Experiences with IDS and Honeypots

Radoslav Bodó <bodik@civ.zcu.cz>

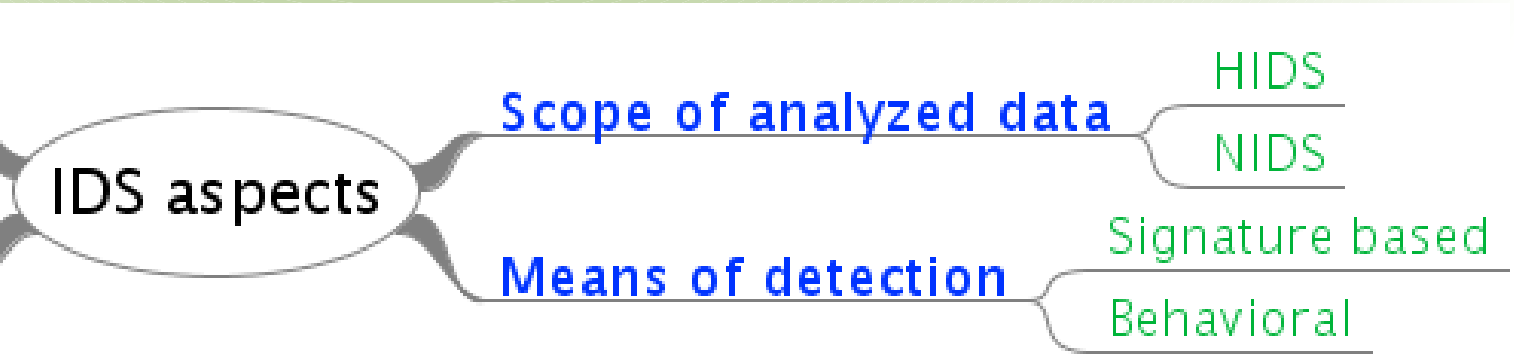
Michal Kostěnec <kostenec@civ.zcu.cz>

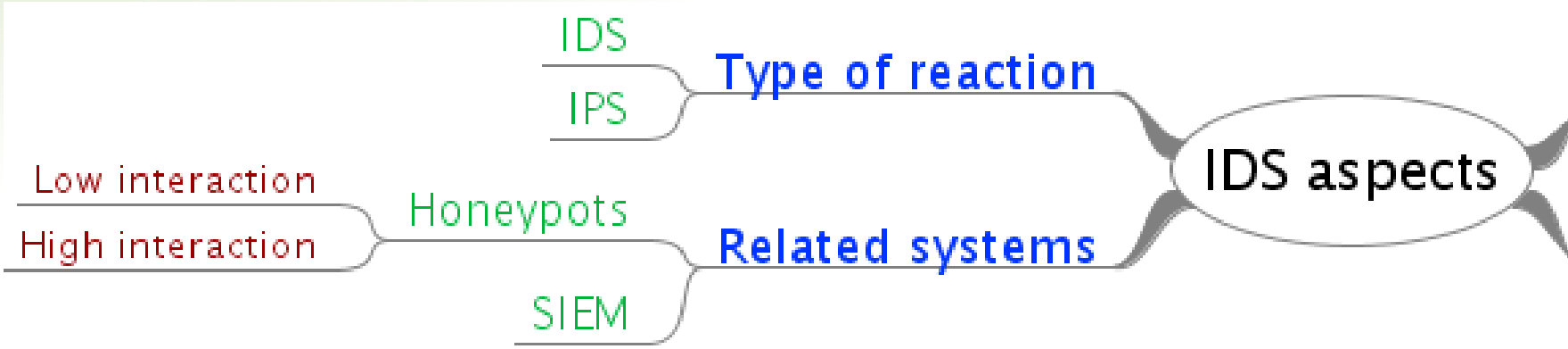
Agenda

- Intro
- 2008 – 2009 : Mysphere1
- 2010 : Other work
- 2011 : Mysphere2
- 2012 : Mysphere3 ?
- Trends
- Resume

Introduction

- What is IDS ?
  - A device or software application that monitors computing environment for malicious activities or policy violations





mysphere1

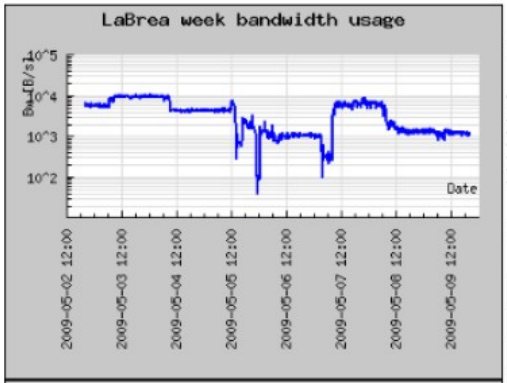
- Started at 2006
  - Labrea by Pavel Vachek (of CESNET)
- Several IDS were tested …
  - Working (actively used)
    - Labrea, Nepenthes, Netflow search, sshcrack.pl
  - Usefull (supplemental usage)
    - apache_rfi, Hihat, penetration tests
  - Abandoned
    - Google Hack Honeypot, PHP HOP, Snort, PE Hunter

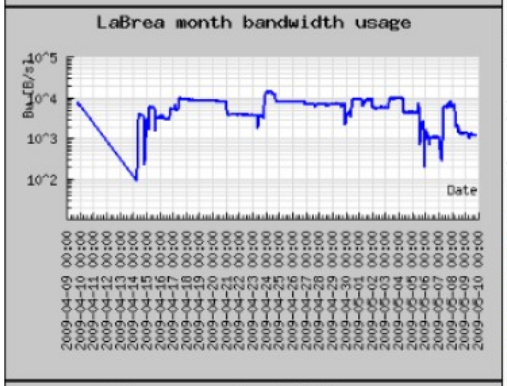
LaBrea

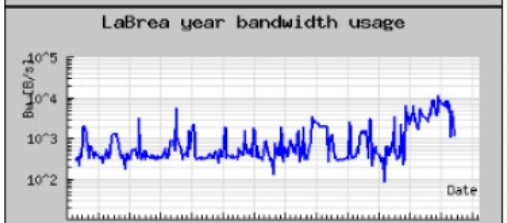
- Tarpit honeypot (cesnet-csirt)
  - Created as a reaction to CodeRed outbreak
- Labrea tries to slowdown the attack ...
  - Using TCP flow management options
    - Not finishing TCP handshakes
    - Advertises zero sized receiving window
  - Virus execution is slowed down by TCP stack, so virus can't attack elsewhere
- Log > Reporting

LaBrea

- Daily report (labrea_report.pl)
- Plots (labrea.loadup)







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	195.113.1[illegible]1	[illegible].166	3145	21705	1	[illegible].vvs-pv.cz
2009-04-27 00:16:29	5	146.102.2[illegible]2	[illegible].48	5042	1433	252	[illegible].vse.cz
2009-04-25 12:50:19	0	195.113.5[illegible]4	[illegible].128	3027	15854	1	[illegible].cuni.cz
2009-04-16 14:15:23	0	78.128.1[illegible]0	[illegible].183	2530	25724	1	[illegible]e.cuni.cz

Port trends

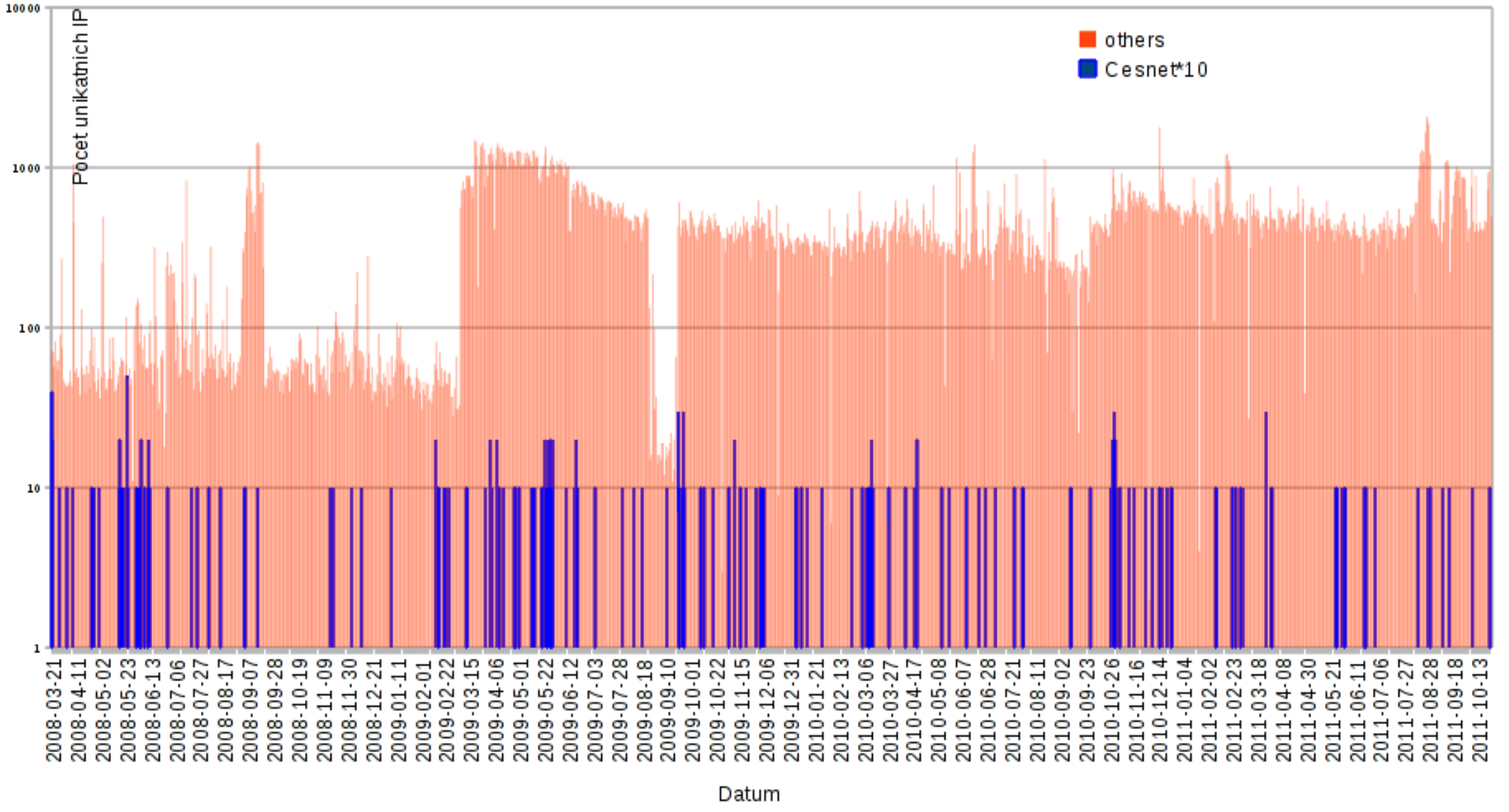
trend = count(dpst) - avg(last 72 hours)

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

```
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 tim


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
```

LaBrea

- Size: 252 addresses
- The results **for the period between 2008 and 2011**
  - 502 689 attackers in total (unique IPs/day)
  - **196 from CESNET** (in graph*10 !)



Nepenthes

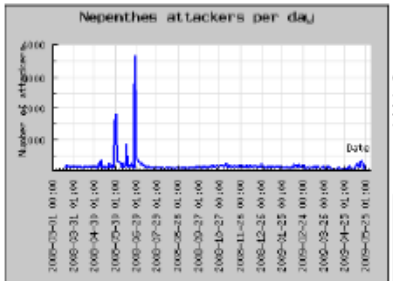
- … not only network intel
- Windows SMB emulator
    - Collecting propagated malware
- C++, problematic output
    - Debug log
    - Prelude IDS:
        - + IDMEF, Plugins, HIDS
        - – Python, DB, GUI
        - Not this time
    - SurfIDS:
        - – Plugins, PostgreSQL
- Neither suited our needs, so we created a custom output module

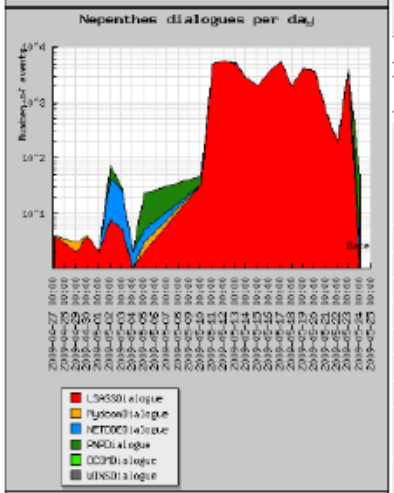
Nepenthes

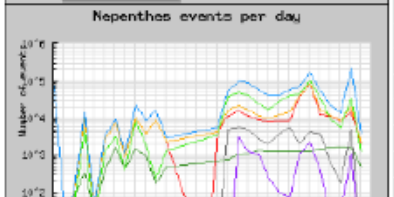
- Module log-grep | nepe_report2.pl

```
Total sessions: 14373
Total events: 60617
                EV_SOCK_TCP_RX: 23151
             EV_SOCK_TCP_CLOSE: 14068
            EV_SOCK_TCP_ACCEPT: 12346
                    EV_HEXDUMP: 4113
                  EV_DOWNLOAD: 1734
   EV_DIALOGUE_ASSIGN_AND_DONE: 1732
             EV_SHELLCODE_DONE: 1732
                    EV_SLAMMER:  869
                 EV_SOCK_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://1:1@58.77.97.100:55083/vPanel
-rw-r--r-- 1 nepe1 nepe1 105472 Nov 16  2008 /opt/nepe/var/binaries/5a0e0370ce40
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/5a0e0370ce40bd8
5a0e0370ce40bd8aa2c25b2a2e8b347e.virus-labels

SUBMISSION: 831f4ee0a7d2d1113c80033f8d6ac372 ftp://anonymous:bin@79.41.216.217:5
-rw-r--r-- 1 nepe1 nepe1 15872 Mar  4  2008 /opt/nepe/var/binaries/831f4ee0a7d2d
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/831f4ee0a7d2d11

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

SUBMISSION: e7801a316bb060178914ae9dbfd0078a ftp://1:1@89.136.110.154:63219/Tile
-rw-r--r-- 1 nepe1 nepe1 214016 Nov 16  2008 /opt/nepe/var/binaries/e7801a316bb0
http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/e7801a316bb0601
e7801a316bb060178914ae9dbfd0078a.virus-labels

Uniq hexdumps: 33
HEXDUMP: 0f7b92f524b404314c0b6cc6c3e76215:    1
-rw-r--r-- 1 nepe1 nepe1 613 Mar 22 19:47 /opt/nepe/var/hexdumps/0f7b92f524b4043
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>
```

- Plots







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.[redacted]0.67 ([redacted]zcu.cz)
Legend: Port rise Port fall Well-known port Registered port Dynamic/private/local port

Ownnet attackers for 30 days

time	hold	ips	ipd	psrc	pdst	count	tot_size	hostname
2009-05-20 02:07:33	4771	[redacted]3.215	[redacted]	4824	445	208	9152	[redacted]zcu.cz
2009-05-11 10:14:09	18800	[redacted]0.67	[redacted]	1977	445	81574	6719456	[redacted]zcu.cz
2009-05-04 13:04:30	685	[redacted].133	[redacted]	58676	3140	57635	734070	[redacted].cz
2009-05-04 12:19:45	77	[redacted].190	[redacted]	1169	21	22	588	[redacted].190

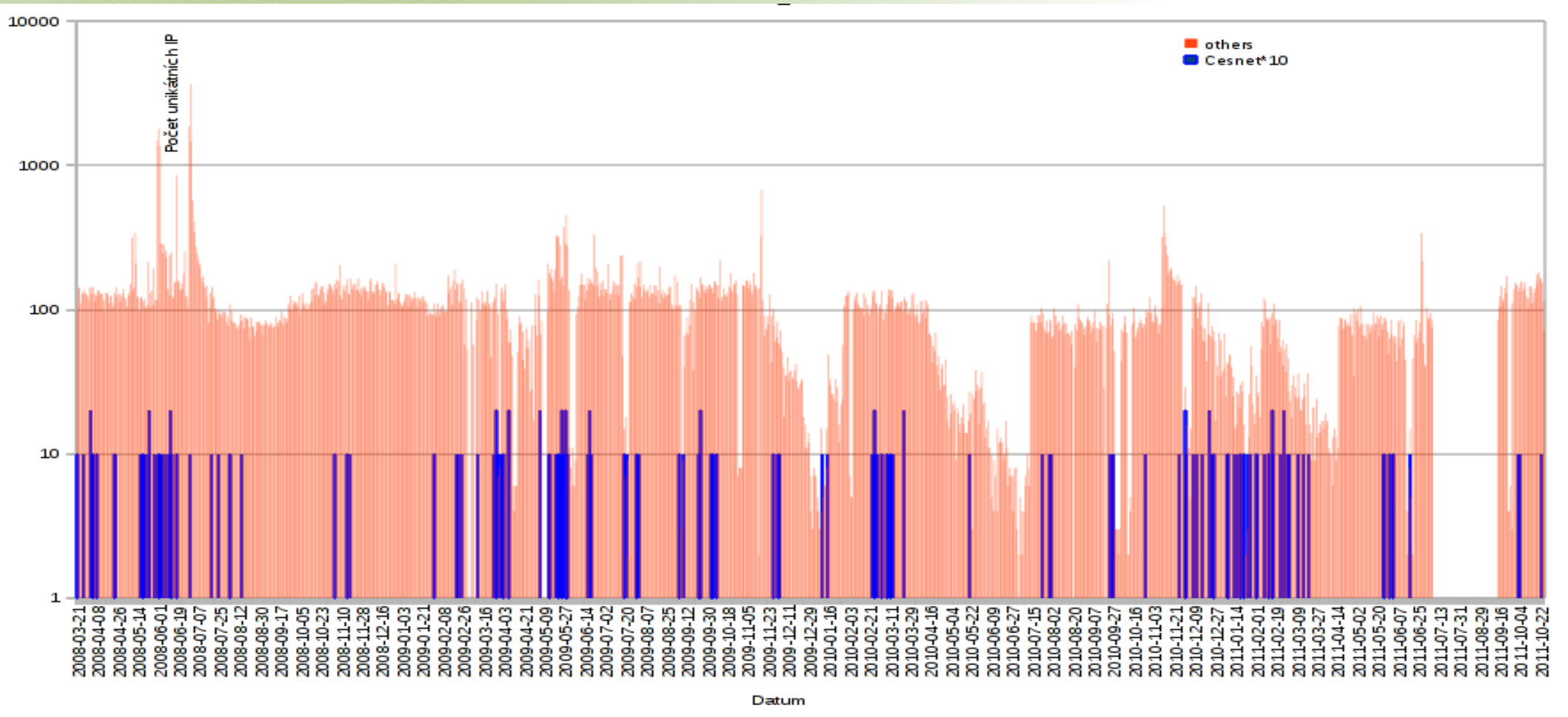
Port trends

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

pdst/name	count	count72	trendRatio
445/microsoft-ds	60145	77288	0.778
0/	8224	4940	1.665
1434/ms-sql-m	3624	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
9359/	875	0	875
28590/	875	0	875
27408/	870	0	870
39382/	866	0	866
39442/	865	0	865
139/netbios-ssn	0	3719	0

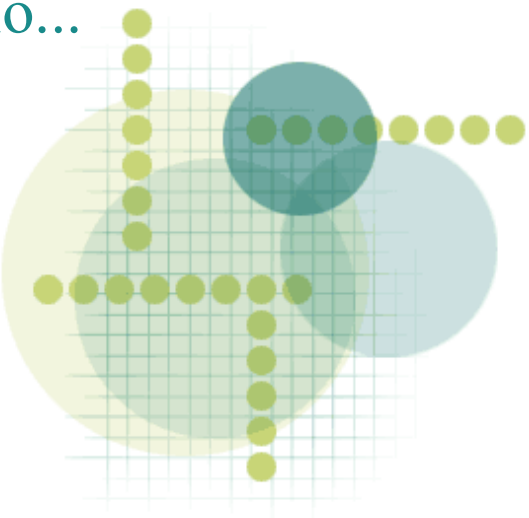
Nepenthes

- Size: 150 address
- The results **for the period 2008 – 2011**
  - 128 372 attackers in total (unique IPs/day)
  - **160 from CESNET** (in graph *10 !)
  - 580 malware samples captures; but we aren't analysing them any further. Project is old and deprecated in favor of Dionaea ...



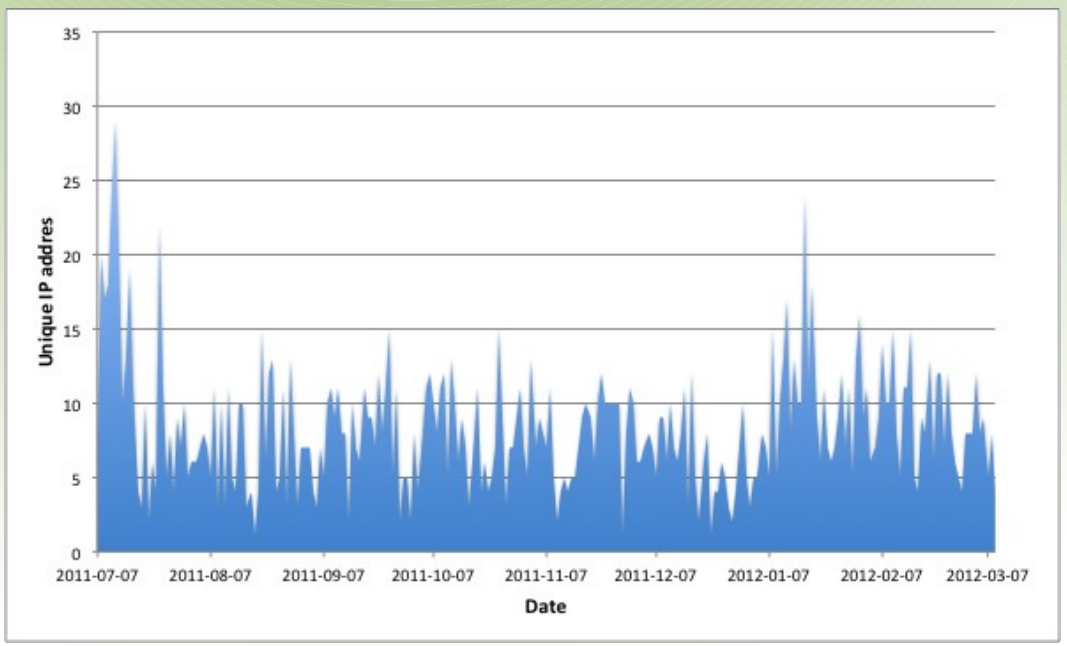
Dionaea

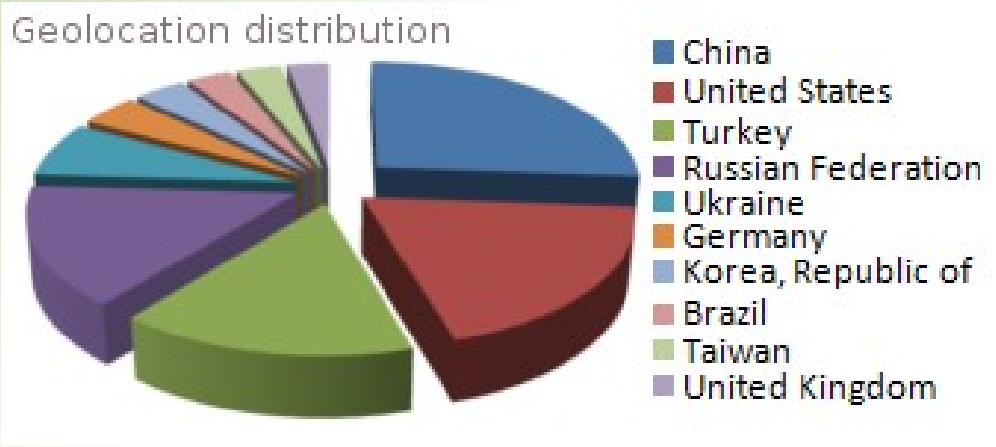
- Service emulator written in Python
  - Nepenthes's successor
  - SMB, HTTP/S, FTP, TFTP, MSSQL, MySQL, SIP
  - IPv6
  - Enhanced shellcode emulation – libemu
    - Syscalls logging, networking and file io...
  - Threaded
  - SQLite database

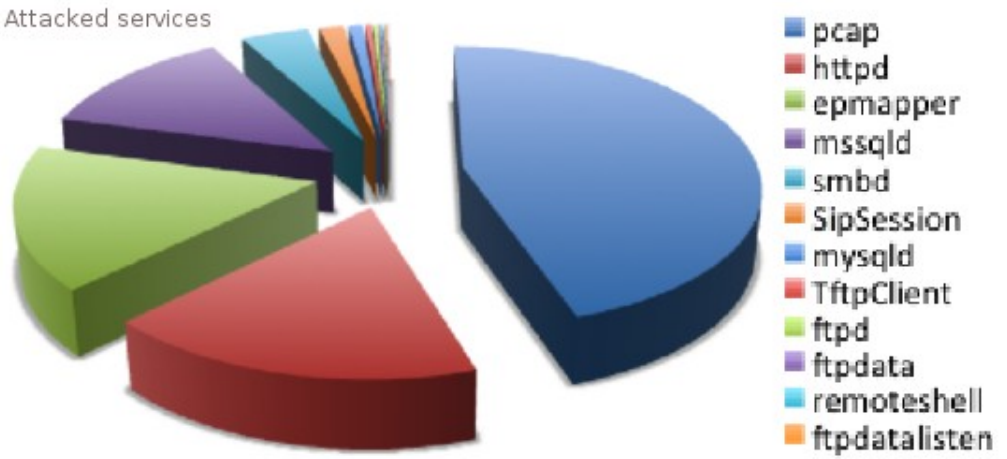


Dionaea

- Size: 1 address
- The results **for the period 2011 – 2012**
  - 6 246 attackers in total (unique IPs/day)
  - **1 from Cesnet** (in graph *10 !)

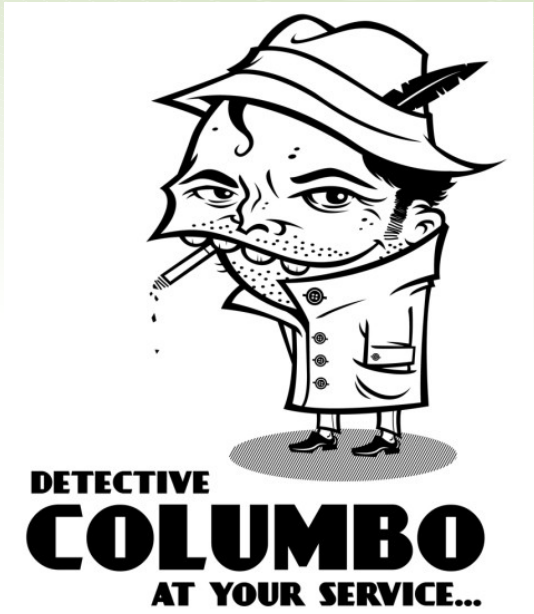






NetFlow search

- But if you don't want to bother with installing some weird piece of software and waste your address space ...
  - Netflow data analysis – any site in Géant network has already some data about a traffic flows
- SQL – **SELECT sip ... WHERE dp=25 GROUP BY sip HAVING conns > 300**
  - spamsearch, sshsearch, winsearch
  - Dnssearch ?
- **Most efficient sensor !**



od Cron Daemon

předmět Cron <bodik@...> time (date; /home/bodik/winsearch2.pl; echo; /home/bodik/spamsearch2.pl; echo; /home/bodik/sshsearch2.pl; echo; /home/bodik/websearch2.pl; echo; /home/bodik/dnssearch.pl; echo; /home/bodik/hlidani_zdroju_knihovny.pl; date)

komu bodik@civ.zcu.cz, Ing. Aleš Padrta Ph.D.

Thu Sep 22 ... CEST 2011

/home/bodik/winsearch2.pl

Time	sum(bytes)	sum(pck)	sip	hostname	conns	tgts
2011-09-22 ...:00	455168	9483	147.228.94.110	el304n01-ket.fel.zcu.cz	4193	4187
2011-09-22 ...:00	657102	12367	147.228.181.102	eduroam-n358.zcu.cz	1012	2
2011-09-22 ...:00	86800	1713	147.228.183.85	eduroam-n853.zcu.cz	581	1
2011-09-22 ...:00	1966240	9645	147.228.99.50	kiosek-ng01.zcu.cz	452	2
2011-09-22 ...:00	1837402	8856	147.228.153.38	kiosek-vc02.zcu.cz	354	2
2011-09-22 ...:00	1505253	6881	147.228.20.103	ps203p14-uk.uk.zcu.cz	352	2
2011-09-22 ...:00	39115	724	147.228.182.114	eduroam-n626.zcu.cz	304	2

/home/bodik/spamsearch2.pl

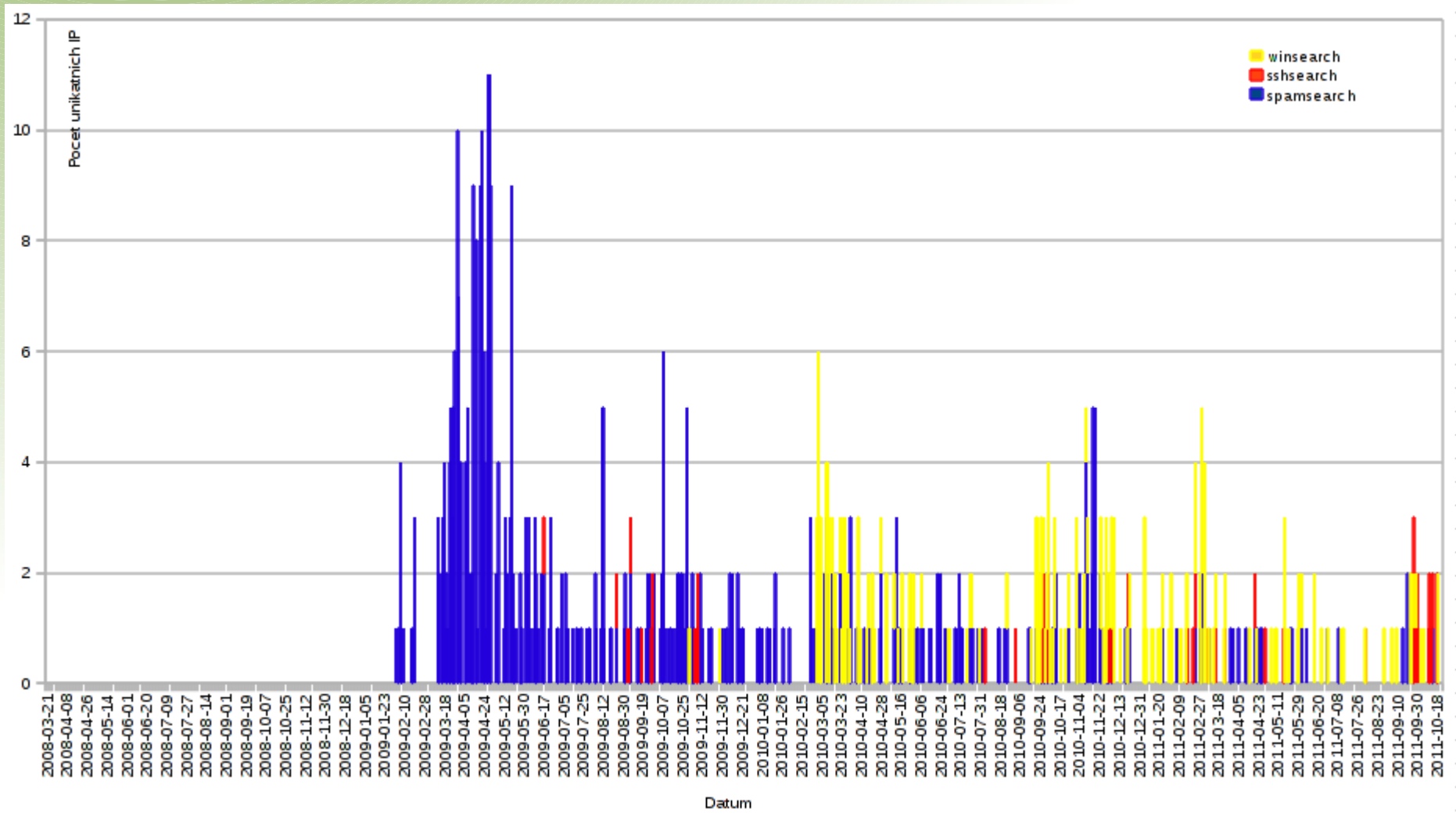
Time	sum(bytes)	sum(pck)	sip	hostname	conns	tgts
2011-09-22 00:...	994109	18477	147.228....	...zcu.cz	1583	1
2011-09-22 00:...	1027734	8043	147.228.19.150	sd206p03-kfi.ff.zcu.cz	564	1
2011-09-22 00:...	939549	4585	147.228....	...zcu.cz	511	1

/home/bodik/sshsearch2.pl

Time	sum(bytes)	sum(pck)	sip	hostname	conns	tgts
2011-09-22 00:...	47513710	117800	147.228....	...zcu.cz	1742	4
2011-09-22 00:...	1507730	10200	147.228....	...zcu.cz	1174	5
2011-09-22 00:...	172920	2882	147.228....	...zcu.cz	548	1
2011-09-22 00:...	9039369	169451	147....	...zcu.cz	507	151
2011-09-22 00:...	3354621	67449	147.228....	...zcu.cz	373	20
2011-09-22 00:...	244282	3863	147.228....	...zcu.cz	341	3
2011-09-22 15:...	1015433	7279	147.228....	...zcu.cz	198	1
2011-09-22 00:...	36697255	195889	147.228.101.109	ui322p01-sis.civ.zcu.cz	149	6
2011-09-22 00:...	463808	2658	147.228.43.85	...zcu.cz	140	1
2011-09-22 11:00:...	49424	839	147.228.185.92	zcu-mobile-n348.zcu.cz	117	99
2011-09-22 ...:...	45228774	850891	147.228.209.162	...zcu.cz	114	9
2011-09-22 00:...	3864785	48700	147.228....	...zcu.cz	109	15

NetFlow search

- In the period 2009 – 2011 there were
  - 515 Spam, 47 ssh, 195 winworm found in WEBnet
    - Graph shows detection rate, not incident count

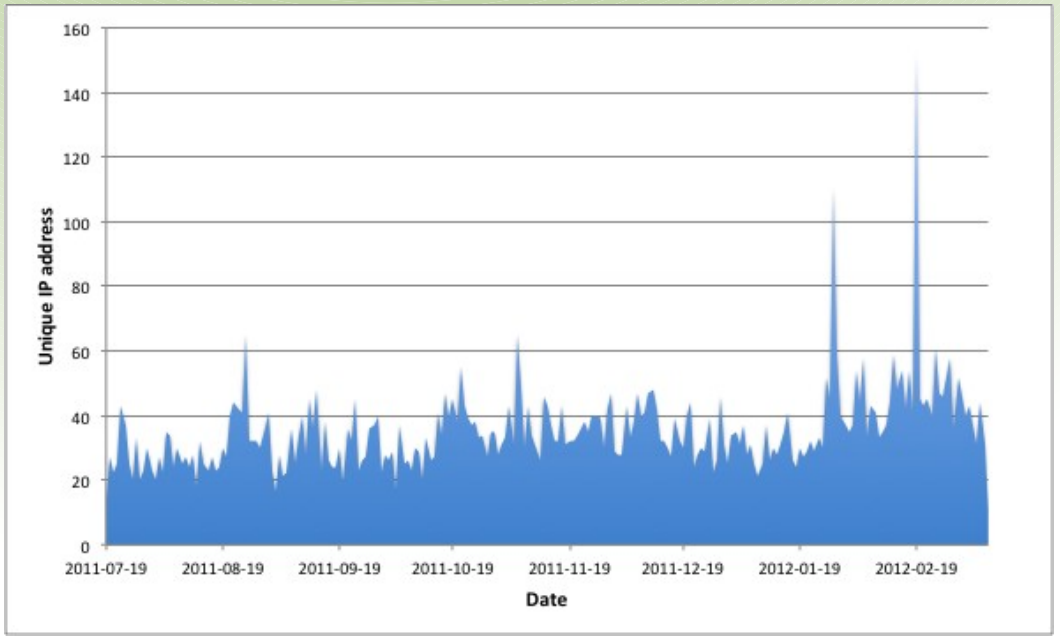


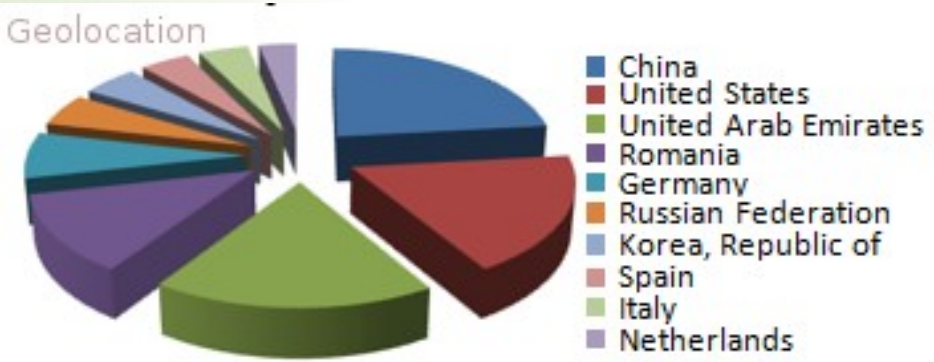
Kipo

- You can also be more more creative on ssh ...
- Kipo is a medium interaction honeypot written in Python
  - Python >> multiplatform
    - Linux, FreeBSD, Windows
  - Customizable Linux shell emulator
    - Static responses in .txt (`ifconfig, dmesg`)
    - Dynamic commands .py (`ping, wget, ...`)

Kipo

- Size: 1 address
- The results **for the period 06/2011 – 02/2012**
  - 1 503 attackers in total (unique Ips/day)
    - 130 malware samples (wget downloads)
  - **None of CESNET**





- 130 malware samples collected (wget downloads)
  - Some of them are really nice ;)
  - Why to bother about rootkits, stealing credentials .. they want to play CounterStrike ...

Kipo malware

```
~/gn3/brno/kipocases/1/redirect
.
├── core_i386.so
├── cstrike
├── debug.cmds
├── debug.log
├── engine_amd.so
├── engine_i486.so
├── engine_i686.so
├── filesystem_stdio_i386.so
├── hlds_amd
├── hlds_i486
├── hlds_i686
├── hlds_run
├── hldsupdatetool.bin
├── InstallRecord.blob
├── libsteam_api_c_linux.so
├── libsteam_api_c.so
├── libsteamvalidateuseridtickets
├── libsteamvalidateuseridtickets
├── libtier0_s.so
├── libvstdlib_s.so
├── linuxreadme.txt
├── platform
├── proxy_i386.so
├── readme.txt
├── reslists
├── SAVE
├── start
├── steam
├── steam_appid.txt
├── steamclient.so
├── stop
├── test1.so
├── test2.so
├── test3.so
└── valve
```

```
BARA="\033[1;34m==========================================================
COPY=" - redirect [csservers.ro] [linux ver "$RED"1.2"$NC"]"
REGULI=" - numar maxim redirecte: "$RED"15"$NC

if [$ip_extern = ""]; then
ip[redacted] -O-  http://www.csservers.ro/ip.php| awk '{gsub(/.*Current IP Add
else
ip_extern=`wget -q -O-  http://checkip.dyndns.com/| awk '{gsub(/.*Current IP Address
fi

#ip_extern=192.168.0.1 (inlocuiti 192.168.0.1 cu alt ip extern , stergeti textul ace

echo -e $BARA;
echo -e $COPY;
echo -e $REGULI;
echo -e $BARA;
echo -e $NC' ip extern: '$CYAN$ip_extern
echo -ne $NC' dns server: '$CYAN
read dns_server
echo -e '\n\t'$NC'('$CYAN'clasic'$NC','$CYAN'respawn'$NC','$CYAN'hidenseek'$NC','$CY
echo -ne $NC' mod: '$CYAN
read mod
echo -ne $NC' nume admin: '$CYAN
read nume_admin
echo -ne $NC' numar redirecte: '$CYAN
read NR_RED
echo -ne $NC

echo -e $RED"\n Pornesc redirectele \n"$NC

COUNTER=0;
        harta=`wget -q -O- http://www.csservers.ro/harta.php?asdfg=$mod/$COUNTER`
        hostname=`wget -q -O- http://www.csservers.ro/mod.php?qwerty=$mod/$dns_serve
        screen -d -m ./hlds_run -game cstrike +ip $ip_extern +maxplayers 22 +map $ha
echo -[redacted] [am pornit redirectul '$COUNTER'] '$NC' \n\t\t num
sleep 1;

port='29000';

COUNTER=1;
while [ $COUNTER -lt $NR_RED ]; do
        harta=`wget -q -O- http://www.csservers.ro/harta.php?asdfg=$mod/$COUNTER`
        hostname=`wget -q -O- http://www.csservers.ro/mod.php?qwerty=$mod/$dns_serve
        screen -d -m ./hlds_run -game cstrike +ip $ip_extern +maxplayers 22 +map $ha
```

- Fully outsourced distributed gaming cloud service ?

Kipo malware

CSSERVERS

LISTA SERVERELOR COUNTER STRIKE 1.6 DIN ROMANIA

- 1596 servere active
- [redacted] cele mai multe de cs.bretonia.ro
- 49401 redirectati pana la ora 16:37:35
- 82364 redirectati ieri
- Castigatori dropuri pentru azi: bb.godplay.ro , locul 2: dr2.godplay.r
- 21075 jucatori online pe toate serverele la ora 16:37:35

STA SERVERE | ADAUGA SERVER | EVIDENTA REDIRECTELOR LIVE | FORUM | CUMPARA COMPONENTE | CASTIGA DROPURI | MASTER

REDIRECTE CS PENTRU TOATE SERVERELE DIN ROMANIA

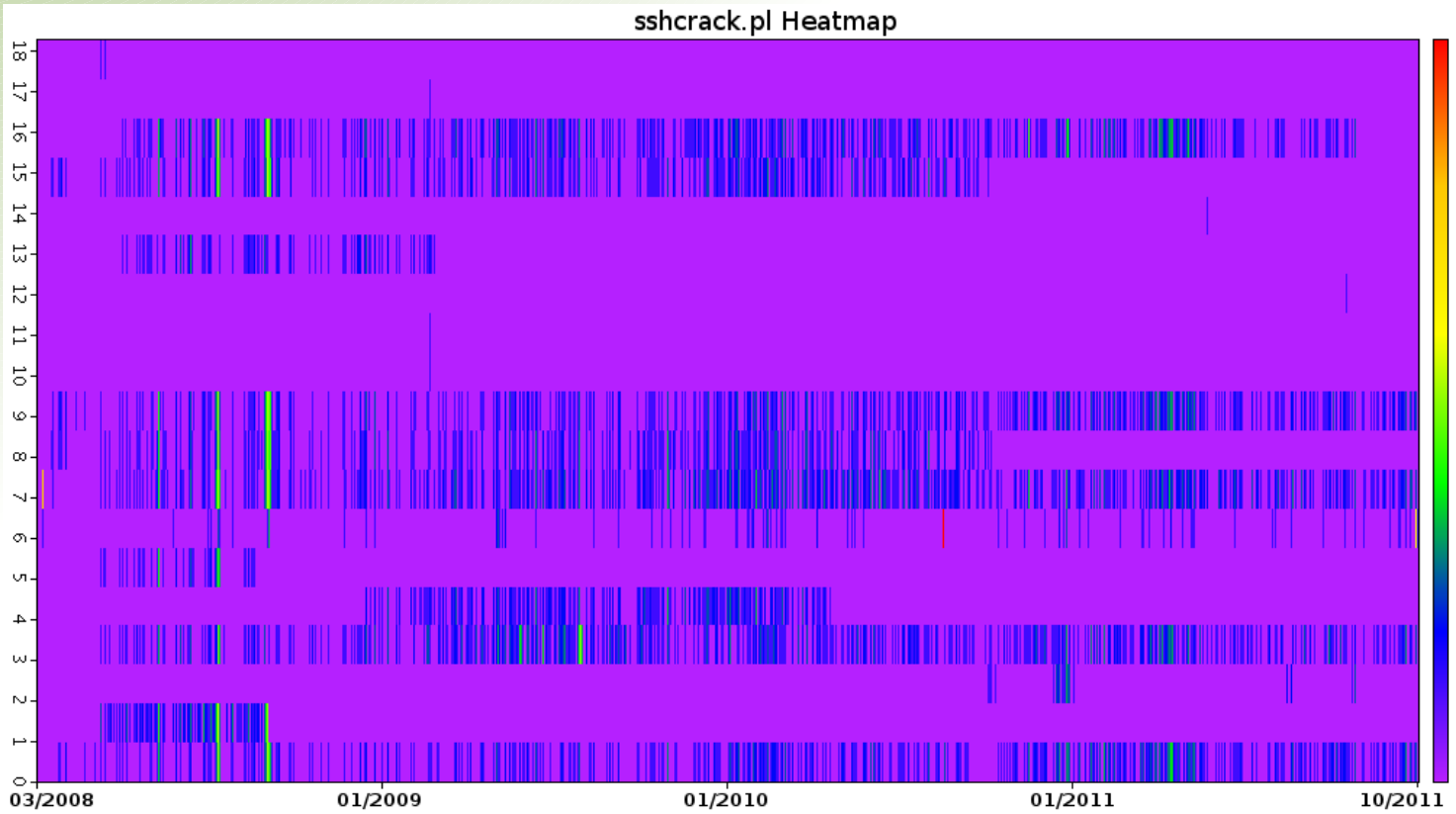
server | harta | toate modurile | filtreaza

Vrei lista asta de servere (FARA REDIRECTE) la tine in Counter Strike ? Click AICI sa ti-o instalezi !

	STATUS	DNS SERVER	JUCATORI	HARTA	MOD	RATING
1	SERVER FULL	pgl.indungi.ro	32:32	cs_italy	clasic	100%
2	SERVER FULL	cs.theonecs.ro	32:32	de_abaddon	clasic	100%
3	SERVER FULL	babilonia.indungi.ro	32:32	de_kabul_32	clasic	100%
4	SERVER FULL	cs.indungi.ro	32:32	de_westwood_newstyle	clasic	100%
5	SERVER FULL	constanta.indungi.ro	32:32	de_westwood	clasic	100%
6	SERVER FULL	dn7.onlypro.ro	32:32	de_inferno	clasic	100%
7	SERVER FULL	cs.alphacs.ro	32:32	de_westwood_big	clasic	100%

sshcrack.pl

- Just not let them in …
- Perl grep auth.log + cron + iptables
  - Autonomous self-defense
  - No monitoring, no development, no problems
    - /afs/zcu.cz/common/tools/sshcrack/sshcrack.pl
    - fail2ban

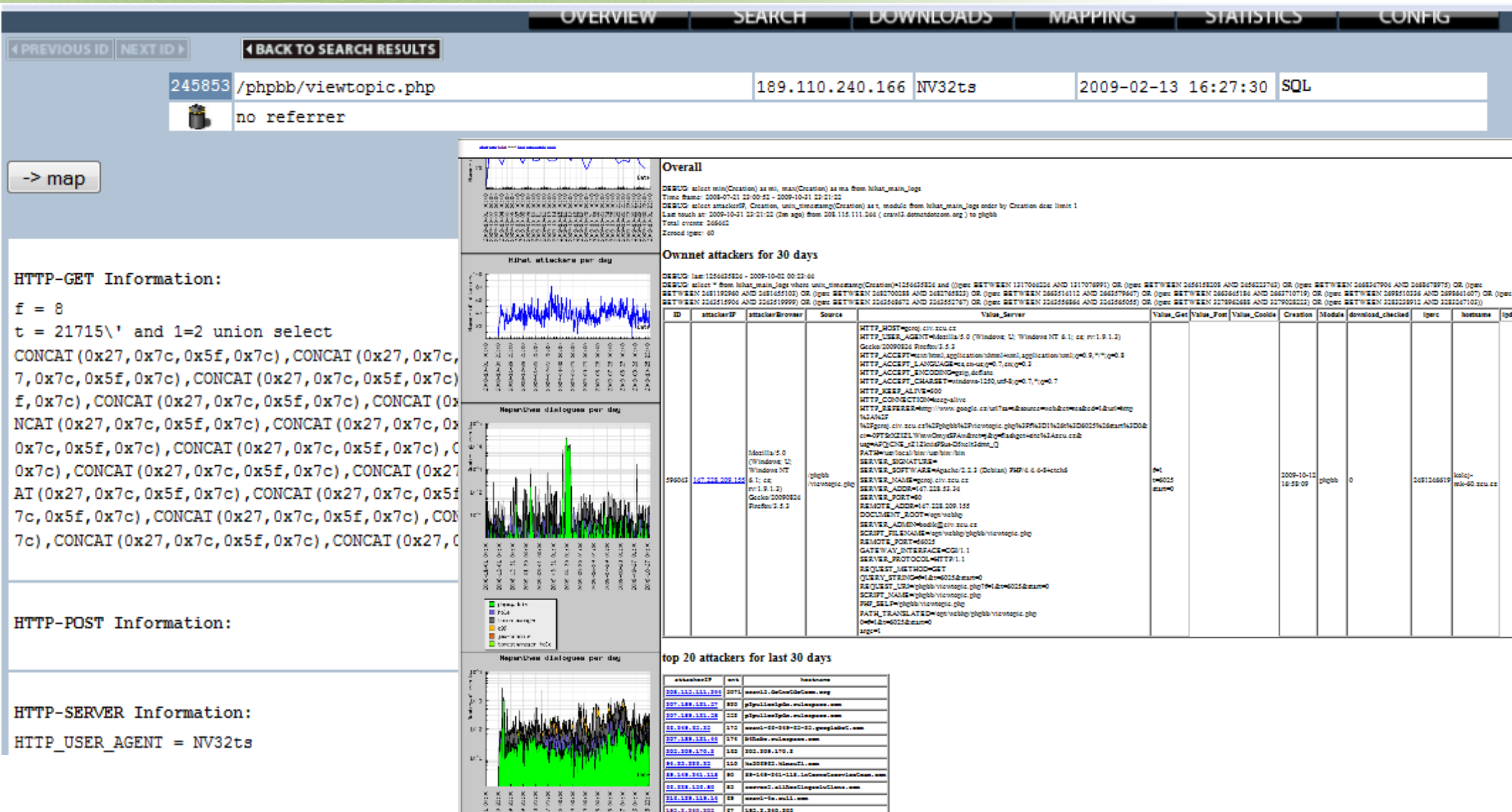


Mysphere1: Usefull IDS

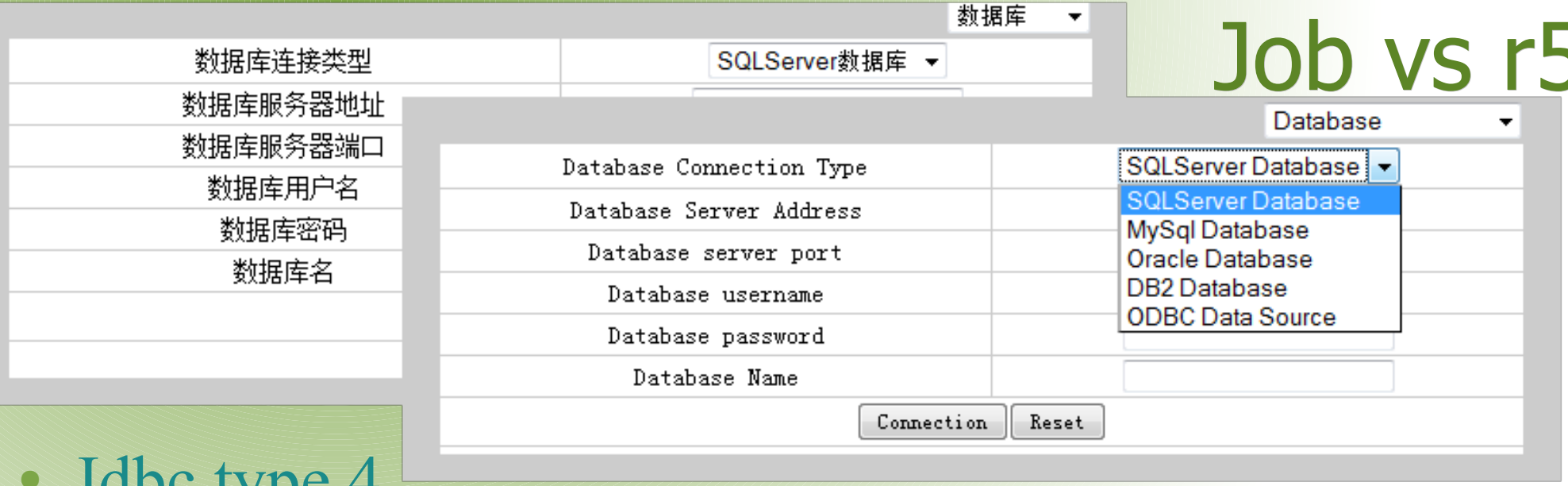
- We were also interrested in web malware ...
  - HIHAT
    - Tool for creating low and high interaction web based honeypots from any application
    - Logging preambule is inserted in every script/entry point and records all properties of the HTTP requests
    - cca 10x PHP apps, 2x J2EE apps

HIHAT – low interaction honeypot

- Web interface
- clean_spiders.sh (never ending story ...)



Job vs r57



- 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="+es
    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.subs
</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
    ")
</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=
</noscript>"
```

- IDS also has their vulnerabilities, especially those with high interaction
- Dionaea HTTPD directory traversal
  >> EFF SSL Observatory

2010 post mysphere1

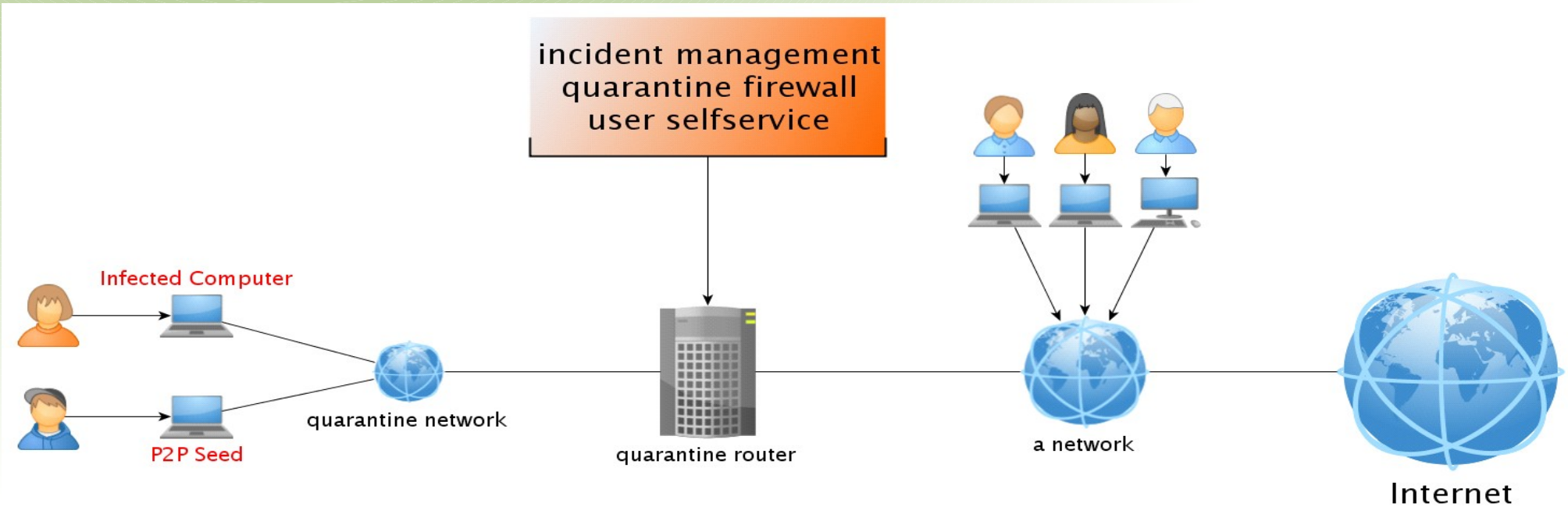
- Mysphere1 works …
  - Students always brings an infected devices ...
    - … and they'r detected.
      - More incidents ...
        - More work … oh my

2011 – mysphere2

- Mysphere2: Improving the process of security incidents response
  - Development fund Cesnet no. 369 + civ.zcu.cz
  - Design and implement a *network orchestrator*
    - Automated blocking of computers in campus and locking users in eduroam
    - Don't disconnect them completely, but provide them with proper informations and tools for incident response
      - Jan Goebel, Jens Hektor, Thorsten Holz: Advanced honeypot-based intrusion detection ;login: v.31 n.6 http://www.usenix.org/publications/login/
    - Link every information about an incident with Request Tracker and other internal agendas ...

Mysphere2 vs User

- So we created
  - Quarantine network and it's management tool (NetSpy)
    - NetSpy switches access ports vlans
  - Captive portal on router from that network

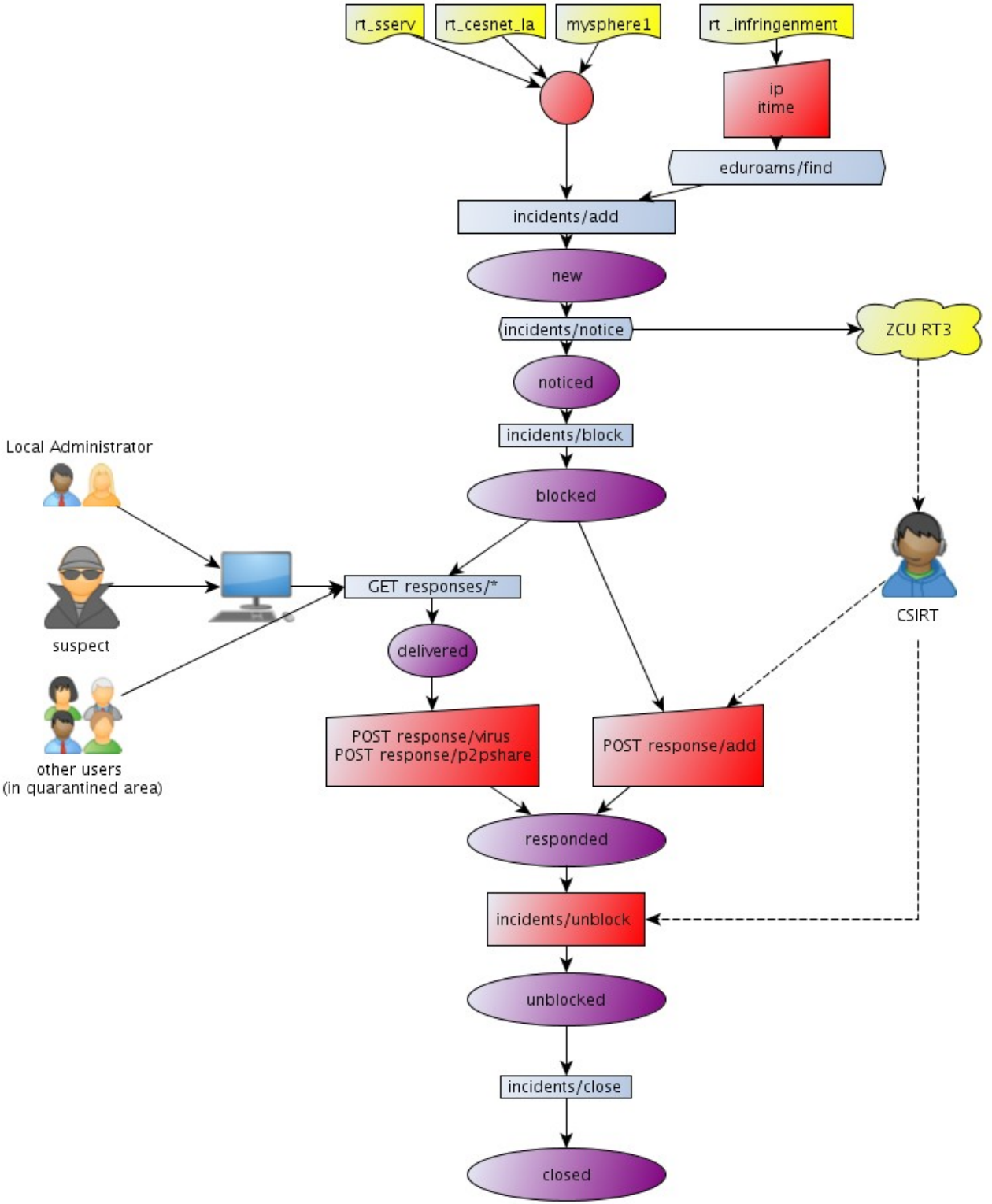


Mysphere2 vs User

- Router steals any connection 80/tcp a redirects those to a local web application
- We are sory, but we have only czech localisation at the moment
    - CakePHP, Doxygene

Mysphere2 and Admin

- Mysphere2 is not just a web page, but it is also a tool for whole incident lifecycle management



mysphere2

- Mysphere2 automates a lot of stuff = computer aided process for incident response and handling in WEBnet network

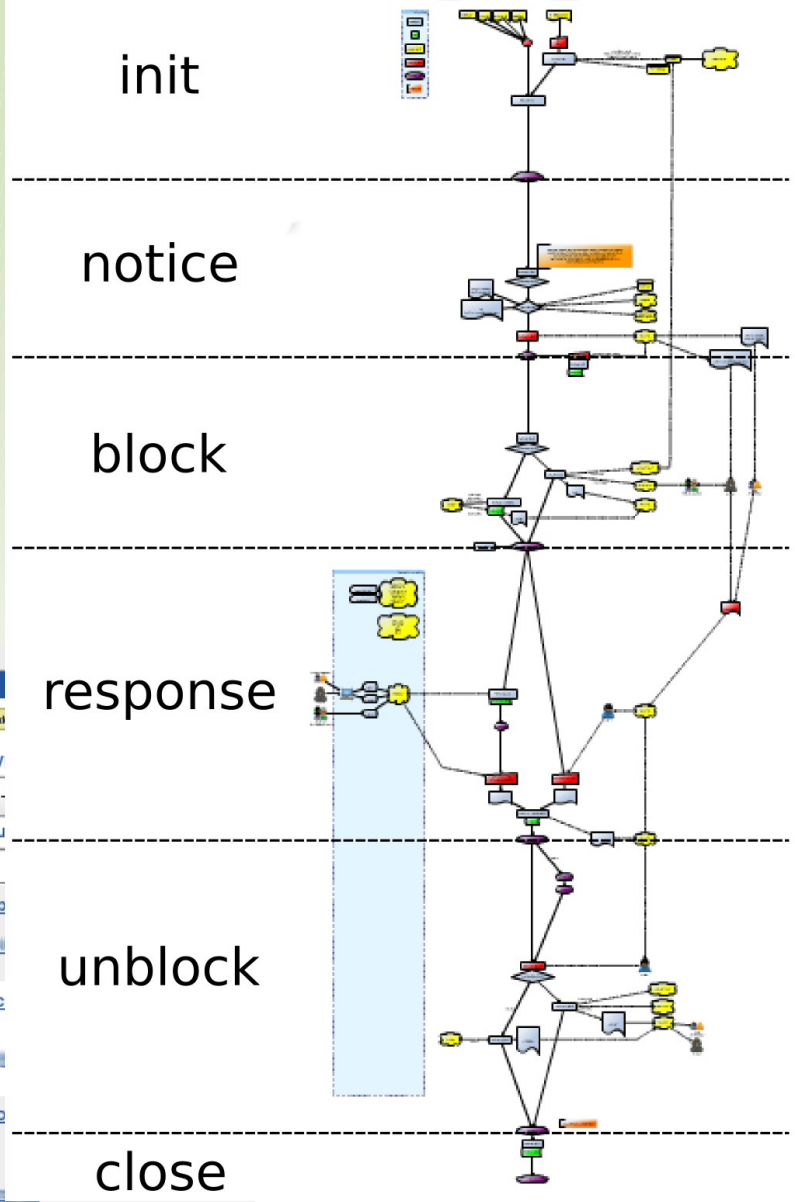
mysphere2: Automat pro ... | mysphere2: Automat pro ... | #131555: [sphr2#119] u...

Mysphere2: incidents incidents/getlabyhostname eduroams responses/show responses redirects types states pages/doc pages/apidoc supp::spra

ncidents

Actions New Incident List Types New Type List Stat

Actions	Id	Ip	Mac	Hostname	Text	State	Ty
F R						--	
		Owner	Claimant	Rt	Ctime	ltime	Su
F R							
V E D	59	147.228.53.150	00:11:09:d1:1a:18	ui505p05-ips.civ.zcu.cz	testovaci incident	unblocked	sp
N B U C		bodik	mysphere1	124412	2011-06-29 16:38:00	2011-06-29 16:38:00	
V E D	52	147.228.185.145	0c:ee:e6:a6:22:c0	zcu-mobile-n401.zcu.cz	/home/bodik/winsearch2.pl Time sum(bytes) sum(pck) sip	blocked	sc
N B U C		bodik	mysphere1	123355	2011-06-02 08:01:00	2011-06-01 10:00:00	
V E D	56	147.228.180.131	00:16:ea:7b:e8:c6	eduroam-n131.zcu.cz	DEBUG: searchradius: epsilon=0. date=2011-06-13 08:44:42. type=ip. starttime=2011-06-13 08:44:00. st	blocked	bo
N B U C		bodik	SSERV	123875	2011-06-16 18:18:00	2011-06-13 08:44:00	
V E D	65	147.228.181.181	00:24:2b:04:7b:a3	eduroam-n437.zcu.cz	mysphere1 /home/bodik/winsearch2.pl Time sum(bytes) sum(pck) si	noticed	botnet
N B U C		bodik	sserv	124821	2011-07-13 12:57:00	2011-07-11 15:43:00	[redacted].edu.pl
V E D	67	147.228.167.46	00:1a:92:f1:d1:6b	http://eddison.fpe.zcu.cz/	Evidentiary Information: Notice ID: 22-156395469 Initial Infringement Timestamp: 8 Aug 2011 19	blocked	p2pshare
N B U C		apadrta	BayTSP	125702	2011-08-08 21:26:00	2011-08-09 22:58:00	
V E D	77	147.228.180.44	00:24:23:07:e8:4a	eduroam-n44.zcu.cz	infr time je o 5 minut jinde, ale predpokladam ze to byl on ... ---------- DEBUG: search	banned	p2pshare



Mysphere2 resume

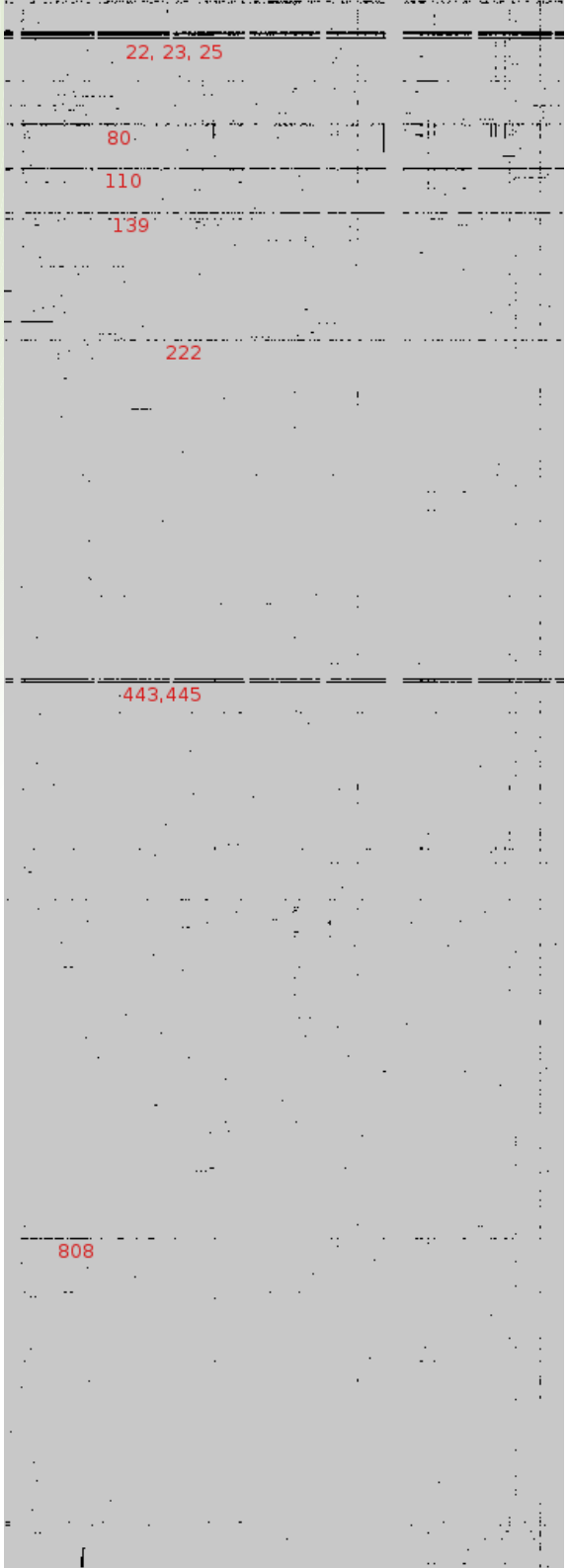
- 70 incidents were resolved so far
  - TTUI – Time to user informed
  - TTFR – Time to (user) first reaction
  - TTR – Time to incident resolution

	TTIU [m]	TTRF [m]	TTR [m]
Without Mysphere2			
Average	564	12562	26126
Median	143	2834	7668
With Mysphere2			
Average	1114	5682	10154
Median	392	1583	6013

Mysphere2 helped to shorten the *time to first user response* and the *total time to resolve the incident* to 50% (measured by RequestTracker correspondence time analysis)

Future work

- Mysphere3 – Honeypots on Ipv6
- Visualization
  - Conti et al
- Statistical modeling
  - `scikit-learn`



R3sum3

- Security is a process, not a product (B.Schneier™)
  - Stay up-to-date
    - isc.edu, full-disclosure, bh, ccc, defcon, ...

- IDS are very usefull, but can work for and againts you, and it's good to know how and why to build them ...
  - http://brmlab.cz/project/warzone
  - http://code.google.com/p/nets-x/

vs.

Experiences with IDS and Honeypots

Q & A ?

Radoslav Bodó <bodik@civ.zcu.cz>

Michal Kostěnec <kostenec@civ.zcu.cz>

Terena.org >> Campus BPD CBPD135