NĚKTERÉ MÉNĚ TRADIČNÍ METODY DETEKCE ŠKODLIVÝCH AKTIVIT V IP SÍTÍCH

Petr Břehovský

ŠKODLIVÉ AKTIVITY

- AUTOMATY (červi, botnety, viry, ...)
- ÚTOČNÍCI
- ÚNIKY DAT „OFICIÁLNÍ“ CESTOU

alliance.mwcollect.org

Collaborative Malware Collection and Sensing

/internal/
Protected Member's Area

Login

»

Join

Benefits, Requirements
Membership Application

/public/
World Viewable Information

Public Data

Data Overview
Attacker World Map
Attack Toplists

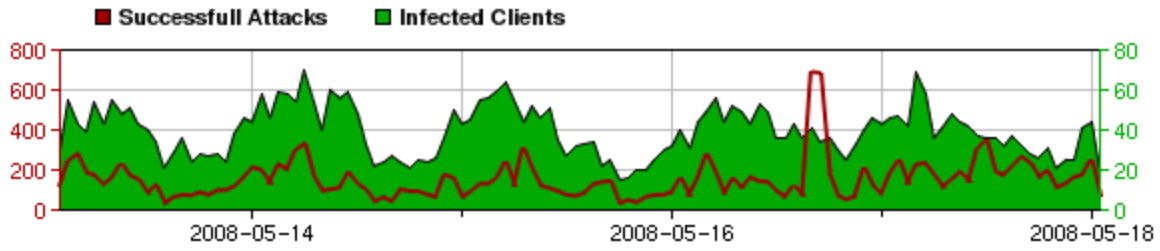
Services

Upload Binary
Search Binary

Data Overview
See what's happening on the internet.

mwcollect Alliance Activity

Activity Timeline



Attack Source Country Distribution

Please note the reduced representativity of this chart as we do not have evenly distributed sensors accross all countries.

Nephentes realtime console

http://nepenthes.csrrt.org:10080/nepenthes/

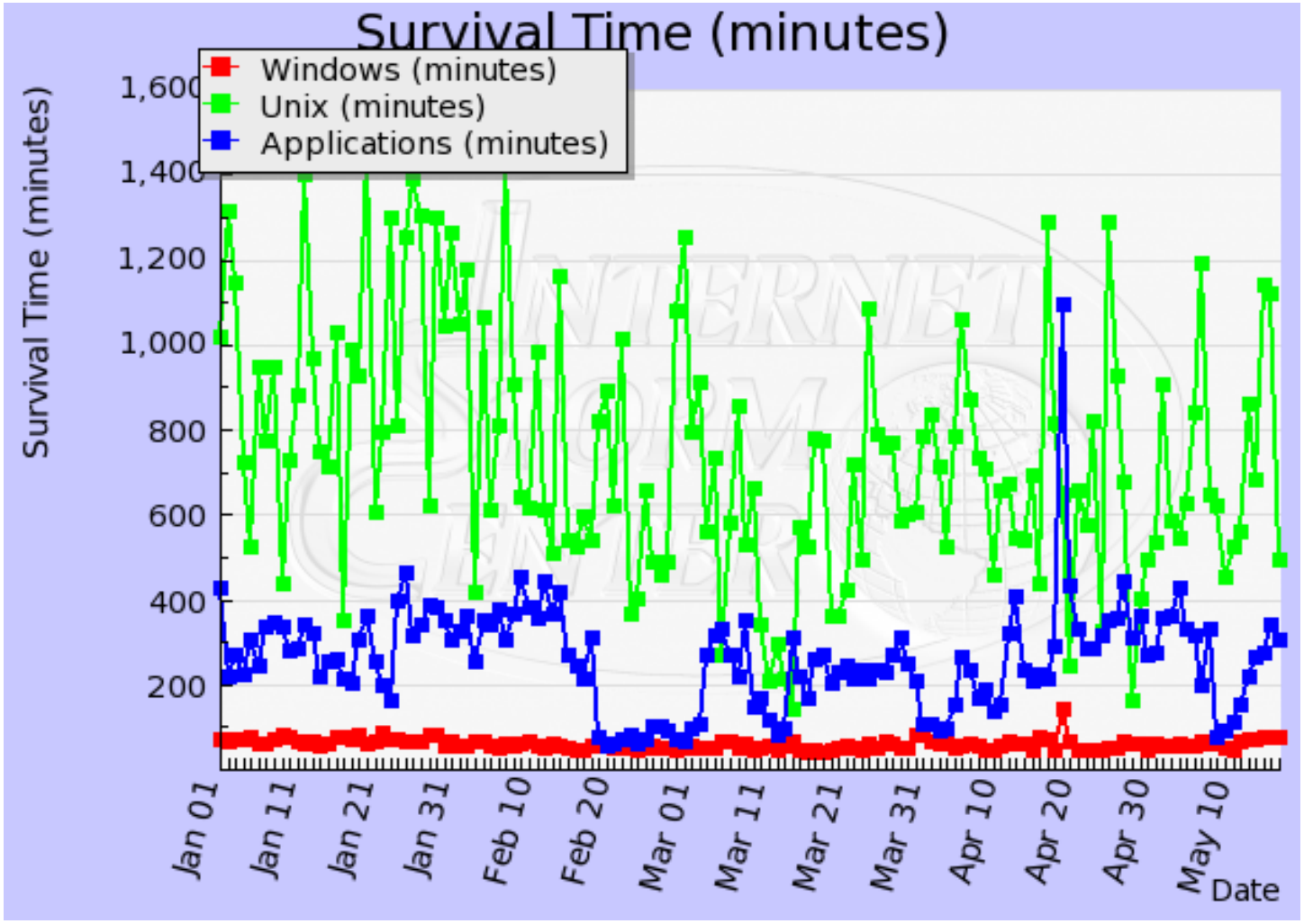
Hash	First Seen	Last Seen	[illegible]	Virus	Norman Result	Hexdump	File
f892a7aa75aa45262ec9b0aff00026	14.05.2008 04:58:44	14.05.2008 04:59:01	1	yes (3)	no (resubmit)	browse	download
6986b7a7e54cee6f0523d7a5cf8d07	19.04.2008 19:15:00	19.04.2008 19:15:16	1	yes (3)	no (resubmit)	browse	download
688b7d2fcacb0a4abcc17a68d0f881	16.04.2008 22:04:08	16.04.2008 22:04:08	0	yes (3)	no (resubmit)	browse	download
e1d6d86f2fc643a555eae0ee3b6b2e	12.04.2008 18:52:56	16.04.2008 00:03:59	294	yes (2)	no (resubmit)	browse	download
ce95b1515cb7ff8acbaeb70cdf783a	08.04.2008 20:47:25	08.04.2008 21:02:09	70	yes (3)	no (resubmit)	browse	download
67591d3c4179831523eadcc9b47503	08.04.2008 10:02:05	08.04.2008 10:02:05	0	yes (3)	no (resubmit)	browse	download
c73b285abf07e2d91e14cdb0b8717e	08.04.2008 01:08:52	08.04.2008 01:08:52	0	yes (3)	no (resubmit)	browse	download
21e2580bb4653dbfdf085541ff7451	16.03.2008 16:18:57	16.03.2008 21:58:57	4	yes (3)	no (resubmit)	browse	download
cdc192048200ab415c9b6e37c973db	13.03.2008 12:56:33	13.03.2008 21:36:19	2	yes (3)	no (resubmit)	browse	download
0c7c0a57471f67a05637f405e7496b	20.02.2008 12:07:52	20.02.2008 12:07:52	0	yes (3)	no (resubmit)	browse	download
55d86578d34ffa544ded8cee984ae1	10.02.2008 12:26:56	12.03.2008 14:36:02	14	yes (1)	no (resubmit)	browse	download
ebc75bdef9b2bb77101e3005c93425	06.02.2008 10:33:49	10.02.2008 15:42:55	4	yes (1)	no (resubmit)	browse	download
c642f1295a9864357e81680871cae9	26.01.2008 23:47:03	04.03.2008 10:06:01	1	yes (3)	no (resubmit)	browse	download
fe3167cfcbdad60fe27f4e43410573	25.01.2008 12:10:40	25.01.2008 12:10:40	0	yes (3)	no (resubmit)	browse	download

llow	< 5 samples	Seems a standard
range	< 25 samples	Easy task
ed	< 250 samples	Should think about security
ack	> 250 samples	Worms heaven, admins hell

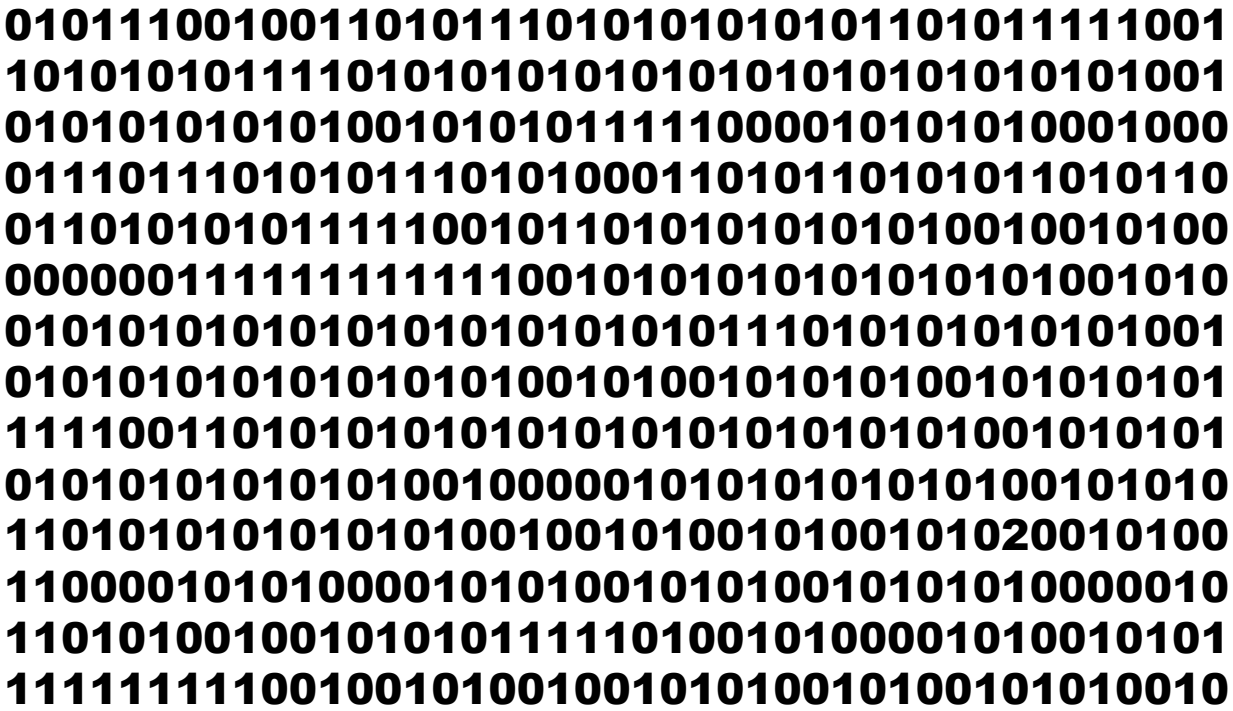
u can click the map, zoom, crawl, whatever you can do with a map, this is not a static picture**

ŽIVOTNOST IMPLICITNÍCH INSTALACÍ

http://isc.sans.org/survivaltime.html



CO S TÍM?


0101110010011010111010101010101101011111001
1010101011110101010101010101010101010101001
0101010101010010101011111000010101010001000
0111011101010111010100011010110101011010110
0110101010111110010110101010101010010010100
0000001111111111111001010101010101010101001010
0101010101010101010101010111010101010101001
0101010101010101010010100101010100101010101
1111001101010101010101010101010101001010101
0101010101010100100000101010101010100101010
1101010101010101001001010010100101020010100
1100001010100001010100101010010101010000010
1101010010010101011111010010100001010010101
1111111110010010100100101010010100101010010

TRADIČNÍ METODY NEJSOU ZCELA SPOLEHLIVÉ

- Antiviry

http://www.av-comparatives.org/

- IDS

falešné poplachy, neznámé útoky

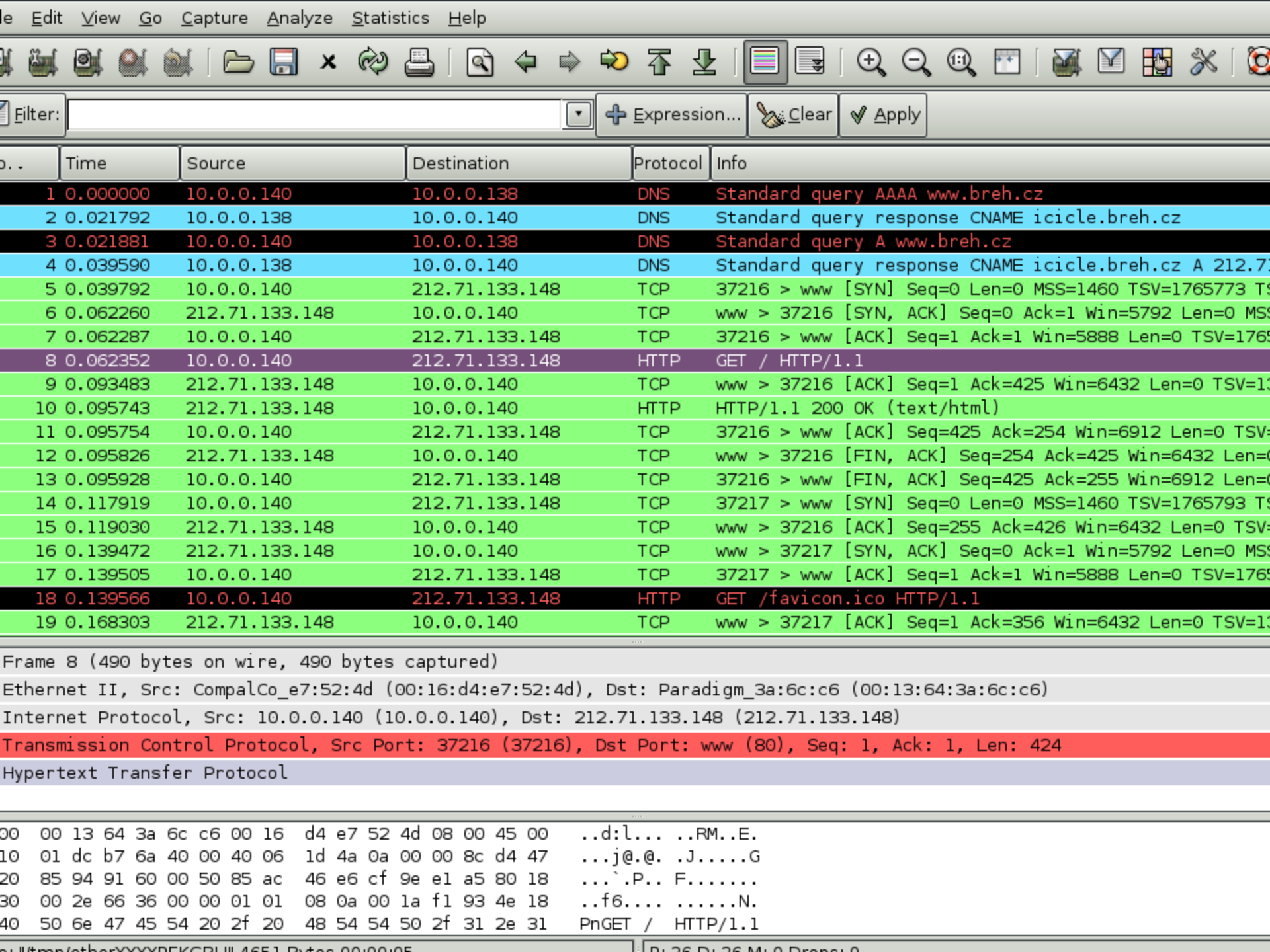
MÉNĚ TRADIČNÍ METODY

- VIZUALIZACE
- ODDĚLENÍ LEGITIMNÍHO PROVOZU

VIZUALIZACE

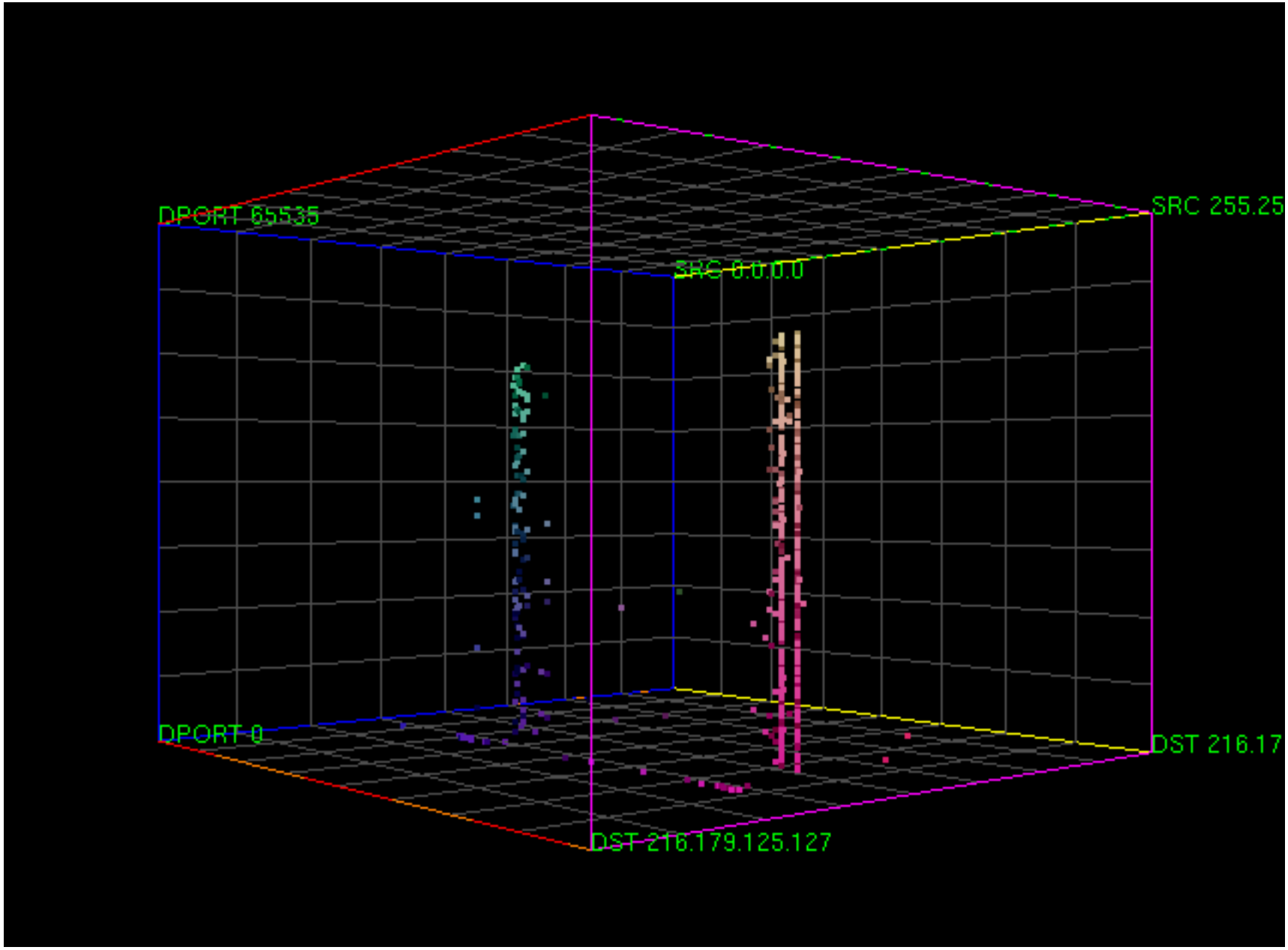
MÉNĚ VHODNÉ ZPŮSOBY REPREZENTACE

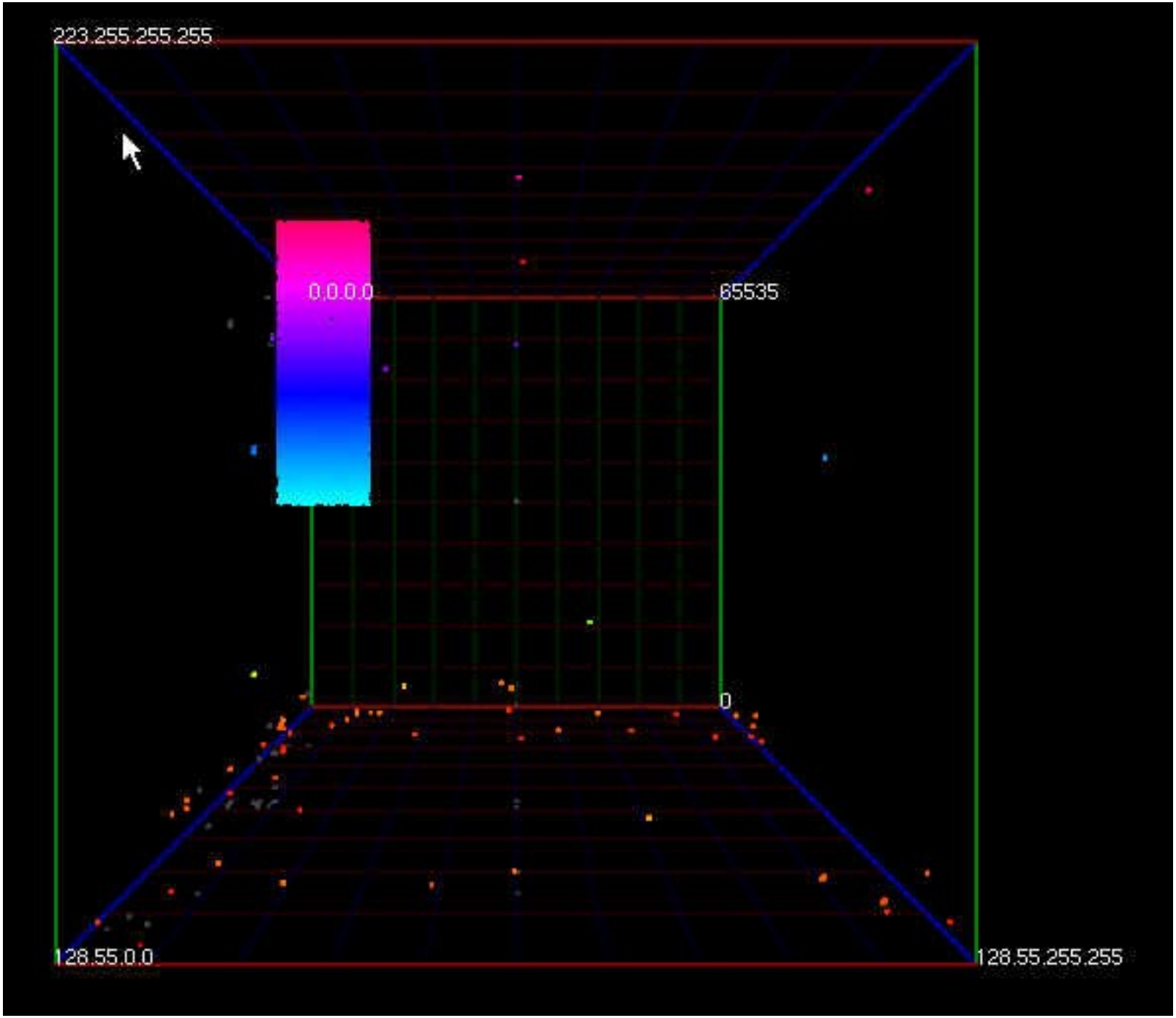
```
01 dc b7 6a 40 00 40 06 1d 4a 0a 00 00 8c d4 47
85 94 91 60 00 50 85 ac 46 e6 cf 9e e1 a5 80 18
00 2e 66 36 00 00 01 01 08 0a 00 1a f1 93 4e 18
50 6e 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31
0d 0a 48 6f 73 74 3a 20 77 77 77 2e 62 72 65 68
2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a
20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31
31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36
3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 38 2e
31 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 38
30 34 30 34 20 49 63 65 77 65 61 73 65 6c 2f 32
2e 30 2e 30 2e 31 34 20 28 44 65 62 69 61 6e 2d
32 2e 30 2e 30 2e 31 34 2d 30 65 74 63 68 31 29
0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78
6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78
6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78
68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74
6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c
61 69 6e 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f
70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 35 0d 0a 41
63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20
```

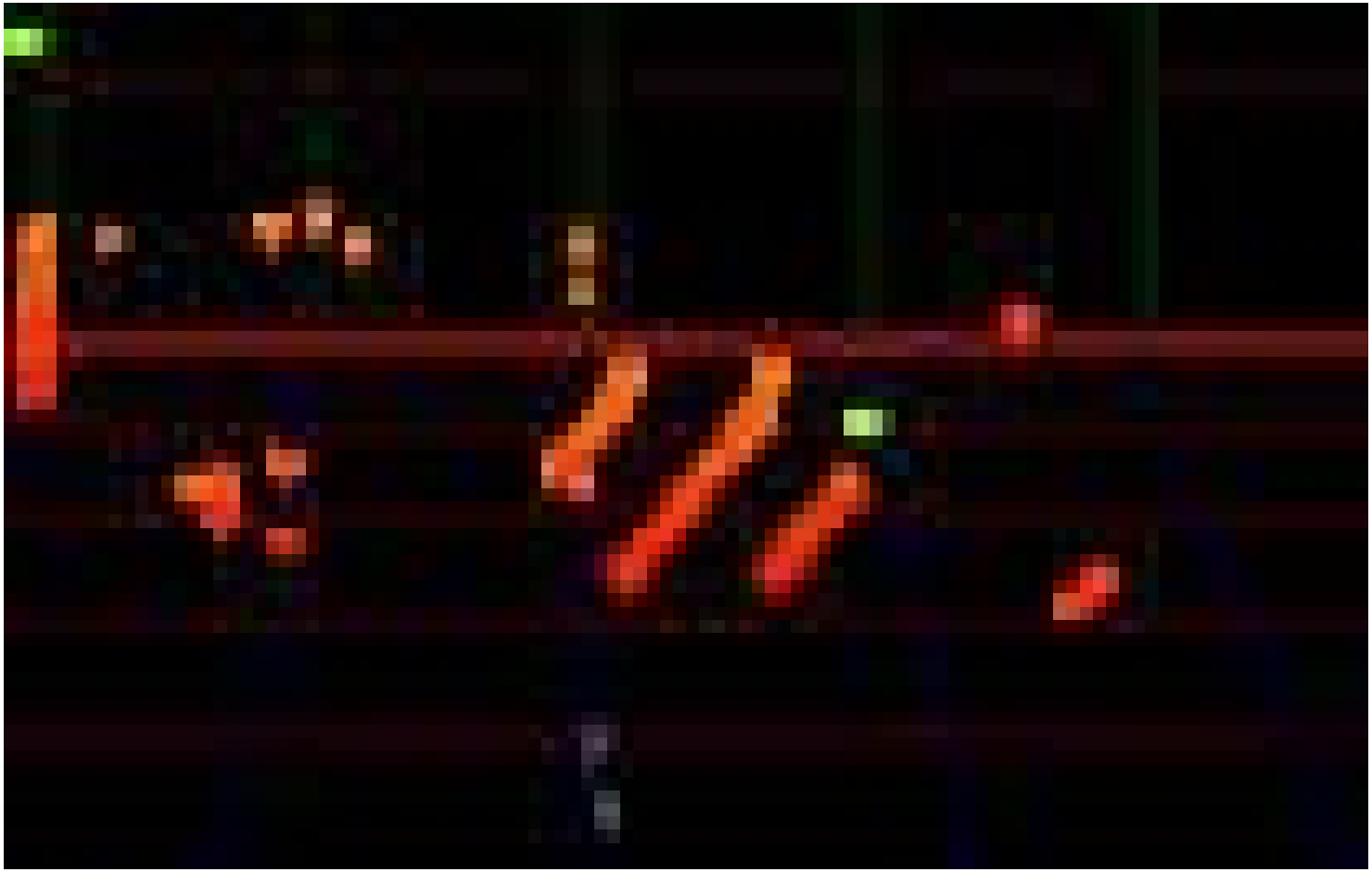

Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.0.0.140 10.0.0.138 DNS Standard query AAAA www.breh.cz
2 0.021792 10.0.0.138 10.0.0.140 DNS Standard query response CNAME icicle.breh.cz
3 0.021881 10.0.0.140 10.0.0.138 DNS Standard query A www.breh.cz
4 0.039590 10.0.0.138 10.0.0.140 DNS Standard query response CNAME icicle.breh.cz A 212.7
5 0.039792 10.0.0.140 212.71.133.148 TCP 37216 > www [SYN] Seq=0 Len=0 MSS=1460 TSV=1765773 TS
6 0.062260 212.71.133.148 10.0.0.140 TCP www > 37216 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
7 0.062287 10.0.0.140 212.71.133.148 TCP 37216 > www [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=1765
8 0.062352 10.0.0.140 212.71.133.148 HTTP GET / HTTP/1.1
9 0.093483 212.71.133.148 10.0.0.140 TCP www > 37216 [ACK] Seq=1 Ack=425 Win=6432 Len=0 TSV=1
10 0.095743 212.71.133.148 10.0.0.140 HTTP HTTP/1.1 200 OK (text/html)
11 0.095754 10.0.0.140 212.71.133.148 TCP 37216 > www [ACK] Seq=425 Ack=254 Win=6912 Len=0 TSV=
12 0.095826 212.71.133.148 10.0.0.140 TCP www > 37216 [FIN, ACK] Seq=254 Ack=425 Win=6432 Len=0
13 0.095928 10.0.0.140 212.71.133.148 TCP 37216 > www [FIN, ACK] Seq=425 Ack=255 Win=6912 Len=0
14 0.117919 10.0.0.140 212.71.133.148 TCP 37217 > www [SYN] Seq=0 Len=0 MSS=1460 TSV=1765793 TS
15 0.119030 212.71.133.148 10.0.0.140 TCP www > 37216 [ACK] Seq=255 Ack=426 Win=6432 Len=0 TSV=
16 0.139472 212.71.133.148 10.0.0.140 TCP www > 37217 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
17 0.139505 10.0.0.140 212.71.133.148 TCP 37217 > www [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=1765
18 0.139566 10.0.0.140 212.71.133.148 HTTP GET /favicon.ico HTTP/1.1
19 0.168303 212.71.133.148 10.0.0.140 TCP www > 37217 [ACK] Seq=1 Ack=356 Win=6432 Len=0 TSV=1
Frame 8 (490 bytes on wire, 490 bytes captured)
Ethernet II, Src: CompalCo_e7:52:4d (00:16:d4:e7:52:4d), Dst: Paradigm_3a:6c:c6 (00:13:64:3a:6c:c6)
Internet Protocol, Src: 10.0.0.140 (10.0.0.140), Dst: 212.71.133.148 (212.71.133.148)
Transmission Control Protocol, Src Port: 37216 (37216), Dst Port: www (80), Seq: 1, Ack: 1, Len: 424
Hypertext Transfer Protocol
0000 00 13 64 3a 6c c6 00 16 d4 e7 52 4d 08 00 45 00 ..d:l... ..RM..E.
0010 01 dc b7 6a 40 00 40 06 1d 4a 0a 00 00 8c d4 47 ...j@.@. .J.....G
0020 85 94 91 60 00 50 85 ac 46 e6 cf 9e e1 a5 80 18 ...`.P.. F.......
0030 00 2e 66 36 00 00 01 01 08 0a 00 1a f1 93 4e 18 ..f6.... ......N.
0040 50 6e 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 PnGET / HTTP/1.1

THE SPINNING CUBE OF POTENTIAL DOOM

http://www.nersc.gov/nusers/security/TheSpinningCube.php


DPORT 65535
SRC 255.25
SRC 0.0.0.0
DPORT 0
DST 216.17
DST 216.179.125.127


223.255.255.255
0.0.0.0
65535
0
128.55.0.0
128.55.255.255



RUMINT

http://www.rumint.org/

ANALÝZA PODEZŘELÝCH PAKETŮ

TCPFLOW
http://www.circlemud.org/~jelson/software/tcpflow/
TCPTRACE
http://jarok.cs.ohiou.edu/software/tcptrace/
WIRESHARK
..Follow tcp stream

ODDĚLENÍ LEGITIMNÍHO PROVOZU

MEDOVÉ HRNCE (HONEYPOTS)

- s nízkou interaktivitou
- s vysokou interaktivitou

S NÍZKOU INTERAKTIVITOU

HONEYD
http://www.honeyd.org/

NEPENTHES
http://nepenthes.mwcollect.org/

HONEYD

- sítě virtuálních zařízení
- síťové topologie s dedikovanými směrovači
- latence a simulované ztráty paketů
- ARPD

```
create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows uptime 1728650
set windows maxfds 3
set windows default tcp action reset
add windows tcp port 80 "sh /usr/share/honeyd/scripts/win32/web.sh"
add windows tcp port 22 "/usr/share/honeyd/scripts/ssh.sh"

create router
set router personality "Cisco 1601R router running IOS 12.1(5)"
set router default tcp action reset
add router tcp port 23 "/usr/share/honyed/scripts/router-telnet.pl"

bind 10.3.0.1 router
bind 10.3.1.1 router
bind 10.3.1.12 windows
```

NEPENTHES

- emuluje známé bezpečnostní díry
- download škodlivého kódu
- zasílání škodlivého kódu k analýze

Norman Sandbox

http://www.norman.com/microsites/nsic/

```
18052008 16:58:46 debug net handler] Connection Socket TCP (accept) 86.133.121.99:4971 -> 212.110.251.116:80 CLOSED
18052008 16:58:46 debug net mgr] Deleting Socket TCP (accept) 86.133.121.99:4971 -> 212.110.251.116:80 due to closed connection
18052008 16:58:46 spam net handler]
18052008 16:58:46 spam net handler] Socket TCP (accept) 86.133.121.99:4971 -> 212.110.251.116:80 clearing DialogueList (1 entries)
18052008 16:58:46 spam net handler] Removing Dialog "IISDialogue"
18052008 16:58:46 spam mgr event]
18052008 16:59:02 debug net mgr] Socket TCP (bind) 0.0.0.0:0 -> 0.0.0.0:80
ialogueFactory ASN1 Dialogue Factory creates dialogues for the SMB and IIS flaw killbill showed us could Accept a Connection
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam net handler] Socket TCP (accept) 86.133.121.99:3113 -> 212.110.251.16:80
18052008 16:59:02 spam net handler] Adding Dialogue ASN1 Dialogue Factory
18052008 16:59:02 spam mgr event]
18052008 16:59:02 debug net mgr] Accepted Connection Socket TCP (accept) 86.133.121.99:3113 -> 212.110.251.16:80
1 Sockets in list
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam mgr event]
18052008 16:59:02 spam net handler] doRecv() 51
18052008 16:59:02 spam sc handler]
18052008 16:59:02 spam sc handler] Shellcode is 51 bytes long
18052008 16:59:02 spam sc handler]
18052008 16:59:02 spam sc handler] Shellcode is 51 bytes long
18052008 16:59:02 spam sc handler]
18052008 16:59:02 spam sc handler] Shellcode is 51 bytes long
18052008 16:59:02 info sc handler] Detected generic prepended unencoded URL Shellcode: "http://217.146.187.124/status.html"
18052008 16:59:02 spam mgr event]
18052008 16:59:02 spam handler event module]
18052008 16:59:02 spam down mgr] Checking Host 217.146.187.124 for locality
18052008 16:59:02 spam down mgr] Host 217.146.187.124 is valid ip
18052008 16:59:02 info down mgr] Handler http download handler will download http://217.146.187.124/status.html
18052008 16:59:02 spam down handler]
18052008 16:59:02 info down handler] Resolving host http://217.146.187.124/status.html ...
18052008 16:59:02 debug spam fixme] addDNS: Adding DNS 217.146.187.124 for ()
18052008 16:59:02 debug spam fixme] DNS is ip 217.146.187.124
18052008 16:59:02 info down handler] url 217.146.187.124 resolved
18052008 16:59:02 spam net mgr]
18052008 16:59:02 debug net handler] Connecting 212.110.251.16:0 -> 217.146.187.124:80
18052008 16:59:02 spam mgr event]
18052008 16:59:02 spam mgr event]
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam down handler dia]
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam down handler dia] HTTP REQ
ET /status.html HTTP/1.0
ser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
ccept: */*
ost: 217.146.187.124:80
onnection: close


18052008 16:59:02 debug net handler] giving data to HTTPDialogue
18052008 16:59:02 debug net handler] sended 151 from 151 bytes
18052008 16:59:02 spam net handler] done sending 151 bytes
18052008 16:59:02 spam net handler]
18052008 16:59:02 spam mgr event]
18052008 16:59:02 spam net handler] doRecv() 572
```

PROJEKT DARKNET

- http://www.team-cymru.org/
- běžně směrovaná síť bez služeb
- z hlediska běžného uživatele prázdná
- obsahuje alespoň jeden server analyzující všechny pakety, které se v síti objeví
- NIDS sonda
- omyl, chybná konfigurace, nekalá aktivita

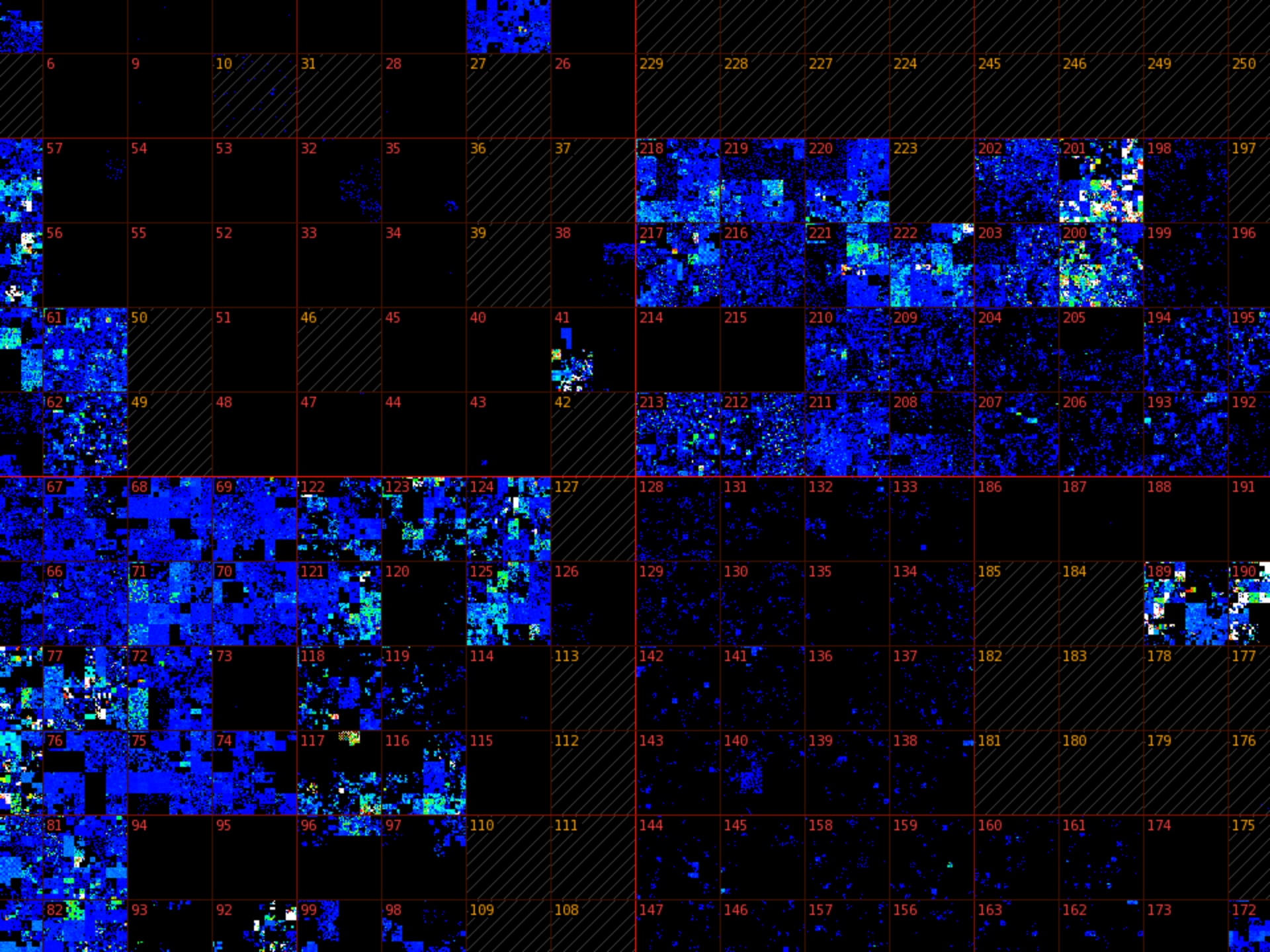
KONFIGURACE DARKNETU

- minimálně jedna síť typu C
- zabezpečený dedikovaný směrovač
- směruje veškerá data na „naslouchací“ rozhraní serveru

TCPDUMP (http://www.tcpdump.org/)

ARGUS(http://www.qosient.com/argus/flow.htm)

rozhraní administrace serveru


6 9 10 31 28 27 26 229 228 227 224 245 246 249 250
57 54 53 32 35 36 37 218 219 220 223 202 201 198 197
56 55 52 33 34 39 38 217 216 221 222 203 200 199 196
61 50 51 46 45 40 41 214 215 210 209 204 205 194 195
62 49 48 47 44 43 42 213 212 211 208 207 206 193 192
67 68 69 122 123 124 127 128 131 132 133 186 187 188 191
66 71 70 121 120 125 126 129 130 135 134 185 184 189 190
77 72 73 118 119 114 113 142 141 136 137 182 183 178 177
76 75 74 117 116 115 112 143 140 139 138 181 180 179 176
81 94 95 96 97 110 111 144 145 158 159 160 161 174 175
82 93 92 99 98 109 108 147 146 157 156 163 162 173 172

KLIENTSKÉ HONEYPOTY

MITRE HoneyClient
http://www.honeyclient.org/
Capture – HPC
https://projects.honeynet.org/capture-hpc/
HoneyC
https://projects.honeynet.org/honeyc/
SpyBye
http://www.spybye.org/
SHELIA
http://www.cs.vu.nl/~herbertb/misc/shelia/

LIMITY

- pasivní zařízení
- neodhalí cílený útok
- neodhalí červa, který se propaguje pomocí hintlistu
- zkušený útočník je může identifikovat