



GN3

Zkušební s (N)IDS

Radoslav Bodó <bodik@civ.zcu.cz>

Agenda

- Úvod
- 2008 – 2009 : Mysphere1
- 2010 : Ostatní
- 2011 : Mysphere2
- 2012 : Mysphere3 ?
- Kam oko dohlédne
- Trendy
- Závěr



mysphere1

- Startér – 2006 ?
 - Labrea od Pavla Vachka
- FR Cesnet č. 230/2007 + CIV, ZČU Plzeň
- Motivace
 - WIRT chtěl nástroj pro detekci napadených PC a začít incidentům předcházet
- Cíle
 - Naučit se problematiku
 - Zlepšit/vybudovat nástroje
 - Zvýšit bezpečnost sítě WEBnet

mysphere1

- Vyzkoušeli jsme několik IDS
 - Funkční (aktivně používané)
 - Labrea, Nepenthes, Netflow search, sshcrack.pl
 - Užitečné (není čas na vyhodnocování ...)
 - apache_rfi, Hihat, Penetrační testy
 - Opuštěné
 - Google Hack Honeypot, PHP HOP, Snort, PE Hunter

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

LaBrea

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	195.113.1.111	0.166	3145	21705	1vvs-pv.cz
2009-04-27 00:16:29	5	146.102.2.202	0.48	5042	1433	252vse.cz
2009-04-25 12:50:19	0	195.113.5.114	0.128	3027	15854	1cuni.cz
2009-04-16 14:15:23	0	78.128.1.111	0.183	2530	25724	1	1.....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
3050/gds_db	250	0	250
9090/	250	569	0.439

- Pohled
- | labrea.loadup >

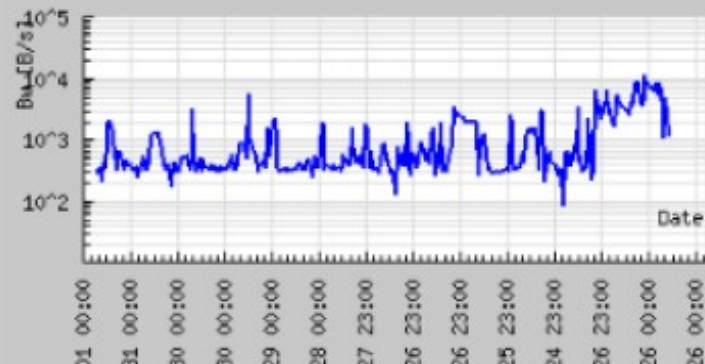
LaBrea week bandwidth usage



LaBrea month bandwidth usage



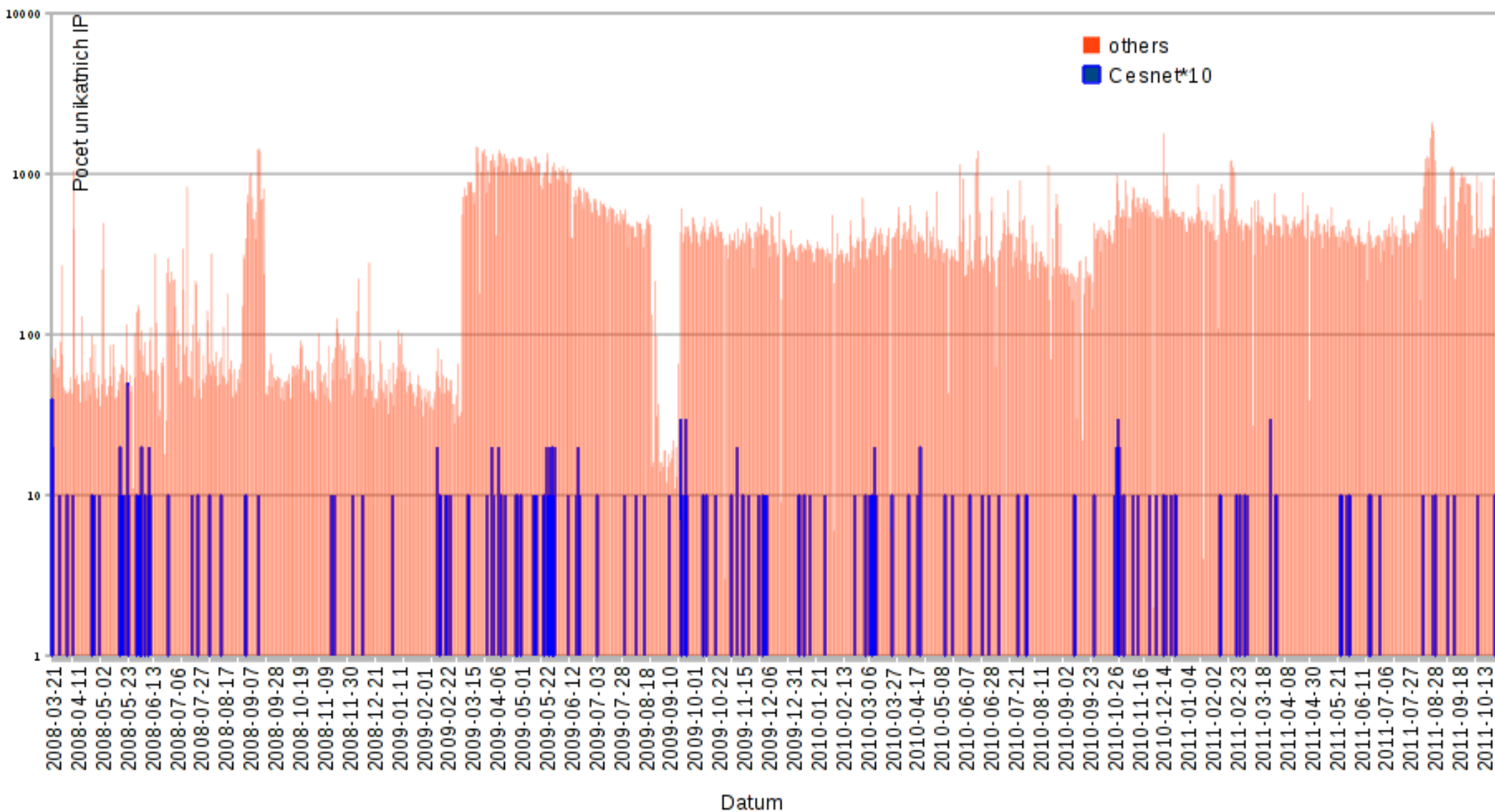
LaBrea year bandwidth usage



- Velikost: 252 adres
- Výsledky za období 03/2008 – 10/2011

LaBrea

- Celkem 502 689 útočníků (velmi nepřesně – unikátní IP/den :)
- **Cesnet 196** (velmi přesně ;) (v grafu *10 !)



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/malware/>
- <http://www.cyber-ta.org/releases/malware/>
- <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: 0f7b92f524b404314c0b6cc6c3e76215: 1

```
-rw-r--r-- 1 nepei nepei 613 Mar 22 19:47 /opt/nepe/var/hexdumps/0f7b92f524b404314c0b6cc6c3e76215.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

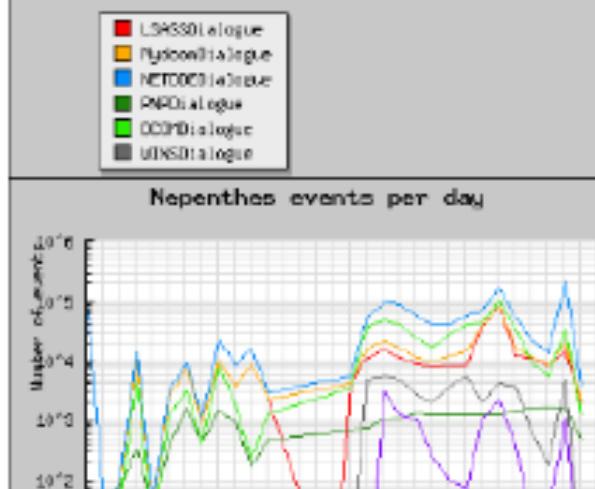
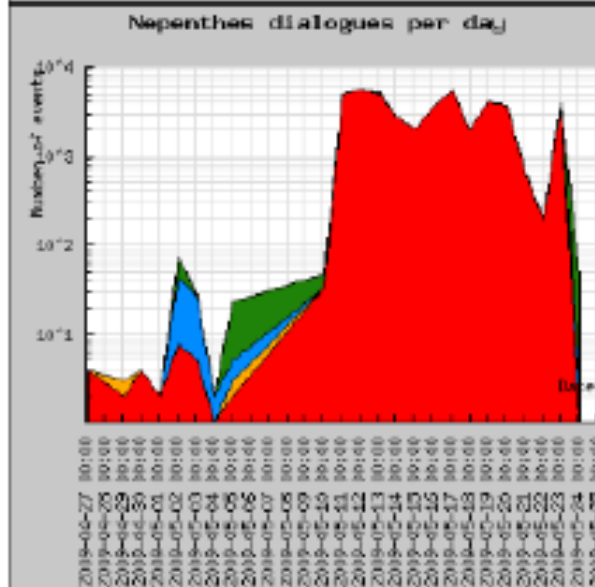
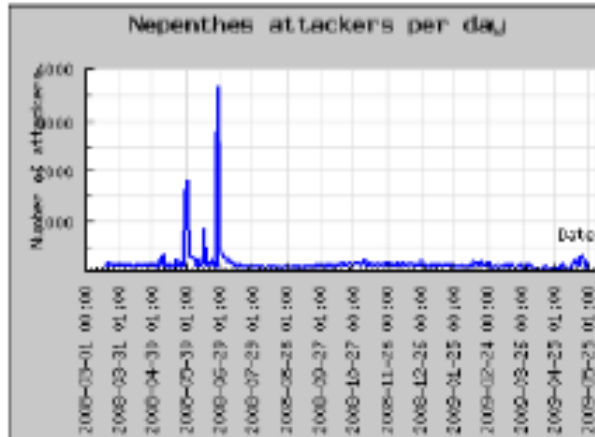
time	held	ips	ipd	psrc	pdst	count	tot_size	hostname
2009-05-20 02:07:33	4771	[REDACTED].215	[REDACTED]	4824	445	208	9152	[REDACTED].cz
2009-05-11 10:14:09	18800	[REDACTED].67	[REDACTED]	1977	445	81574	6719456	[REDACTED].cz
2009-05-04 13:04:30	665	[REDACTED].133	[REDACTED]	58676	3140	37635	734070	[REDACTED].cz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

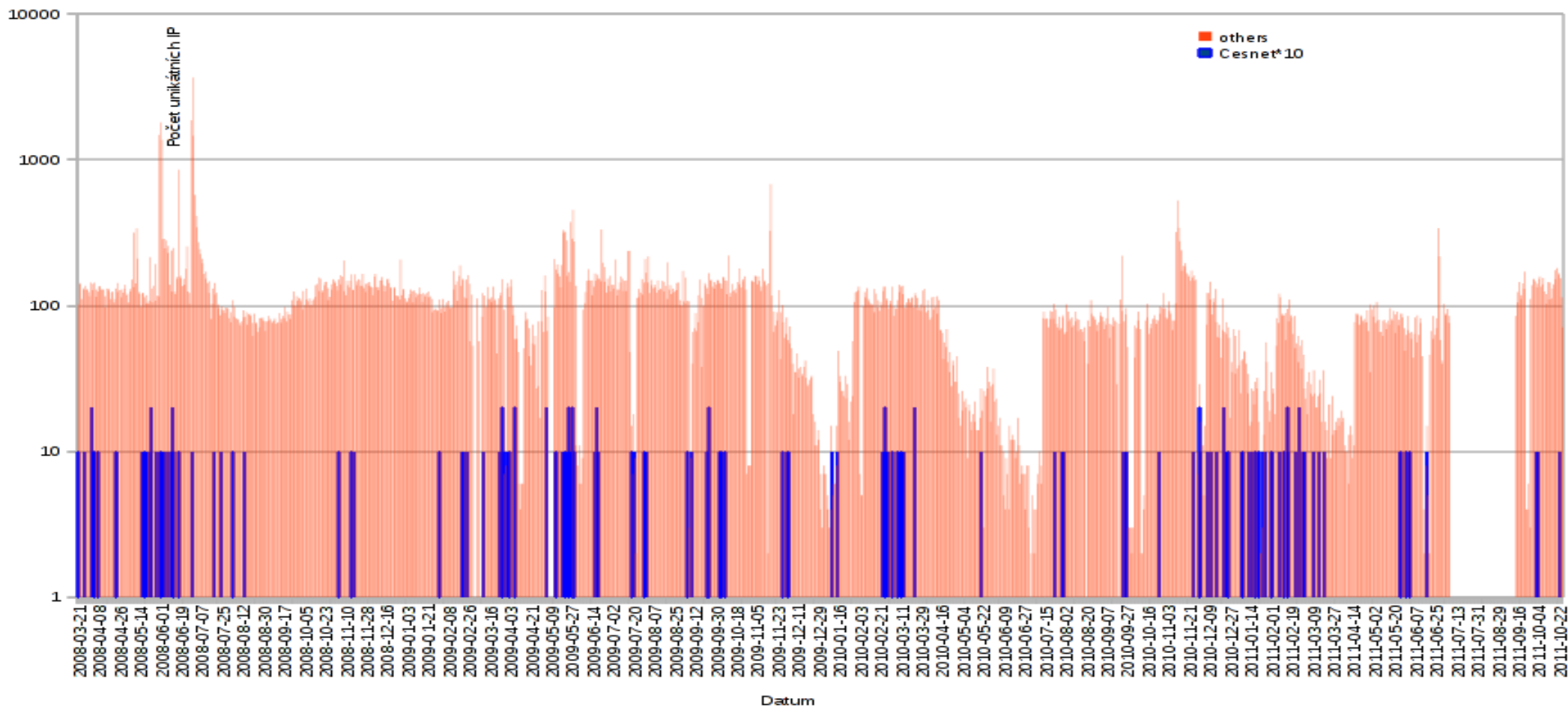
- Pohled
- | nepe.loadup >



- Velikost: 150 adres
- Výsledky za období 03/2008 – 10/2011

Nepenthes

- Celkem 128 372 útočníků (velmi nepřesně – unikátní IP/den :)
- **Cesnet 160** (velmi přesně ;) (v grafu *10 !)
- 580 vzorků malware; zachycený malware neanalyzujeme (tedy používáme to spíše jako labreu). Simulované zranitelnosti jsou stejně staré >> kostenec dionaea



- Analýza informací o síti

NetFlow search

- SQL – WHERE dp=25 GROUP BY sip HAVING conns > 300

- spamsearch, sshsearch, winsearch
- Dnssearch ?

- Nejúčinější senzor !



**DETECTIVE
COLUMBO
AT YOUR SERVICE...**

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 Padrt Ph.D.

Thu Sep 22 11:00:00 CEST 2011
/home/bodik/winsearch2.pl

Time	sum(bytes)	sum(pck)	sip
22 00:00:00	455168	9483	147.228.94.110
22 00:01:00	657102	12367	147.228.181.102
22 00:02:00	86800	1713	147.228.183.85
22 00:03:00	1966240	9645	147.228.99.50
22 00:04:00	1837402	8856	147.228.153.38
22 00:05:00	1505253	6881	147.228.20.103
22 00:06:00	39115	724	147.228.182.114

dik/spamsearch2.pl

Time	sum(bytes)	sum(pck)	sip
22 00:00:00	994109	18477	147.228.181.102
22 00:01:00	1027734	8043	147.228.19.150
22 00:02:00	939549	4585	147.228.181.102

dik/sshsearch2.pl

Time	sum(bytes)	sum(pck)	sip
22 00:00:00	47513710	117800	147.228.181.102
22 00:01:00	1507730	10200	147.228.181.102
22 00:02:00	172920	2882	147.228.181.102
22 00:03:00	9039369	169451	147.228.181.102
22 00:04:00	3354621	67449	147.228.181.102
22 00:05:00	244282	3863	147.228.181.102
22 00:06:00	1015433	7279	147.228.181.102
22 00:07:00	36697255	195889	147.228.101.109
22 00:08:00	463808	2658	147.228.43.85
22 00:09:00	49424	839	147.228.185.92
22 00:10:00	45228774	850891	147.228.209.162
22 00:11:00	3864785	48700	147.228.181.102

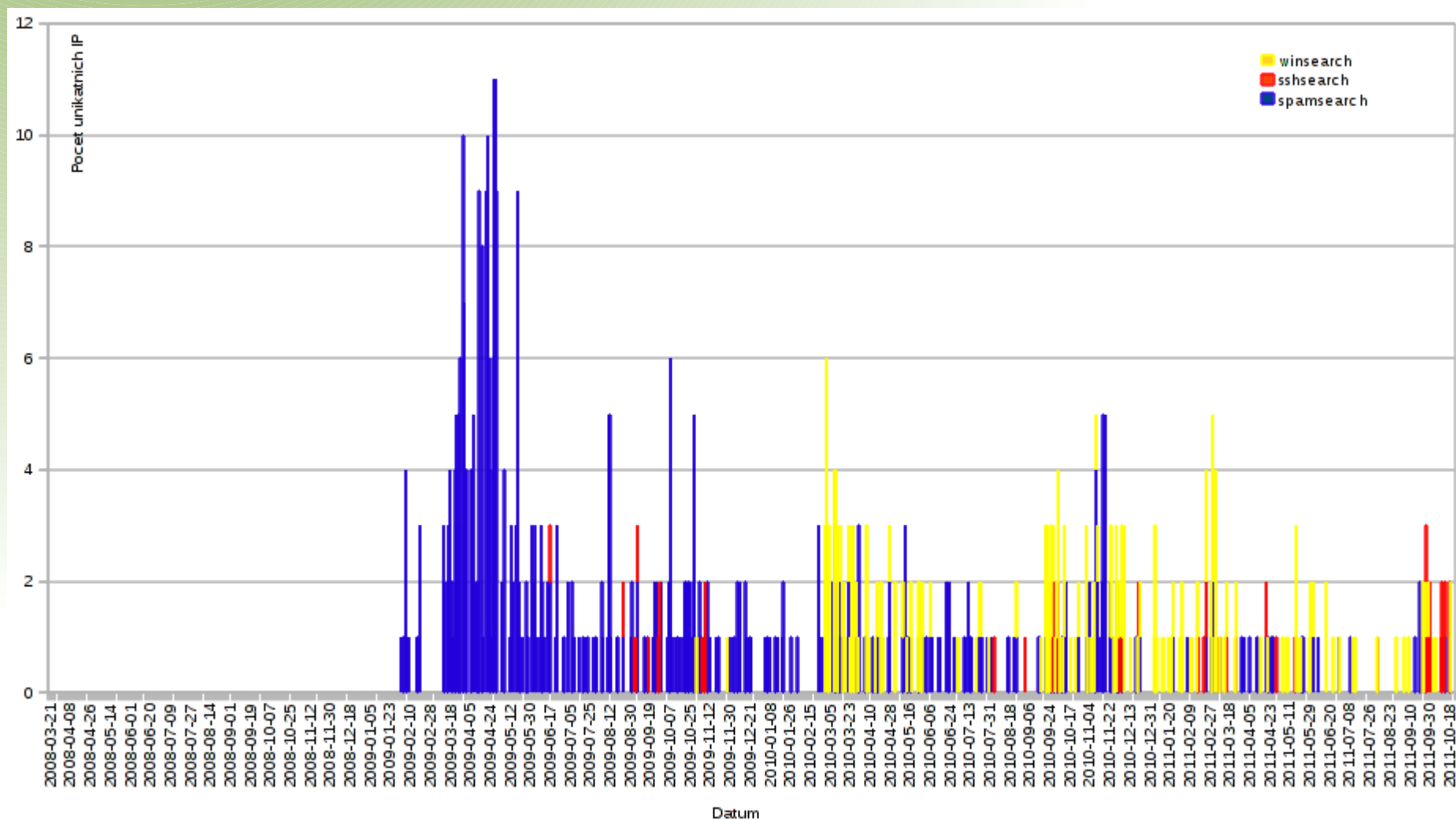
hostname	conns	tgts
el304n01-ket.fel.zcu.cz	4193	4187
eduroam-n358.zcu.cz	1012	2
eduroam-n853.zcu.cz	581	1
kiosek-ng01.zcu.cz	452	2
kiosek-vc02.zcu.cz	354	2
ps203p14-uk.uk.zcu.cz	352	2
eduroam-n626.zcu.cz	304	2

hostname	conns	tgts
1001301-sus.net.zcu.cz	1583	1
sd206p03-kfi.ff.zcu.cz	564	1
sd206p03-kfi.ff.zcu.cz	511	1

hostname	conns	tgts
sd206p03-kfi.ff.zcu.cz	1742	4
sd206p03-kfi.ff.zcu.cz	1174	5
sd206p03-kfi.ff.zcu.cz	548	1
sd206p03-kfi.ff.zcu.cz	507	151
sd206p03-kfi.ff.zcu.cz	373	20
sd206p03-kfi.ff.zcu.cz	341	3
sd206p03-kfi.ff.zcu.cz	198	1
ui322p01-sis.civ.zcu.cz	149	6
kones-fav.zcu.cz	140	1
zcu-mobile-n348.zcu.cz	117	99
kolej-mk-110.zcu.cz	114	9
sd206p03-kfi.ff.zcu.cz	109	15

NetFlow search

- Za období 02/09 – 10/11
 - Spam 515, ssh 47, win 195
 - To nejsou incidenty pouze detekce unikátních IP/den



sshcrack.pl

- Jednoduché a funkční IPS
- Perl grep auth.log + cron + iptables (fail2ban)
 - Autonomní sebeobrana (simple autonomous selfdefense)
 - Bez dohledu, bez vývoje, funkční, stabilní
 - Ad-hoc deployment >> FAI
 - `/afs/zcu.cz/common/tools/sshcrack/sshcrack.pl`

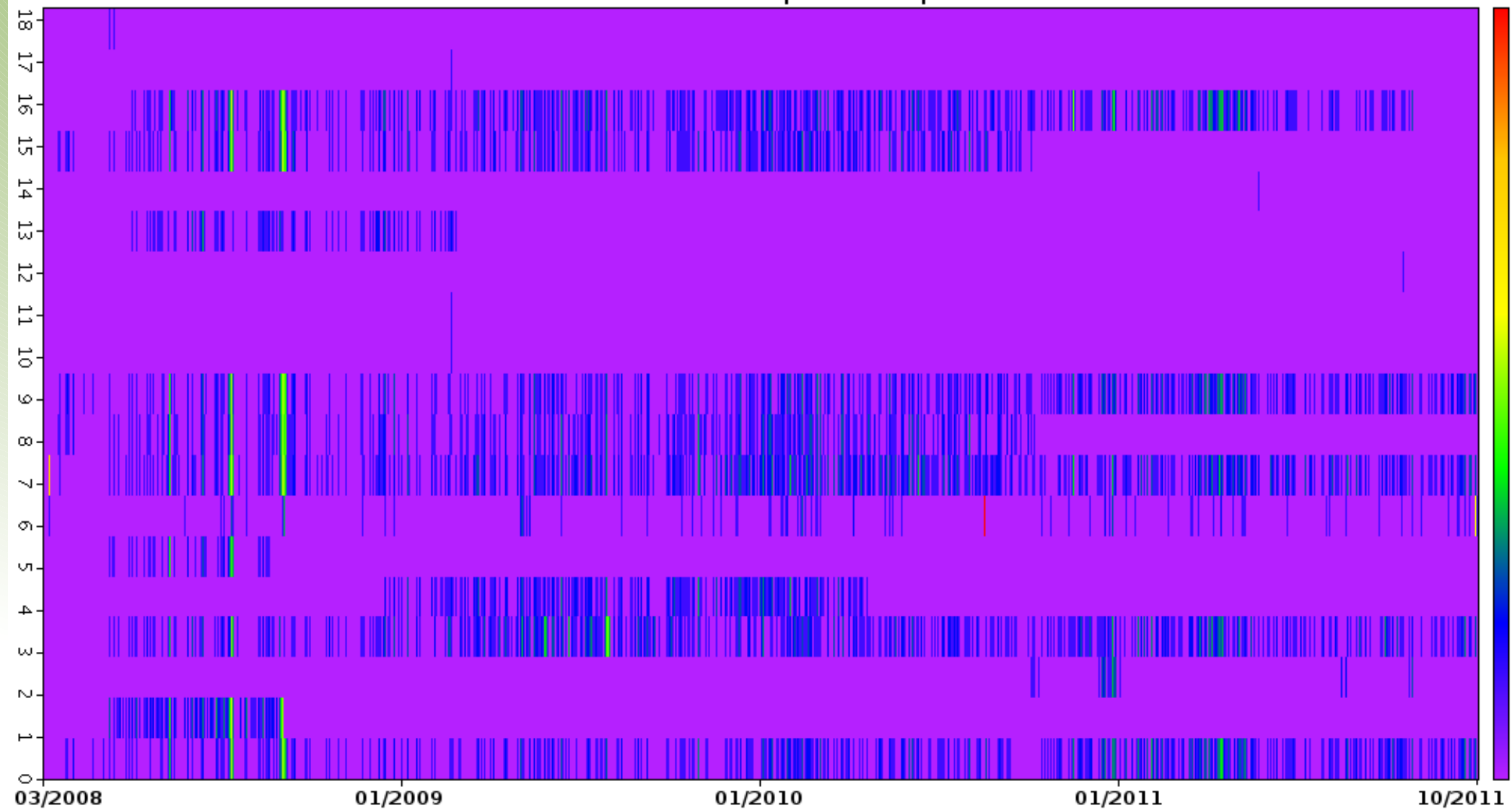


VS.



sshcrack.pl

sshcrack.pl Heatmap



Mysphere1: užitečné IDS

- Užitečné IDS, ale není na ně čas
 - `apache_rfi.pl`
 - apache log analyzer (perl)
 - malware downloader
 - HIHAT
 - Nástroj pro vytváření webových honeypotů s nízkou i vysokou interakcí
 - PHP apps, J2EE apps
 - Penetrační testy
 - Často se při testech najdou průniky ...



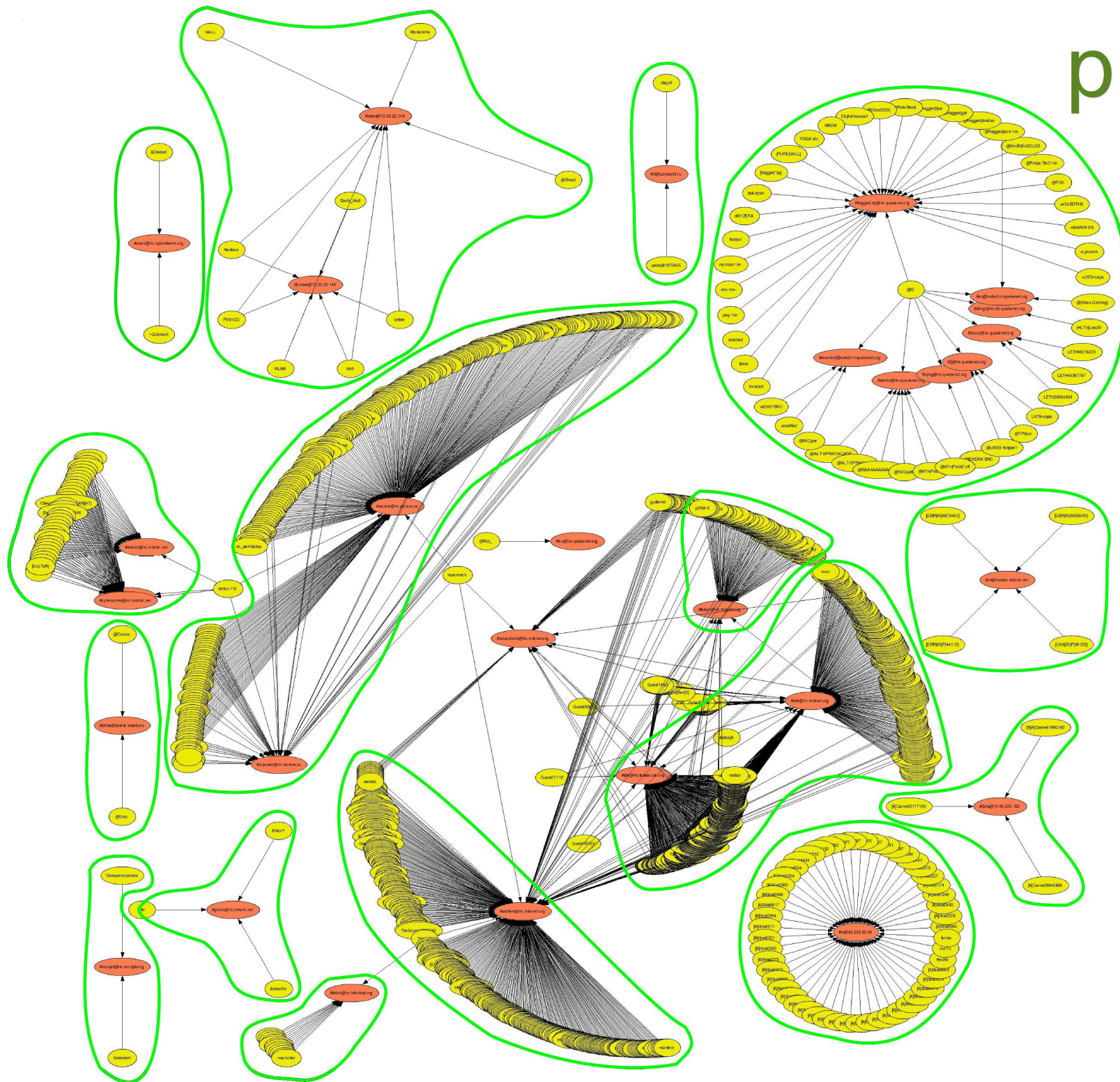
Vzorky Apache RFI

- 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

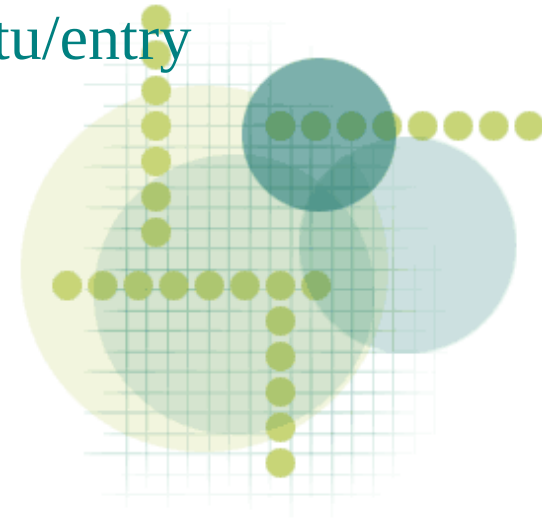
pbotmap

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



Mysphere1: užitečné IDS

- Užitečné IDS, ale není na ně čas
 - `apache_rfi.pl`
 - Apache PHP RFI log analyzer
 - malware downloader
 - HIHAT
 - Nástroj pro vytváření webových honeypotů s nízkou i vysokou interakcí
 - Logovací preambule do každého skriptu/entry pointu
 - cca 10x PHP apps, 2x J2EE apps
- Penetrační testy
 - Často se při testech najdou průniky ...



HIHAT s nízkou interakcí

- Webové rozhraní, clean_spiders.sh

OVERVIEW

SEARCH

DOWNLOADS

MAPPING

STATISTICS

CONFIG

PREVIOUS ID

NEXT ID

BACK TO SEARCH RESULTS

245853

/phpbb/viewtopic.php

189.110.240.166

NV32ts

2009-02-13 16:27:30

SQL

no referrer

-> map

HTTP-GET Information:

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

HTTP-POST Information:

HTTP-SERVER Information:

HTTP_USER_AGENT = NV32ts

Overall

DEBUT select min(Creation) as min, max(Creation) as ma from hihat_main_logs

Time Range: 2008-07-31 23:00:00 - 2009-10-21 23:00:00

DEBUT select attackerIP, Creation, union_time(Creation) as t, module from hihat_main_logs order by Creation desc limit 1

Last touch at: 2009-10-21 23:00:00 (2m ago) from 205.115.111.566 (crawl2.dominet.com.org) to phlbb

Total events: 266602

Zoomed (per: 40)

Ownnet attackers for 30 days

DEBUT lam:1256025826 - 2009-10-01 00:00:00

DEBUT select * from hihat_main_logs where union_time(Creation)>1256025826 and ((per BETWEEN 1217060226 AND 1217079991) OR (per BETWEEN 1265159208 AND 1265223742) OR (per BETWEEN 1265347906 AND 1265478978) OR (per BETWEEN 1265192960 AND 1265195102) OR (per BETWEEN 1265700218 AND 1265745822) OR (per BETWEEN 1265516112 AND 1265579667) OR (per BETWEEN 1265645184 AND 1265710719) OR (per BETWEEN 1265651026 AND 1265661607) OR (per BETWEEN 1265519904 AND 1265519999) OR (per BETWEEN 1265556672 AND 1265557767) OR (per BETWEEN 1265556666 AND 1265556666) OR (per BETWEEN 127965688 AND 1279658222) OR (per BETWEEN 128238912 AND 1282471022))

Attacker/Source

Value_Server

Value_Geo

Value_Fort

Value_Coolde

Creation

Module

download_checked

Iperc

hostname

ip

187.208.155.155

phlbb

victronic.phg

2009-10-12 16:28:09

phlbb

0

2451266619

kolaj-

mb-60.szu.cz

top 20 attackers for last 30 days

attackerIP

attacker

hostname

208.133.133.200

2071

www12.0.com

207.148.133.27

810

phlbb.victronic.phg

207.148.133.28

223

phlbb.victronic.phg

88.168.82.82

170

www12-01-08-22-22.googleusercontent.com

207.148.133.28

174

phlbb.victronic.phg

202.208.170.3

163

202.208.170.3

88.168.82.82

110

www12-01-08-22-22.googleusercontent.com

88.168.82.82

80

www12-01-08-22-22.googleusercontent.com

88.168.82.82

82

www12-01-08-22-22.googleusercontent.com

212.159.139.16

58

www12-01-08-22-22.googleusercontent.com

180.7.200.200

27

180.7.200.200

Job vs r57

数据库	
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	

Connection Reset

- Jdbc type 4

- Traceback

- Dionaea HTTPD directory traversal
>> EFF SSL Observatory

- Kippo >> kipoScan

```
===== 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=
    ")
</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>
```

Mysphere1: užitečné IDS

- Užitečné IDS, ale není na ně čas
 - `apache_rfi.pl`
 - Apache PHP RFI log analyzer
 - malware downloader
 - HIHAT
 - Nástroj pro vytváření webových honeypotů s nízkou i vysokou interakcí
 - Logovací preambule do každého skriptu/entry pointu
 - PHP apps, J2EE apps
- Penetrační testy
 - Často se při testech najdou průniky ...

Mysphere1: opuštěné IDS

- Google Hack Honeypot
- PHP HOP
 - Projekty webových honeypotů
 - Zastaralé, nefunkční nebo neflexibilní
- Snort, PE Hunter
 - Příliš mnoho FP
 - Problematická údržba signatur
 - SSL
 - Časem se k němu vrátíme, ale ne teď ...



2010 post mysphere1

- ... Mysphere1 : 2008 – 2009 ...
- 2010 – studentské projekty
 - Labrea pro Ipv6
 - 2 funkční implementace
 - **Labrea fork**
 - **Vlastní impl.**
 - Žádní útočníci (ani Van Hauser ;(
 - Pracujeme na tom ...
 - IDT – statistické vyhodnocování NetFlow
 - Behavioral analysis (baselining/modeling, ...)
 - Nedotažené ;(
 - Stejně předěláme pomocí **scikit-learn**

2010 post mysphere1

- Mysphere1 funguje ...
 - Napadené stroje jsou detekovány
 - Více detekcí
 - Více bezpečnostních incidentů
 - Více práce



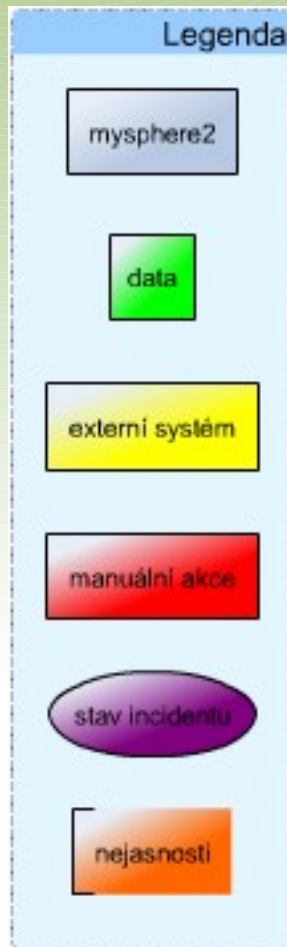
- (netchat) Najít port, (nechat) odpojit port (nespy, ale ...), najít správce, obeslat správce, počkat na odpověď správce, obeslat uživatele, počkat na odpověď uživatele, domluvit si schůzku. *Uživateli mezitím nefunguje internet !*

2011 – mysphere2

- Mysphere2
 - FR Cesnet č. 369 + civ.zcu.cz
 - Zkvalitnění (:) procesu řešení bezpečnostních incidentů
 - Navrhnout a implementovat *orchestrátor síťového prostředí*
 - Automatizované karanténování v campusu, blokování eduroam identit, ...
 - Ukrást HTTP a tlačít informace uživatelům přímo do browseru ...
 - Stroj neodpojit úplně, ale poskytnout uživateli nástroje pro řešení
 - Notifikace a provázání s RT

mysphere2

- = computer aided process for incident response and handling in WEBnet network



init

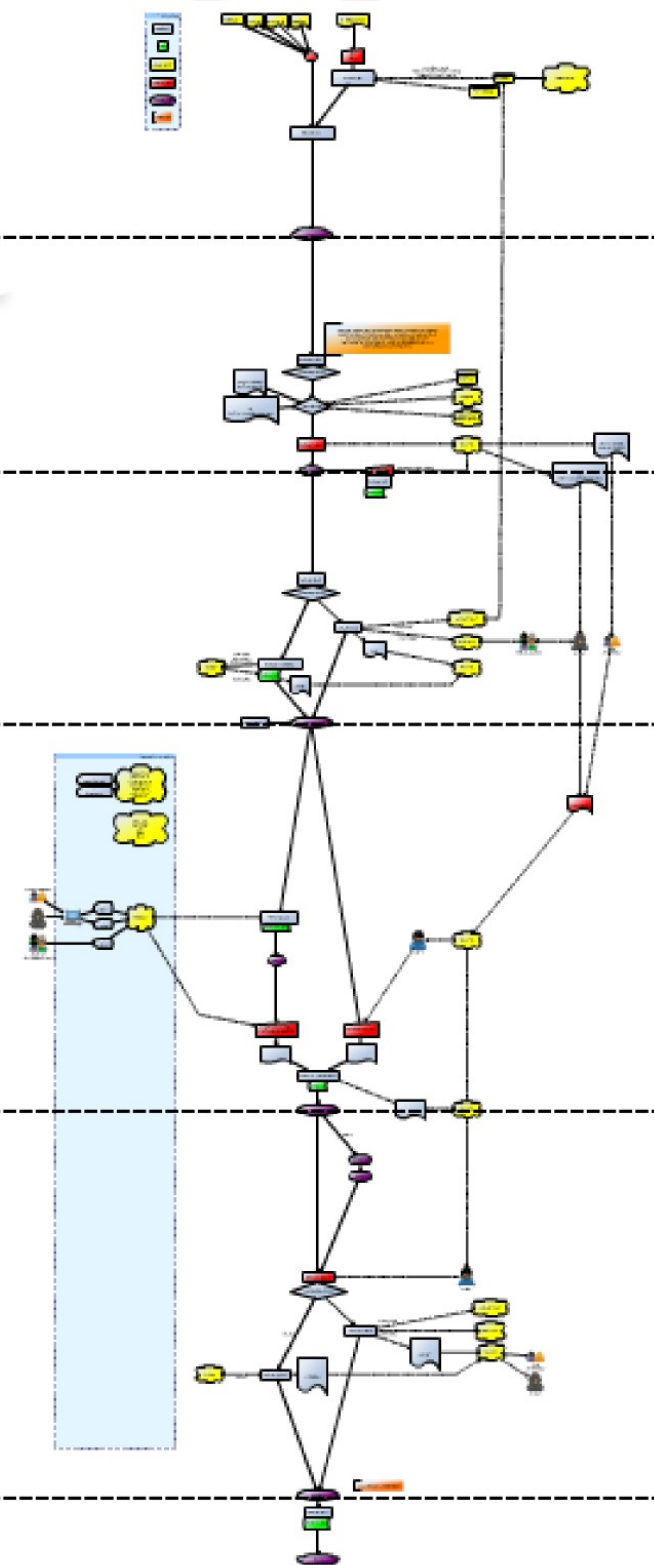
notice

block

response

unblock

close





Tento počítač byl odpojen od sítě WEBnet

Přístup na požadovanou stránku
<http://go.microsoft.com/fwlink/...> Vám byl z bezpečnostních důvodů odepřen.

Bylo detekováno nevhodné chování tohoto počítače (ui505p05-lps.civ.zcu.cz :: 147.228.53.150), které indikuje jeho napadení virem nebo jiné zneužití. Konkrétně rozesílá vysoké množství nevyžádaných zpráv. Pro opětovné odblokování, prosím, postupujte jednou z následujících možností:



- A. Kontaktujte, prosím, svého lokálního správce (support.zcu.cz - [Seznam lokálních správců](#)), který zařídí nápravu.
- B. Uvedte počítač do vhodného stavu svépomocí dle návodu support.zcu.cz - [Jak postupovat v případě zavirování počítače](#).
Po reinstalaci nebo odvirování připojte nezávadný stroj do sítě a vyplňte [žádost o odblokování](#). Odblokování je možno provést ihned po odpojení závadného stroje od sítě, není tedy třeba čekat na přeinstalaci (bude se hodit např. je-li do zásuvky připojen switch, který je využíván více stroji).

I přes blokování jsou pro vyřešení problému stále dostupné vybrané informační systémy:

- <https://webmail.zcu.cz>
- <http://support.zcu.cz>
- <http://phone.zcu.cz>

Děkujeme za spolupráci
CIV (abuse@zcu.cz)

2011 – mysphere2

- Ban interface



Reagovat na incident (sphr2 l#59)

Bylo detekováno nevhodné chování tohoto počítače (ui505p05-lps.civ.zcu.cz :: 147.228.53.150), které indikuje jeho napadení virem nebo jiné zneužití. Konkrétně rozesílá vysoké množství nevyžádaných zpráv. Po odvírování stroje můžete použít níže uvedený formulář nebo <https://webmail.zcu.cz> a dát nám vědět, že byl incident vyřešen a jakým způsobem.

1. Kontaktním formulářem

Vyberte prosím provedenou akci:

▼

Stroj byl zbaven virové nákazy
Stroj byl přeinstalován
Stroj byl odpojen od sítě, jedná se o sdílenou zásuvku
Jiná akce, prosím uveďte jaká

Odeslat

2. Kontaktovat lokálního správce

V případě problémů, můžete kontaktovat lokálního správce. Jejich seznam naleznete na adrese support.zcu.cz - [Seznam lokálních správců](#).

- <https://webmail.zcu.cz>
- <http://phone.zcu.cz>

3. Ručně emailem

Přihlaste k systému <https://webmail.zcu.cz> a zašlete nám zprávu na abuse@zcu.cz ručně. Zprávu formulujte podle vzoru:

Subject: [ZCU RT3 #124412] [sphr2#59] ui505p05-lps.civ.zcu.cz - napadený stroj
AddRequestor: simekm@civ.zcu.cz

Text nad tímto řádkem ignorujte, následuje sdělení pro uživatele...
Please ignore lines above, message for user follows ...

Dobry den, chtel bych pozadat o odblokovani pripojeni pro stroj
ui505p05-lps.civ.zcu.cz (147.228.53.150).

- A) Stroj byl zbaven virové nákazy. (cleaned)
- B) Stroj byl přeinstalován. (reinstalled)
- C) Stroj byl odpojen od sítě, jedná se o sdílenou zásuvku. (shareduplink)
- D) Jiná akce, prosíme uveďte jaká. (other)

S pozdravem

2011 – mysphere2

- Response interface

2011 – mysphere2

- ... ale nepředbíhejme ;)
 - Vyčkejme na závěrečnou zprávu
 - Prezentaci na semináři řešitelů v Mikulově
 - 22.11.2011 – 09:00 Salonek Pálava



2012 na západě čech

- Mysphere3 ?
- Vizualizace
 - Conti et al.
 - Studentské práce
 - Google Charts API
 - Matplotlib
- dns-anomaly (nic.cz)
- IPv6
 - Jako fakt už nejvyšší čas !
 - IDS *už máme*, a co vy ? ;)



- ... víme že nejsme sami ...
- cesnet.cz
 - PV – LaBrea, SSERV, ORR
 - TK – FTAS (bylo by super jej využívat jako IDS)
 - AK – mentat, warden, ...
- muni.cz
 - Namtar – bez vnějších vztahů s komunitou, zaměřený na NAC windows (nad WMI)
 - Vykopal et. al. – ???
- vsb.cz – uslyšíme odpoledne ...

Myšlenky dne

- Trendy
 - O zneužívání mobilních zařízení máme první zprávy
 - konference, ORR
 - USA oficiálně prohlásila internet za sféru bojových operací !!!!
 - Různé subjekty (nejen hloupí spameři) na planetě mají regulérní jednotky pro boj v datasféře a ty chtějí **NAŠE** stroje/prostředky
 - EU/NATO, USA, CN, RU, ...
 - SSL/TLS/PKI nefunguje, co s tím ???
 - GSM již není druhý bezpečný kanál
 - viz CCC2009

Z8v2r

- Bezpečnost není výrobek, ale proces (B.SchneierTM)
 - Když už ne IDS, tak je minimálně potřeba zůstat v obraze
 - isc.edu, full-disclosure, bh, ccc, defcon, ...
- Na výrobu expertního systému potřebujeme experty. Tím se ale člověk nestane čtením publikací ...
 - <http://brmlab.cz/project/warzone>
 - <http://code.google.com/p/nets-x/>



VS.





Otázky ?

