETWEEN 1245169295 AND 1245169297) OR (ipper BETWEEN 1245169298 AND 1245169300) OR (ipper BETWEEN 1245169301 AND 1245169303) OR (ipper BETWEEN 1245169304 AND 1245169306) OR (ipper BETWEEN 1245169307 AND 1245169309) OR (ipper BETWEEN 1245169310 AND 1245169312) OR (ipper BETWEEN 1245169313 AND 1245169315) OR (ipper BETWEEN 1245169316 AND 1245169318) OR (ipper BETWEEN 1245169319 AND 1245169321) OR (ipper BETWEEN 1245169322 AND 1245169324) OR (ipper BETWEEN 1245169325 AND 1245169327) OR (ipper BETWEEN 1245169328 AND 1245169330) OR (ipper BETWEEN 1245169331 AND 1245169333) OR (ipper BETWEEN 1245169334 AND 1245169336) OR (ipper BETWEEN 1245169337 AND 1245169339) OR (ipper BETWEEN 1245169340 AND 1245169342) OR (ipper BETWEEN 1245169343 AND 1245169345) OR (ipper BETWEEN 1245169346 AND 1245169348) OR (ipper BETWEEN 1245169349 AND 1245169351) OR (ipper BETWEEN 1245169352 AND 1245169354) OR (ipper BETWEEN 1245169355 AND 1245169357) OR (ipper BETWEEN 1245169358 AND 1245169360) OR (ipper BETWEEN 1245169361 AND 1245169363) OR (ipper BETWEEN 1245169364 AND 1245169366) OR (ipper BETWEEN 1245169367 AND 1245169369) OR (ipper BETWEEN 1245169370 AND 1245169372) OR (ipper BETWEEN 1245169373 AND 1245169375) OR (ipper BETWEEN 1245169376 AND 1245169378) OR (ipper BETWEEN 1245169379 AND 1245169381) OR (ipper BETWEEN 1245169382 AND 1245169384) OR (ipper BETWEEN 1245169385 AND 1245169387) OR (ipper BETWEEN 1245169388 AND 1245169390) OR (ipper BETWEEN 1245169391 AND 1245169393) OR (ipper BETWEEN 1245169394 AND 1245169396) OR (ipper BETWEEN 1245169397 AND 1245169399) OR (ipper BETWEEN 1245169400 AND 1245169402) OR (ipper BETWEEN 1245169403 AND 1245169405) OR (ipper BETWEEN 1245169406 AND 1245169408) OR (ipper BETWEEN 1245169409 AND 1245169411) OR (ipper BETWEEN 1245169412 AND 1245169414) OR (ipper BETWEEN 1245169415 AND 1245169417) OR (ipper BETWEEN 1245169418 AND 1245169420) OR (ipper BETWEEN 1245169421 AND 1245169423) OR (ipper BETWEEN 1245169424 AND 1245169426) OR (ipper BETWEEN 1245169427 AND 1245169429) OR (ipper BETWEEN 1245169430 AND 1245169432) OR (ipper BETWEEN 1245169433 AND 1245169435) OR (ipper BETWEEN 1245169436 AND 1245169438) OR (ipper BETWEEN 1245169439 AND 1245169441) OR (ipper BETWEEN 1245169442 AND 1245169444) OR (ipper BETWEEN 1245169445 AND 1245169447) OR (ipper BETWEEN 1245169448 AND 1245169450) OR (ipper BETWEEN 1245169451 AND 1245169453) OR (ipper BETWEEN 1245169454 AND 1245169456) OR (ipper BETWEEN 1245169457 AND 1245169459) OR (ipper BETWEEN 1245169460 AND 1245169462) OR (ipper BETWEEN 1245169463 AND 1245169465) OR (ipper BETWEEN 1245169466 AND 1245169468) OR (ipper BETWEEN 1245169469 AND 1245169471) OR (ipper BETWEEN 1245169472 AND 1245169474) OR (ipper BETWEEN 1245169475 AND 1245169477) OR (ipper BETWEEN 1245169478 AND 1245169480) OR (ipper BETWEEN 1245169481 AND 1245169483) OR (ipper BETWEEN 1245169484 AND 1245169486) OR (ipper BETWEEN 1245169487 AND 1245169489) OR (ipper BETWEEN 1245169490 AND 1245169492) OR (ipper BETWEEN 1245169493 AND 1245169495) OR (ipper BETWEEN 1245169496 AND 1245169498) OR (ipper BETWEEN 1245169499 AND 1245169501) OR (ipper BETWEEN 1245169502 AND 1245169504) OR (ipper BETWEEN 1245169505 AND 1245169507) OR (ipper BETWEEN 1245169508 AND 1245169510) OR (ipper BETWEEN 1245169511 AND 1245169513) OR (ipper BETWEEN 1245169514 AND 1245169</p>						



# HIHAT s nízkou interakcí

- Velikost: 1 doména, 10 php app, 24 instancí
  - phpBB, phpmyadmin, phpnuke, mambo, wordpress, ...
- Výsledky za období 07/08 – 05/09
- Celkem 147 130 útoků
- WEBnet/Cesnet2 0:0
- Pokračujeme

Detekovaný typ	Počet
Hádání hesla	135 691
RFI	7 047
Manager upload	1 628
SQL Injection	2 712
Directory traversal	48
Directory traversal + LFI	4
Ostatní	33 923
Útoků	147130
Celkem požadavků	181 053

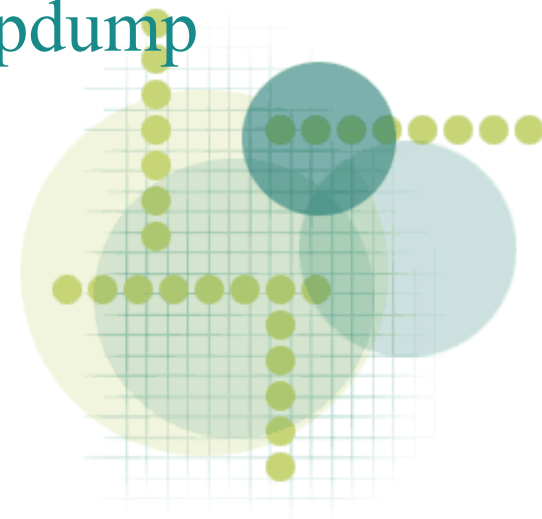
# J2EE HIHAT

- Nejen síť, Windows a PHP
- J2EE aplikační a webové servery
  - Tomcat – manager
  - JBoss – jmx-console
- Velikost: 150 IP, 2 aplikace
- Nelinkován do GYM



# J2EE HIHAT

- Za období 08/08 – 05/09
- Celkem 46 útočníků, 31 761 blind útoků
  - manager 46, jmx-console 0
  - WEBnet/Cesnet 0:0
- No GYM > čistá sada generických pokusů
  - HIHAT neumí multipart/form-data > tcpdump
  - FexShell – WinWorm
  - JShell/job – remote shell/admin
- Pokračujeme



# job

- Program Home
- File System
- System commands
- Database
- Configuration
- About program
- Exit

## Server Information

Server Name

Server port

OS

The current user name

The current user directory

The current user working directory

Procedures relative path

Program absolute path

Network Protocol

Server software version information

JDK version

JDK installation path

JAVA Virtual Machine version of the

JAVA Virtual Machine Name

JAVA class path

JAVA loaded library search path

JAVA temporary directory

JIT compiler name

Expansion of the directory path

## Client Inf

Client Address

Service machine name

Username

Request method

## 服务器信息

服务器名

服务器端口

操作系统

当前用户名

当前用户目录

当前用户工作目录

程序相对路径

程序绝对路径

网络协议

服务器软件版本信息

JDK版本

JDK安装路径

JAVA虚拟机版本

JAVA虚拟机名

JAVA类路径

JAVA载入库搜索路径

JAVA临时目录

JIT编译器名

扩展目录路径

## 客户端信息

客户机地址

服务器名

用户名

请求方式

应用安全套接字层

160.97.113.113.cz

80

Linux 2.6.21.7serv i386

prell

/prell

/opt/prell/webapps/portal

/prell/job3.jsp

/opt/prell/webapps/portal/job3.jsp

HTTP/1.1

Apache Tomcat/6.0.16

1.6.0\_06

/usr/lib/jvm/java-6-sun-1.6.0.06/jre

1.0

Java HotSpot(TM) Server VM

:/opt/prell/bin/bootstrap.jar

/usr/lib/jvm/java-6-sun-1.6.0.06/jre/lib  
/i386/server:/usr/lib/jvm/java-6-sun-  
1.6.0.06/jre/lib/i386:/usr/lib/jvm/java-  
6-sun-1.6.0.06/jre/..lib/i386:  
/opt/prell/product/10.2.0/client\_1  
lib:/opt/prell/product/10.2.0/client\_1  
/jdbc/lib:/usr/java/packages/lib/i386:  
/lib:/usr/lib

/opt/prell/temp

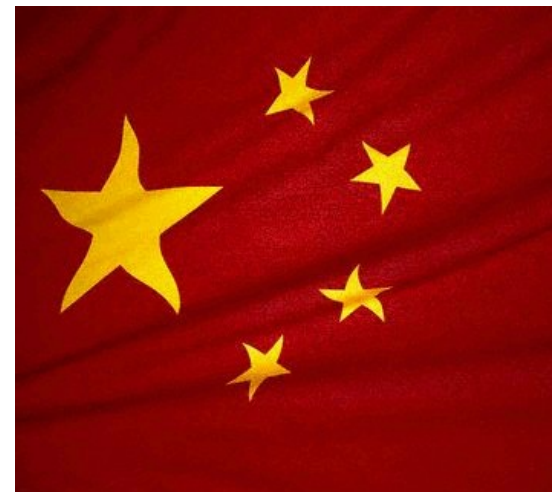
/usr/lib/jvm/java-6-sun-1.6.0.06/jre/lib  
/ext:/usr/java/packages/lib/ext

160.97.113

160.97.113

http

否





# Job vs r57

数据库连接类型

SQLServer数据库

数据库服务器地址

数据库服务器端口

数据库用户名

数据库密码

数据库名

Database

Database Connection Type

SQLServer Database

Database Server Address

Database server port

Database username

Database password

Database Name

SQLServer Database

MySQL Database

Oracle Database

DB2 Database

ODBC Data Source

Connection

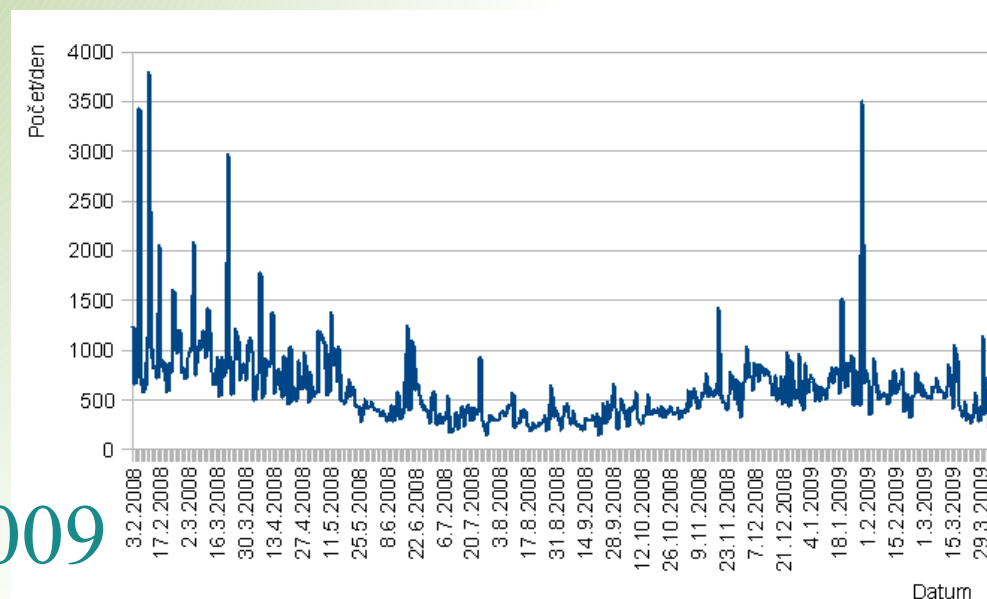
Reset

- Jscript
- Jdbc type 4
- Traceback

```
===== c1 =====string(1027)
<script language="javascript">
  hotlog_js="1.0";
  hotlog_r="" + math.random() + "&s=81606&im=1&r=" + escape(document.referrer) + "&pg=" + escape(
    document.cookie="hotlog=1; path=/";
    hotlog_r+="&c=" + (document.cookie?"y":"n");
  </script>
<script language="javascript1.1">
  hotlog_js="1.1";
  hotlog_r+="&j=" + (navigator.javaenabled()?"y":"n")
</script>
<script language="javascript1.2">
  hotlog_js="1.2";
  hotlog_r+="&wh=" + screen.width + 'x' + screen.height + "&px=" + ((navigator.appname.substr(0,4) == "MSI"
</script><script language="javascript1.3">
  hotlog_js="1.3"
</script>
<script language="javascript">
  hotlog_r+="&js="+hotlog_js;
  document.write("
    <a href='http://click.hotlog.ru/?81606' target='_top'>
    <img "+" src='http://hit4.hotlog.ru/cgi-bin/hotlog/count?"+hotlog_r+"&' border=0
    ")
  </script>
<noscript>
  <a href=http://click.hotlog.ru/?81606 target=_top>
  <imgsrc="http://hit4.hotlog.ru/cgi-bin/hotlog/count?s=81606&im=1" border=0width="1
</noscript>
```

# Apache RFI

- Nejen honeypoty
- Analýza logů produkčních 2 webserverů
- apache\_rfi.\*
  - Grep
  - Download
  - Report
- Za období 03/2008 – 03/2009
- Celkem 31 228 (WEBnet:0, Cesnet2:18 :)
- Získaných vzorků 5 234
- Pokračujeme, natrénovat podle J2EE HIHAT



# Apache RFI

```
FOUND RFI ATTACKER IN CESNET:
147.228.4.20 at 147.228.0.0/14:
 29/Oct/2009:12:16:37+0100 147.228.4.20
http://seminare.fav.zcu.cz/prehled-udalosti/1.atom
4b1505083da29e6e9d66bd29523ca0c6
GET/~bodik/atom/atom2rss.php?source=http://seminare.fav.zcu.cz/prehled-udalosti/1.atom
/var/log/apache2/access.log
```

```
FOUND RFI SCRIPT IN CESNET:
http://seminare.fav.zcu.cz/prehled-udalosti/1.atom at 147.228.0.0/14:
 29/Oct/2009:12:16:37+0100 147.228.4.20
http://seminare.fav.zcu.cz/prehled-udalosti/1.atom
4b1505083da29e6e9d66bd29523ca0c6
GET/~bodik/atom/atom2rss.php?source=http://seminare.fav.zcu.cz/prehled-udalosti/1.atom
/var/log/apache2/access.log
```

```
Total: 13 attackers
  1 in Cesnet
 94.236.23.242: 21
211.223.201.177: 15
 209.126.189.35: 10
  210.51.180.86: 9
  203.252.90.80: 5
 208.89.214.167: 4
   91.121.64.10: 4
 139.142.180.81: 3
 203.246.79.115: 3
  147.46.234.66: 3
212.115.201.232: 3
  147.228.4.20: 1
 189.41.71.127: 1
```

```
Total: 11 included URLs
  1 in Cesnet
31: http://www.koreadefence.net/data/shirohige/zfxid.txt??
15: http://photoworld.com.ua////zfxid1.txt?
9: http://nic.bupt.edu.cn/media/id1.txt??
6: http://www.museum-mputantular.com//AhoK/ip.txt???
5: http://www.kannunci.it/case/apache.jpg??
4: ftp://ftp.ikec.or.kr/pub/cmd22?
4: http://hana.nef-i.co.kr/pds/zfxid1.txt??
3: http://home.covenantberks.org/language/chi.txt??
3: http://www.daxx.net/recipe/baner.txt?
1: http://seminare.fav.zcu.cz/prehled-udalosti/1.atom
1: http://www.inaneponderings.com/plugins/system/ask.txt?
```

- `apache_rfi_report.sh`
- `fp`



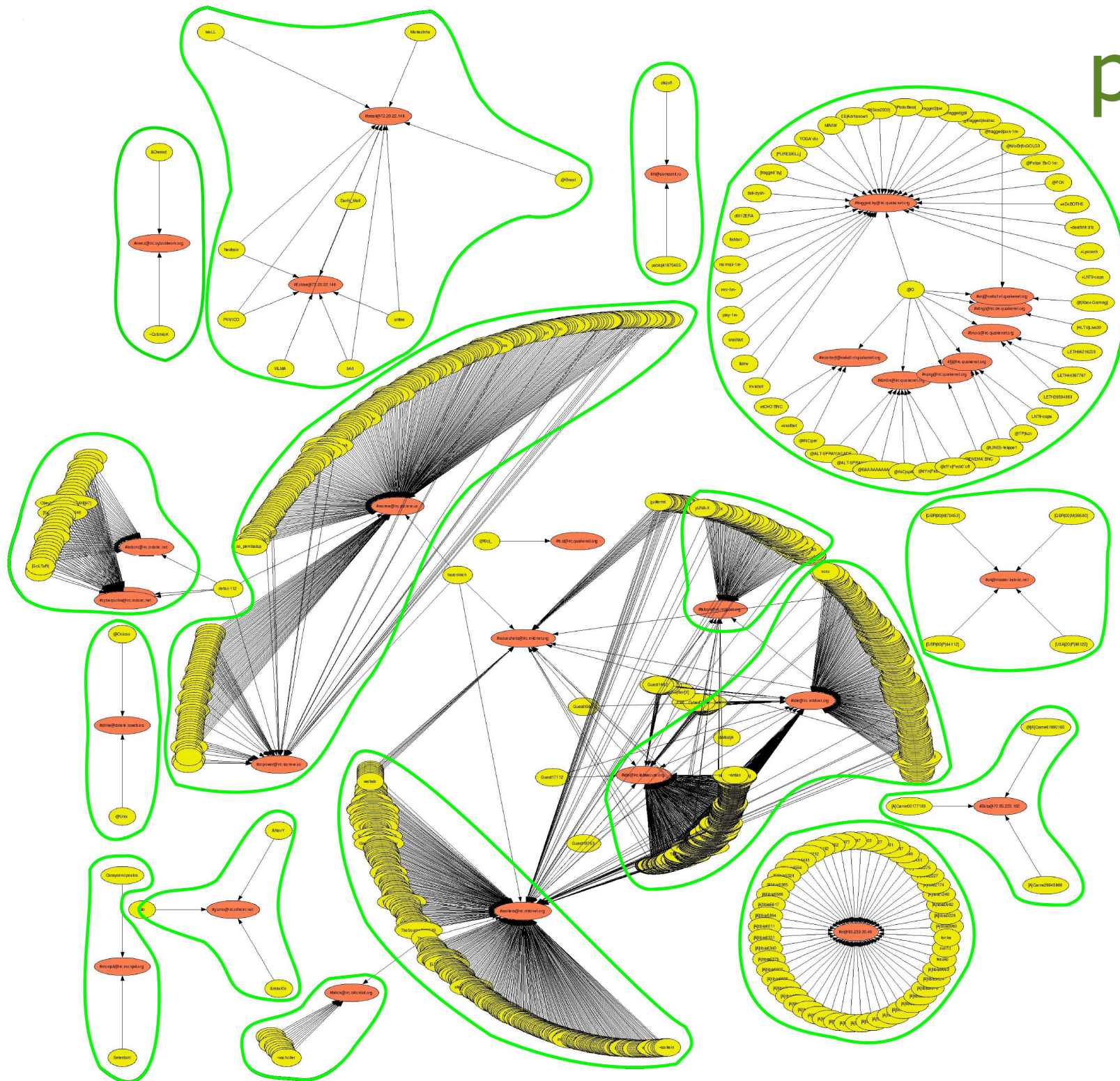
# Vzorky Apache RFI

- Vytrídili bayesovským klas.
  - dbacl + ruční korekce a třídy
  - Info, (Web | mail ) dropzone
  - Iframe injection
  - Backdoor tool
  - Bot exec
    - Pbot, pbotmap

Název kategorie	Počet vzorků
obfuscated	67
genericprobewithiframeinjection	14
iframe	25
frames	63
phpbot	3
perlbot	9
botexecplus	9
shellbot	34
pbot	523
botexec	201
exec	21
defacingtool	45
tools	34
c99	62
fileletool	70
r57	69
massmailer	122
genericprobe	610
maildrop	558
userfinger	100
safemode	75
dynamicprobes	57
staticprobes	29
genericprobewithmaildrop	20
webdrop	6
empty	3
error	4
misc	12
bin	13
404	15
rss	26
html	58
spam	2277
Celkem	5234

# pbotmap

- IRC
- graphviz
- 30 kanálů
- 1300 klientů
- Servery lžou

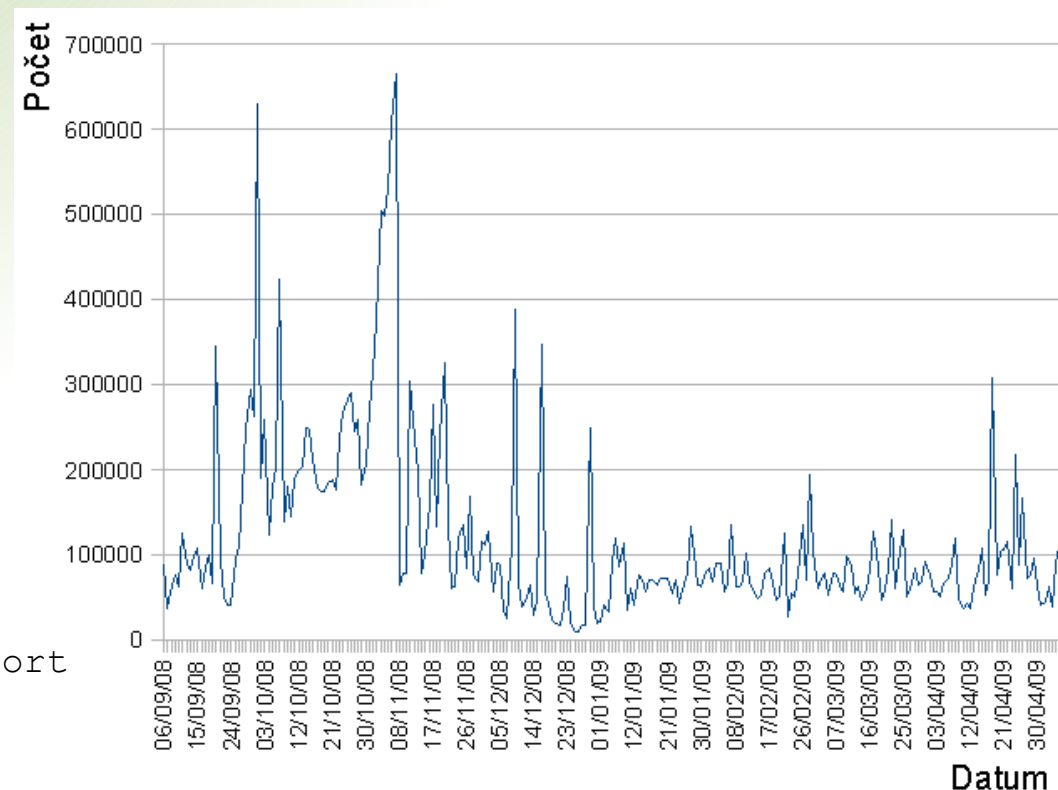




# Snort

- Snort – signaturový IDS
  - Množina signatur (snort + emergingthreats)
  - Nasazení na páteřní lince
    - Ztráty a výkon (100Eth vs DWDM)
    - Velikost DB
    - SSL
- BASE
- searchp2p.sh
- Pokračujeme doplňkově

```
ET MALWARE Suspicious 220 Banner on Local Port  
ATTACK-RESPONSES id check returned root
```





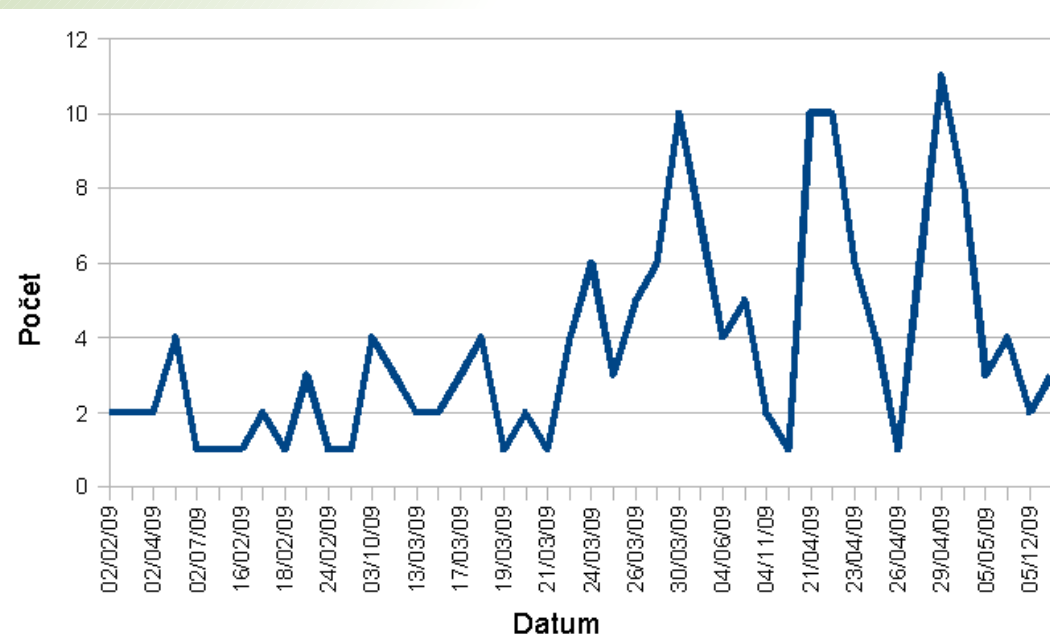
# PE Hunter

- Dynamický preprocesor pro Snort
- Ve streamech hledá PE soubory
  - Pro páteř potřebuje patch
- Za období 01/09 – 04/09
- Celkem 3 111 PE souborů
- Pouze 3 malware (ClamAV)
- Opustili jsme, umístíme na lepší místo



# spamsearch.pl

- Nejen honeypoty 2
- Analýza dat NetFlow
- SQL – počet spojení na 25/tcp
  - Více než 300 > report
- Za období 02/09 – 05/09
- WEBnet/Cesnet2 99:0
- Pokračujeme, rozšíříme (ssh, win,...)
  - Karanténa (walled garden)

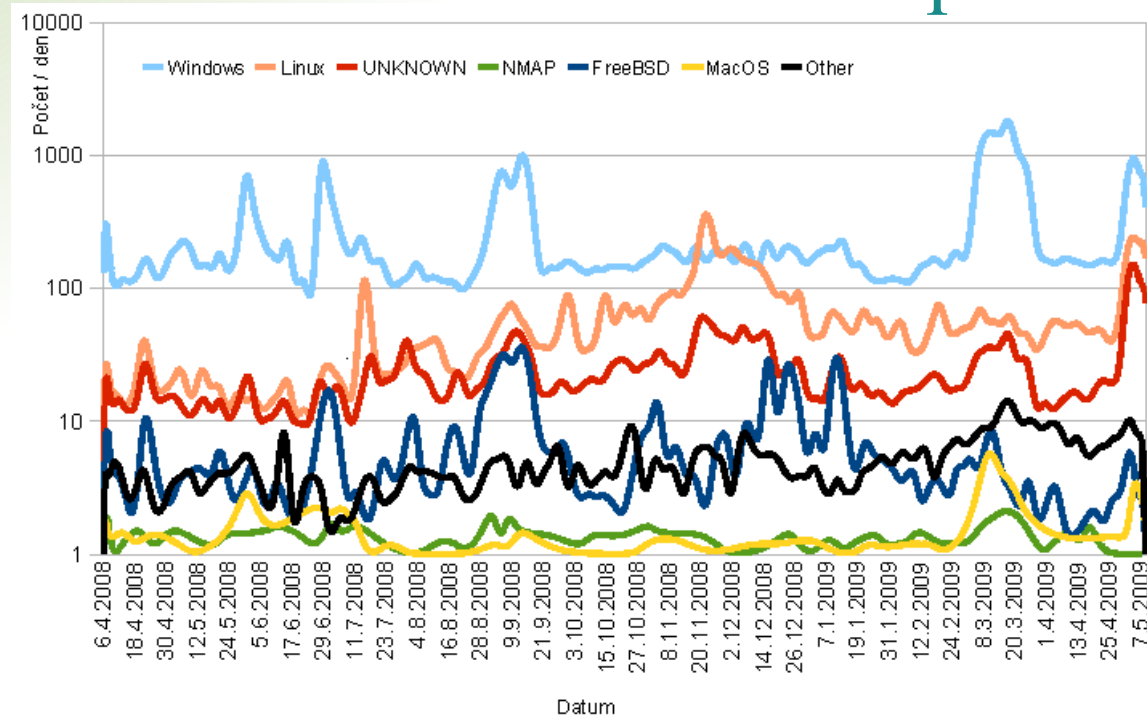


# Rekapitulace

- V provozu 5 IDS
  - Labrea, nepenthes, hihat, apache rfi, spamsearch.pl
  - Snort, p0f ?
  - PE Hunter, honeytrap

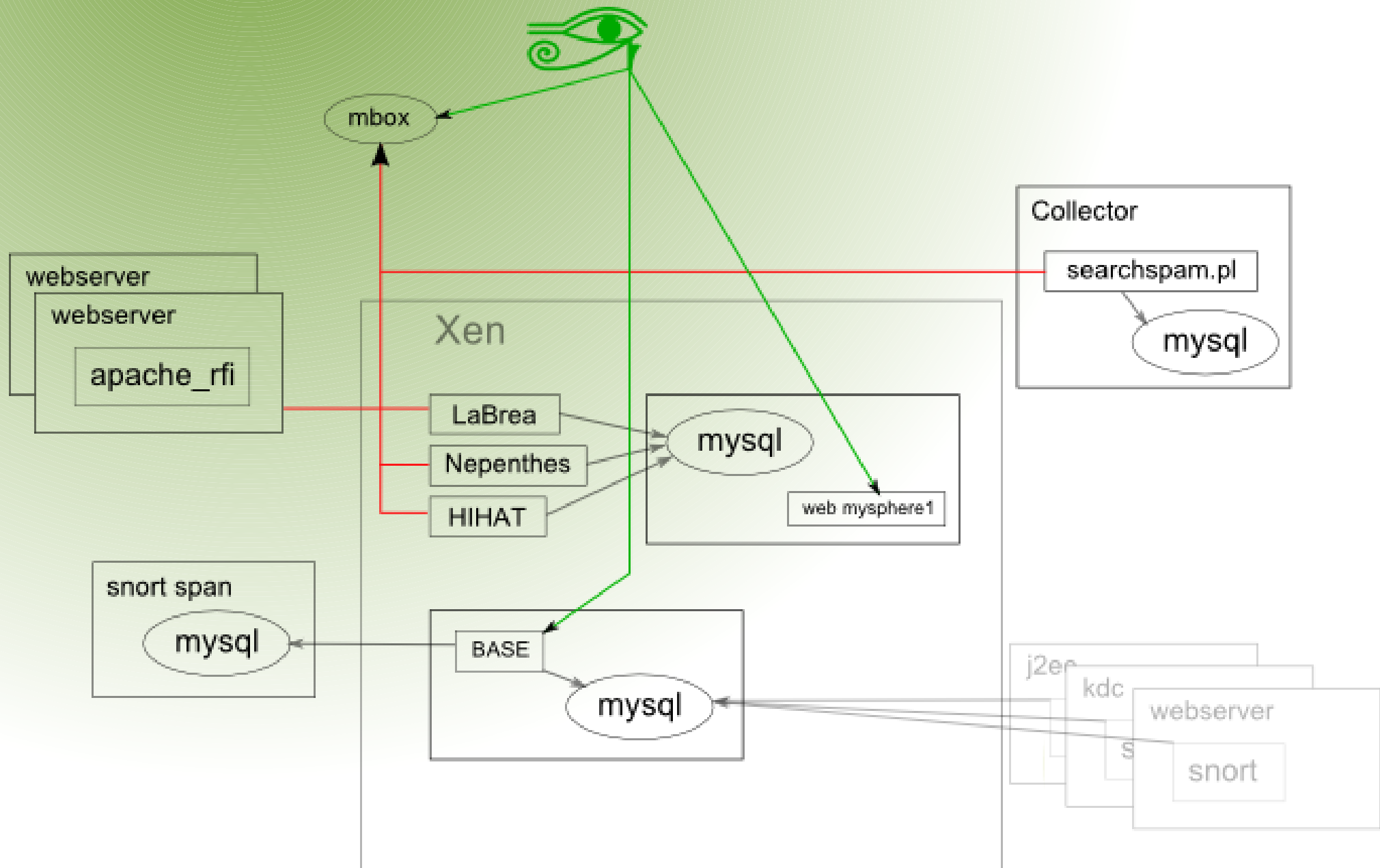
- Incidentů řešeno  
WEBnet:Cesnet2  
107:10

p0f





# Architektura



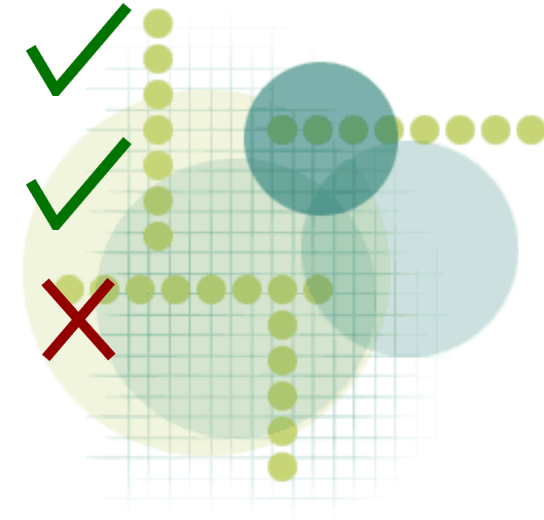
# Výstupy

- Nasazené systémy zapojeny do *incidentů WIRT*
- Prostředí pro další rozvoj – Xen server
- Data, skripty
- Publikace
  - Europen.cz – Buffer overflow
  - Europen.cz – Bezpečnost dnes v 7:00 ráno
  - BlackHat report (civ, cesnet csirt-forum)
- Knihy – Meziknihovní VS
- Řešené incidenty



# Dosažené cíle

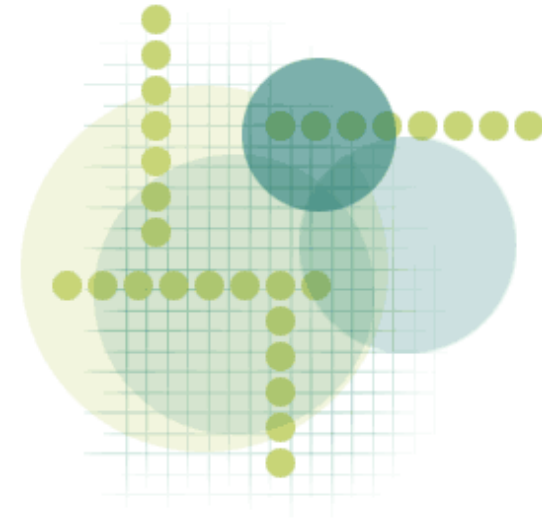
- Výchozí stav
  - snort, nepenthes
  - Bez reportingu, procesní reakce, znalostí
- Cílový stav
  - Získat znalosti (literatura, konference) ✓
  - Prostředky (Xen server) ✓
  - Provozně 2 – 3 systémy ✓
  - Reporting a reakce ✓
  - Výměna získaných dat ✓





# Plány

- Integrace (IDMEF)
- Centrální reporting i pohled
- Výměna dat (cesnet, dshield, honeynet)
- Vylepšení vyhledávání v NetFlow
  - sshsearch2.pl, winsearch.pl
- Automatické odpojování
- LaBrea IPv6
- Vizualizace (Conti ...)



# Závěr

- FR Cesnet č. 230/2007
- CIV, ZČU Plzeň
- Motivace
  - WIRT chtěl nástroj pro detekci napadených PC
  - Začít incidentům předcházet
- Cíle
  - Naučil se problematiku
  - Zlepšil stávající nástroje
  - Zvýšil bezpečnost sítě WEBnet



Radoslav Bodó <bodik@civ.zcu.cz>

Aleš Padrta <apadrta@civ.zcu.cz>



Otázky ? + ....