Rogue Email Server Detection

presented by

US-CERT/NetSA

Rogue Server Reporting

- Rule:
  - Only SMTP servers should provide SMTP service
    - Port 25 is off-limits for all others
- Success of the system depends on:
  - Developing/Maintaining Whitelists
  - Timely reporting
  - **Feedback**

Finding Servers

- Analyzed all hosts observed to have SMTP connections
  - SMTP connections
    - Src/Dest port is 25
    - At least 3 packets (unidirectional)
    - At least 120 bytes (unidirectional)
- Evaluate hosts based on their characteristics

Characteristics

- Administrative
  - Naming convention (SMTP, MAIL, RELAY, MX, etc.)
  - MX Records
- Behavioral
  - History of being servers
  - Majority of their traffic is mail related
    - We use 85% for a threshold
    - Based on observations of verified mail servers

Whitelist Tuning

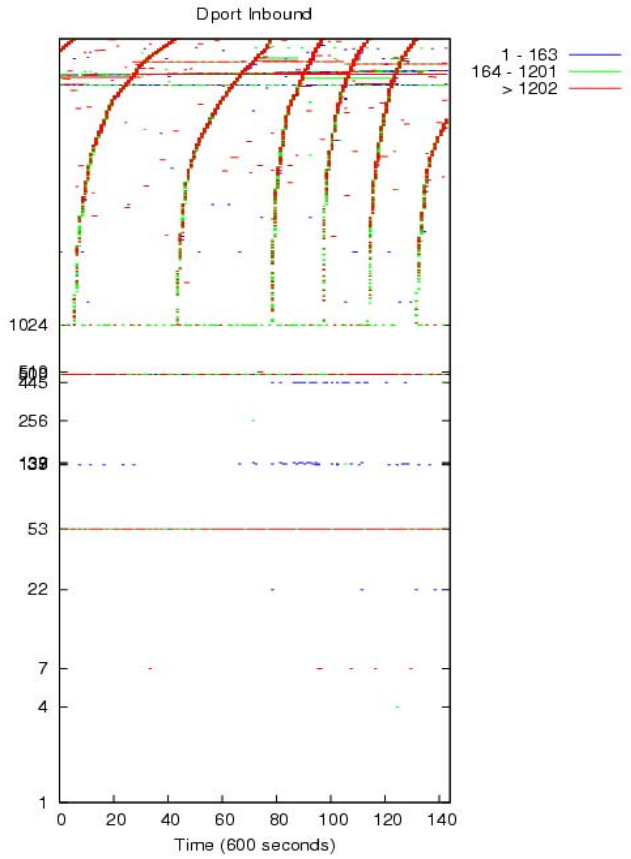
- The initial whitelist was verified by hand
- Add new addresses to whitelist if:
  - Administrative and/or behavioral characteristics are consistent with that of an SMTP server
  - Verified as being an SMTP server by the network administrator

Reporting

- Report includes:
  - Images of port usage:
    - Dport inbound
    - Sport outbound
  - List of external clients and servers
  - History of activity

Existence Plot

- Color based on the 1st and 3rd quartile
- 2D plot
  - *X*-axis is time (binned)
  - *Y*-axis is port number
- Label the reserved ports only



Agency successes

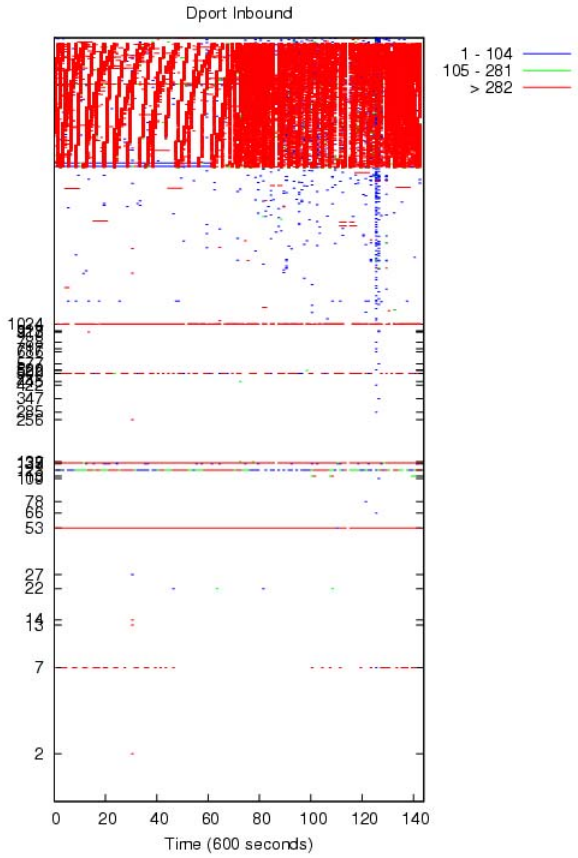
- 2/22/08 – VPN Issue
- 2/26/2008 - New mail servers
- 03/11/2008 - Misconfiguration, config lost, default behavior took over

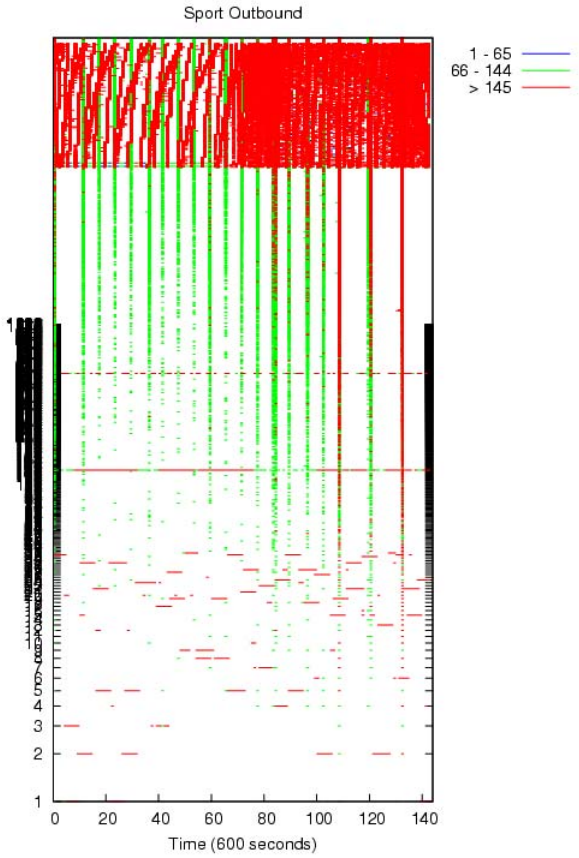
VPN Issue

VPN Issue Background

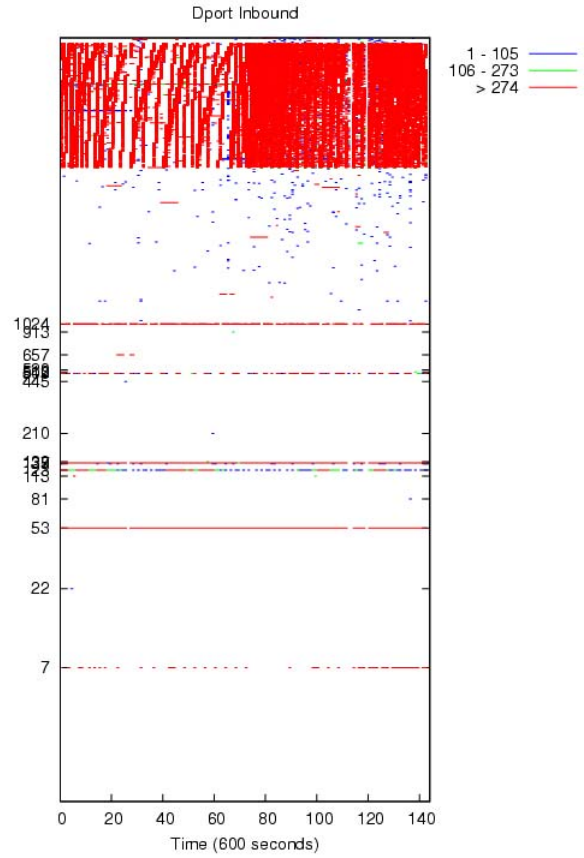
- NetSA observed this host responding on many low ports
- Traffic appeared over a two week period, 02/07/2008 through to 02/20/2008
- Notified agency about traffic on 02/20
- Agency requested traffic from 02/16

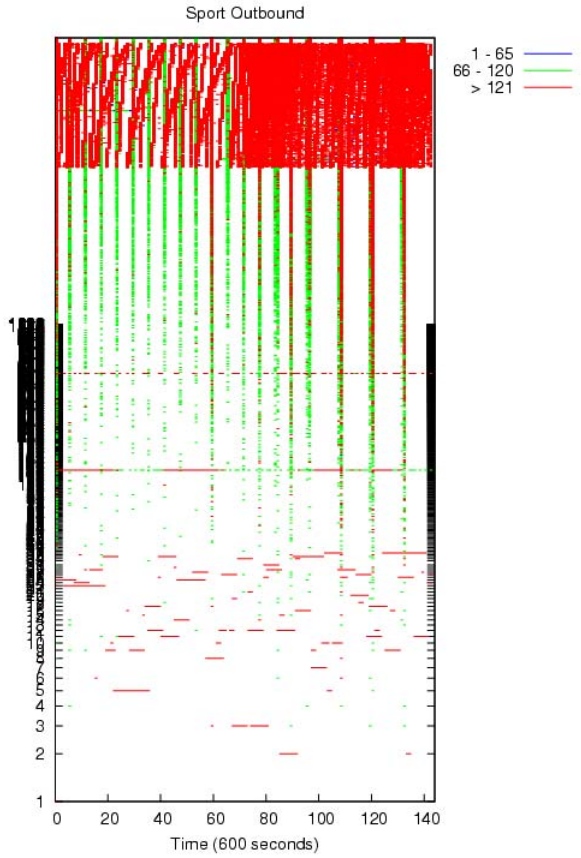
02/07


Dport Inbound
1 - 104
105 - 281
> 282
1024
347
256
139
78
66
53
27
22
14
13
7
2
0
20
40
60
80
100
120
140
Time (600 seconds)

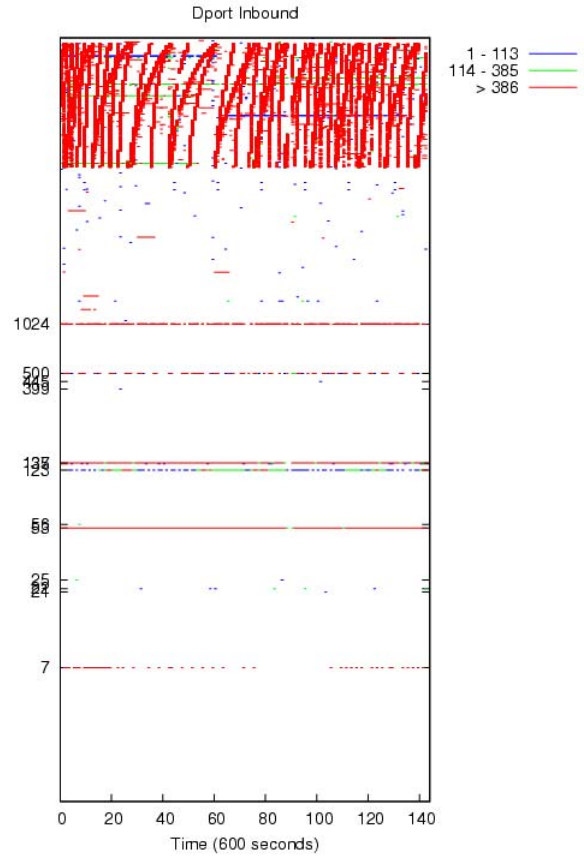

Sport Outbound
1 - 65
66 - 144
> 145
1
2
3
4
5
6
7
0
20
40
60
80
100
120
140
Time (600 seconds)

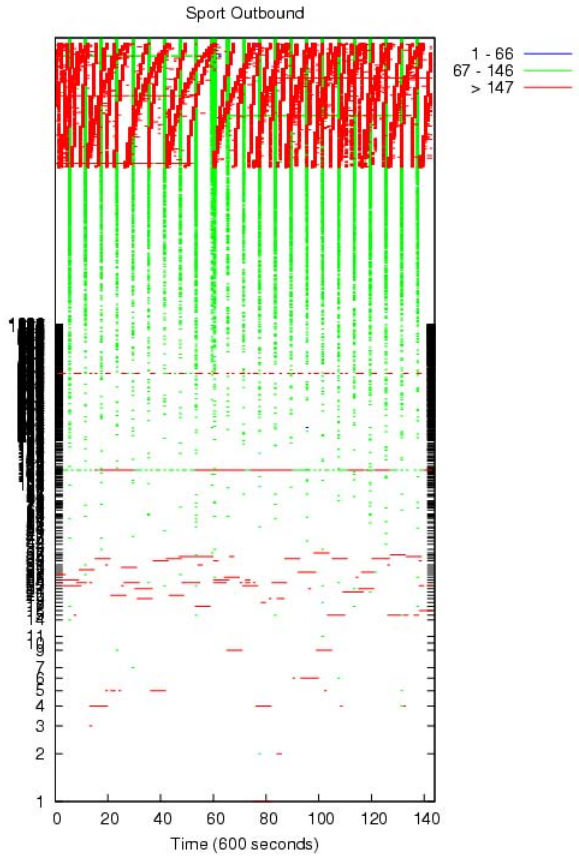
02/08


Dport Inbound
1 - 105
106 - 273
> 274
1024
913
657
445
210
81
53
22
7
0
20
40
60
80
100
120
140
Time (600 seconds)

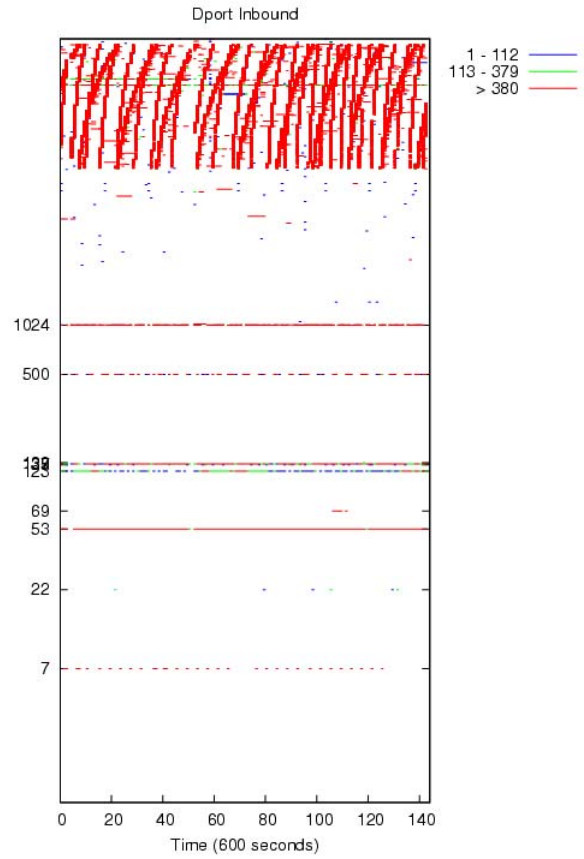

Sport Outbound
1 - 65
66 - 120
> 121
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

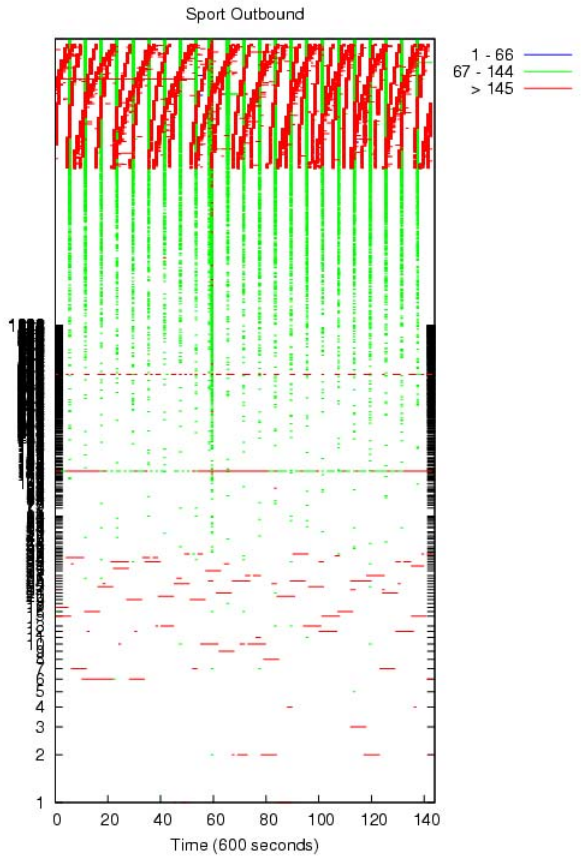
02/09


Dport Inbound
1 - 113
114 - 385
> 386
1024
500
399
135
125
58
25
7
0
20
40
60
80
100
120
140
Time (600 seconds)

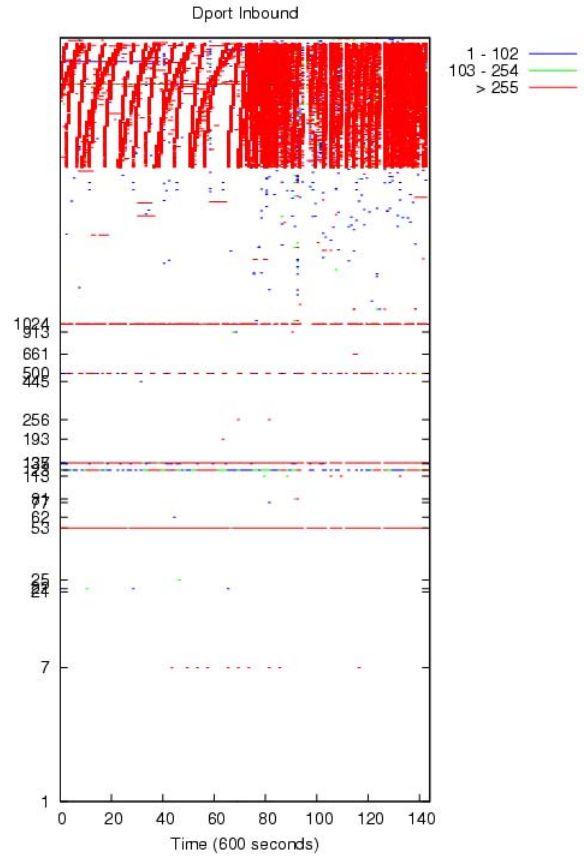

Sport Outbound
1 - 66
67 - 146
> 147
1
2
3
4
0
20
40
60
80
100
120
140
Time (600 seconds)

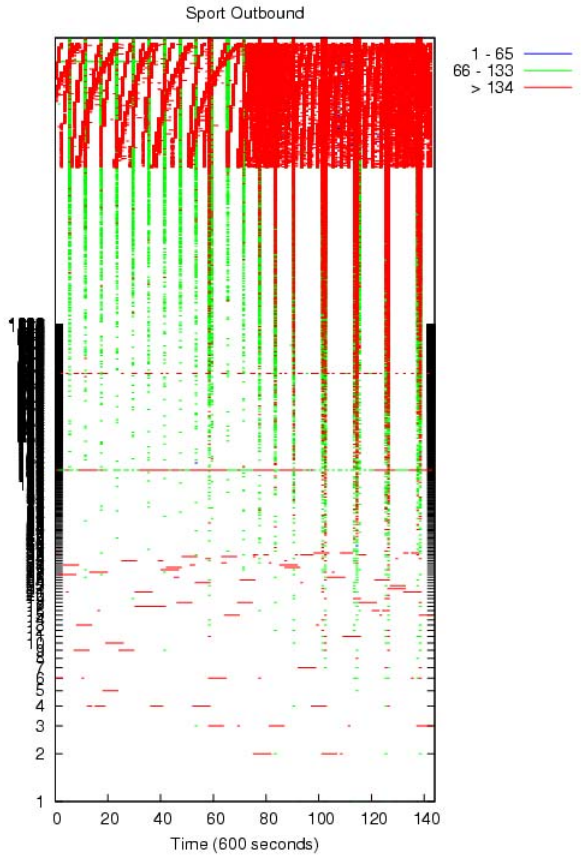
02/10


Dport Inbound
1 - 112
113 - 379
> 380
1024
500
69
53
22
7
0
20
40
60
80
100
120
140
Time (600 seconds)

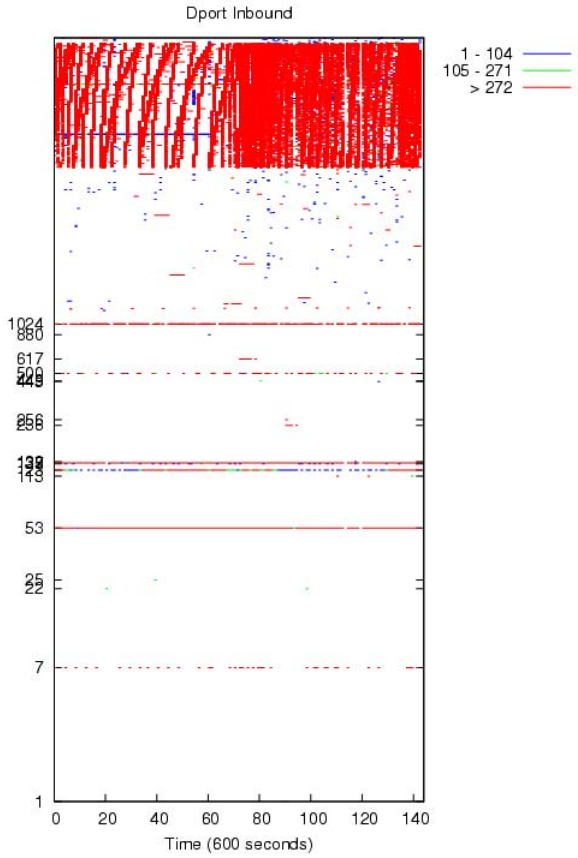

Sport Outbound
1 - 66
67 - 144
> 145
1
2
3
4
0
20
40
60
80
100
120
140
Time (600 seconds)

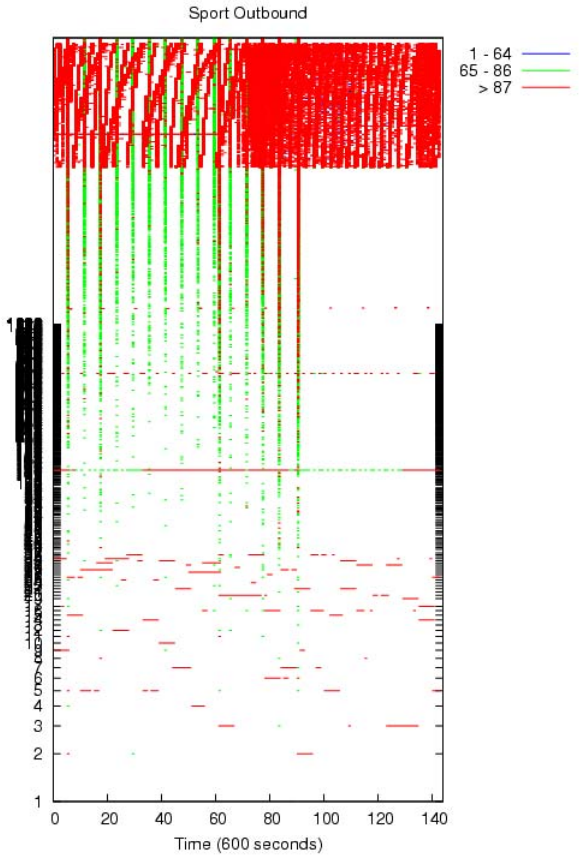
02/11


Dport Inbound
1 - 102
103 - 254
> 255
1024
913
661
500
445
256
193
7
1
0
20
40
60
80
100
120
140
Time (600 seconds)

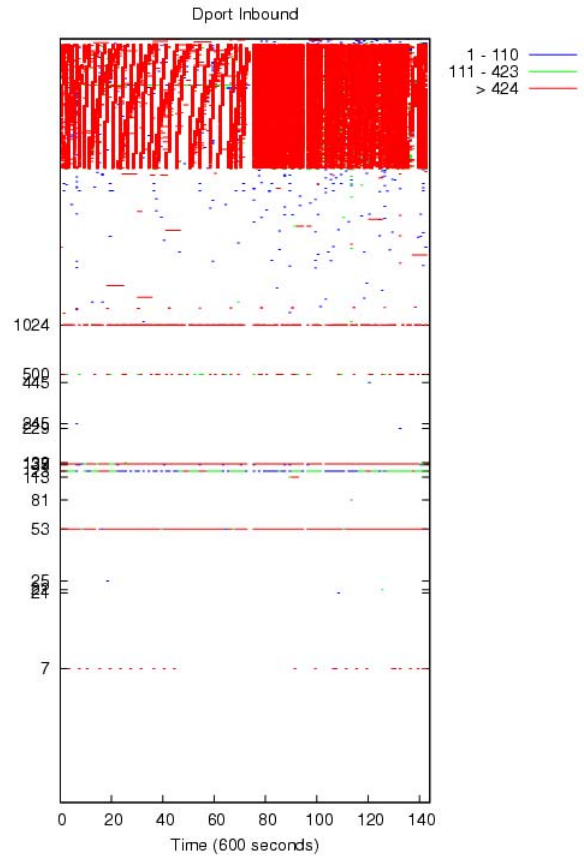

Sport Outbound
1 - 65
66 - 133
> 134
1
2
3
4
0
20
40
60
80
100
120
140
Time (600 seconds)

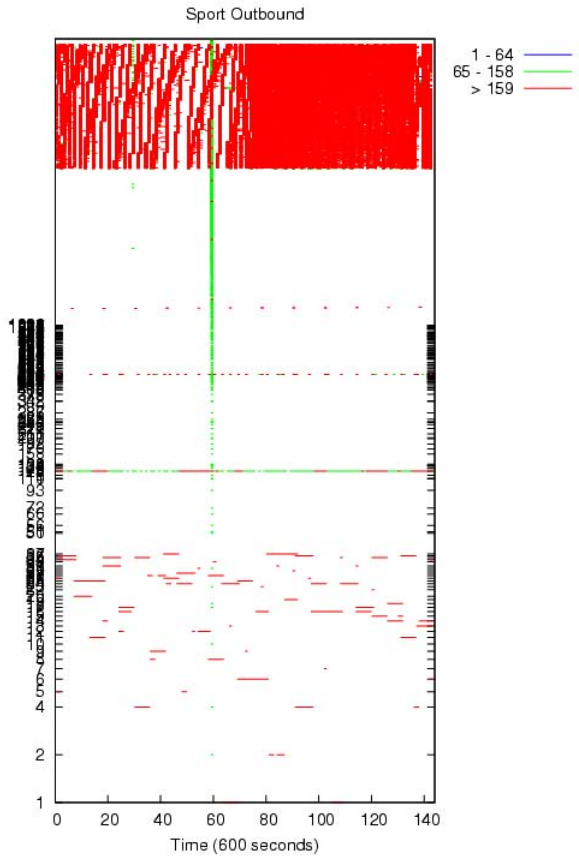
02/12


Dport Inbound
1 - 104
105 - 271
> 272
1024
860
617
500
445
256
238
143
53
25
22
7
1
0
20
40
60
80
100
120
140
Time (600 seconds)

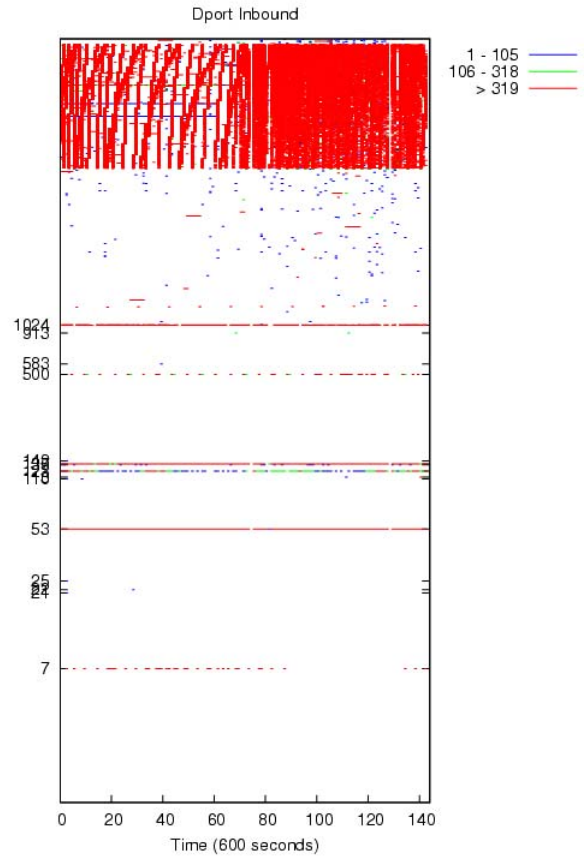

Sport Outbound
1 - 64
65 - 86
> 87
1
2
3
4
5
6
7
0
20
40
60
80
100
120
140
Time (600 seconds)

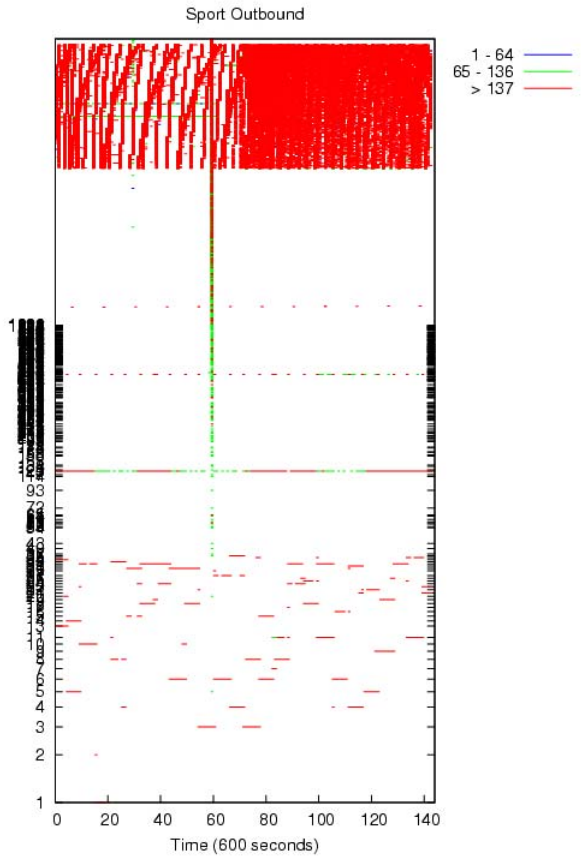
02/13


Dport Inbound
1 - 110
111 - 423
> 424
1024
500
445
81
53
25
7
0
20
40
60
80
100
120
140
Time (600 seconds)

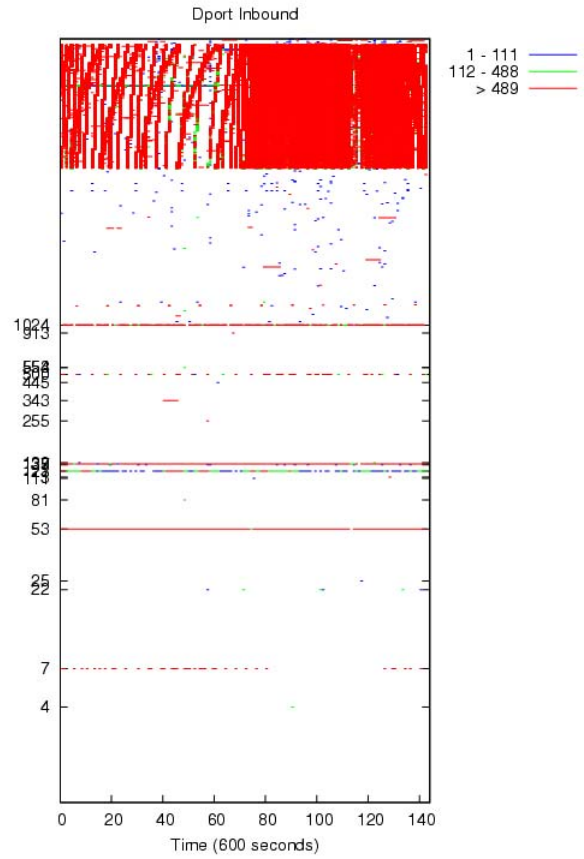

Sport Outbound
1 - 64
65 - 158
> 159
4
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

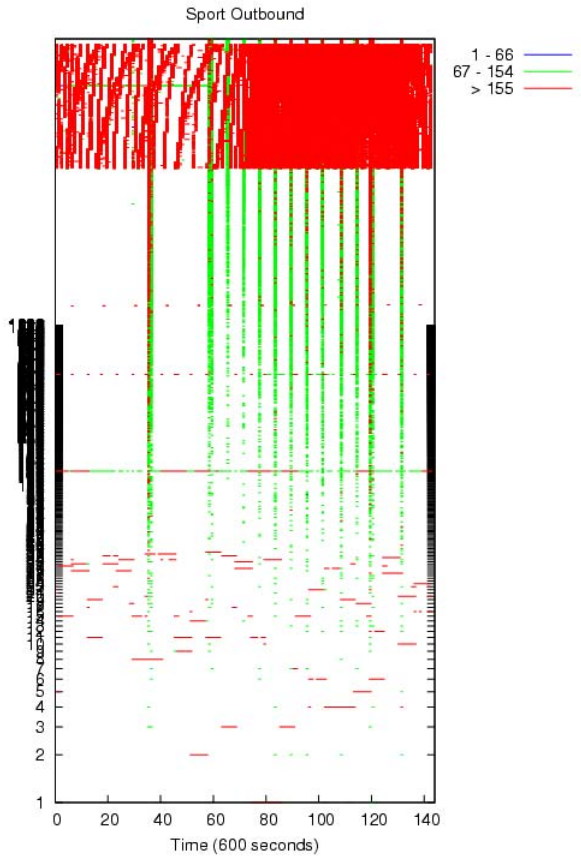
02/14


Dport Inbound
1 - 105
106 - 318
> 319
1024
913
583
500
53
25
7
0
20
40
60
80
100
120
140
Time (600 seconds)

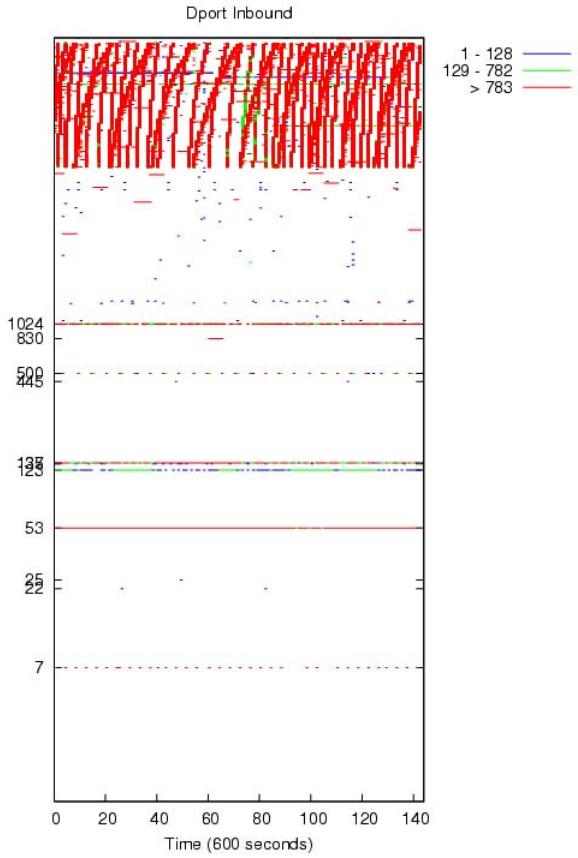

Sport Outbound
1 - 64
65 - 136
> 137
93
72
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

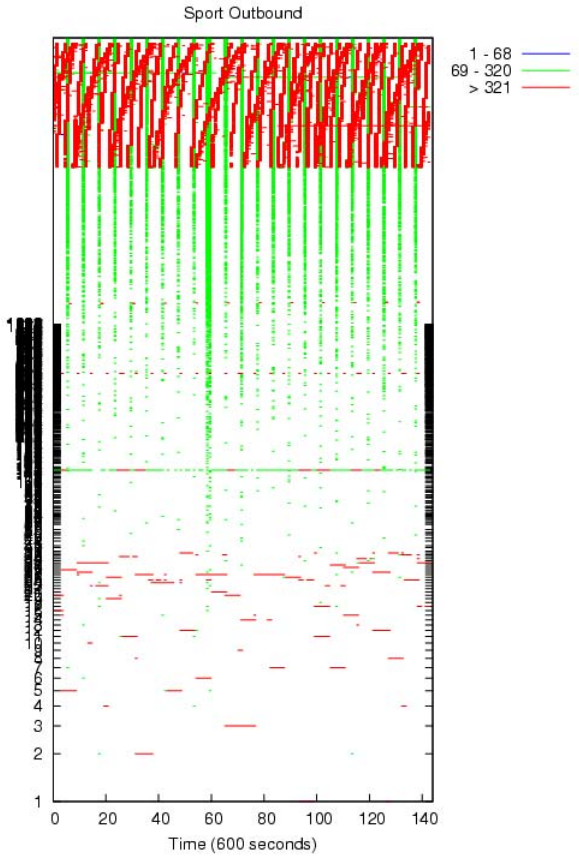
02/15


Dport Inbound
1 - 111
112 - 488
> 489
1024
513
343
255
81
53
25
22
7
4
0
20
40
60
80
100
120
140
Time (600 seconds)

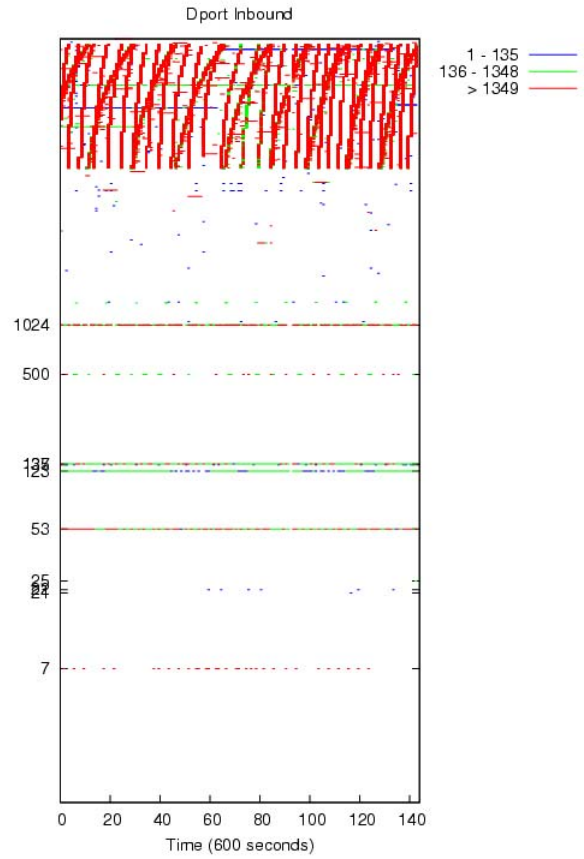

Sport Outbound
1 - 66
67 - 154
> 155
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

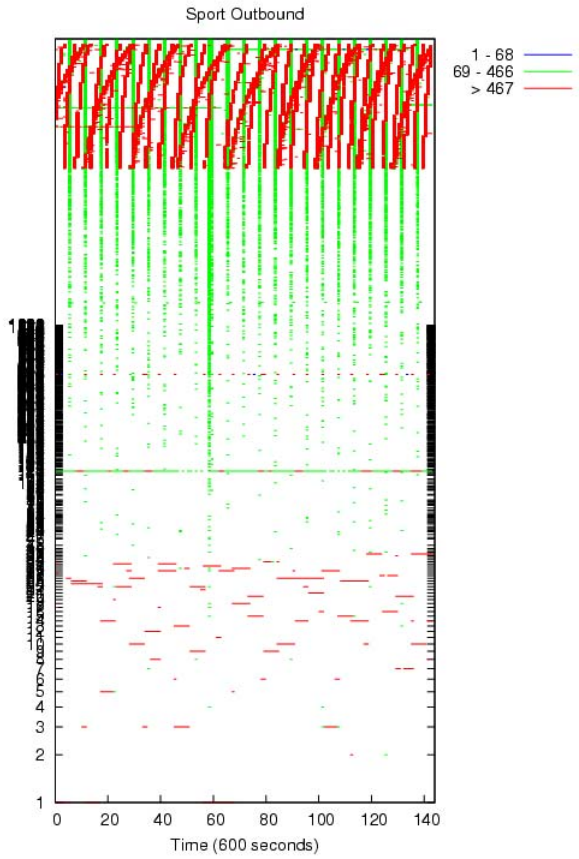
02/16


Dport Inbound
1 - 128
129 - 782
> 783
1024
830
500
445
135
125
53
25
22
7
0
20
40
60
80
100
120
140
Time (600 seconds)

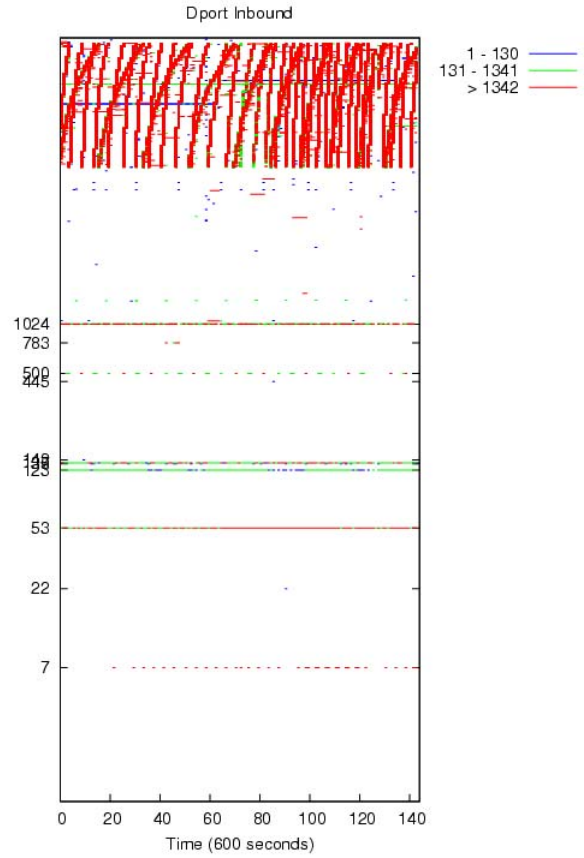

Sport Outbound
1 - 68
69 - 320
> 321
1
2
3
4
5
6
7
0
20
40
60
80
100
120
140
Time (600 seconds)

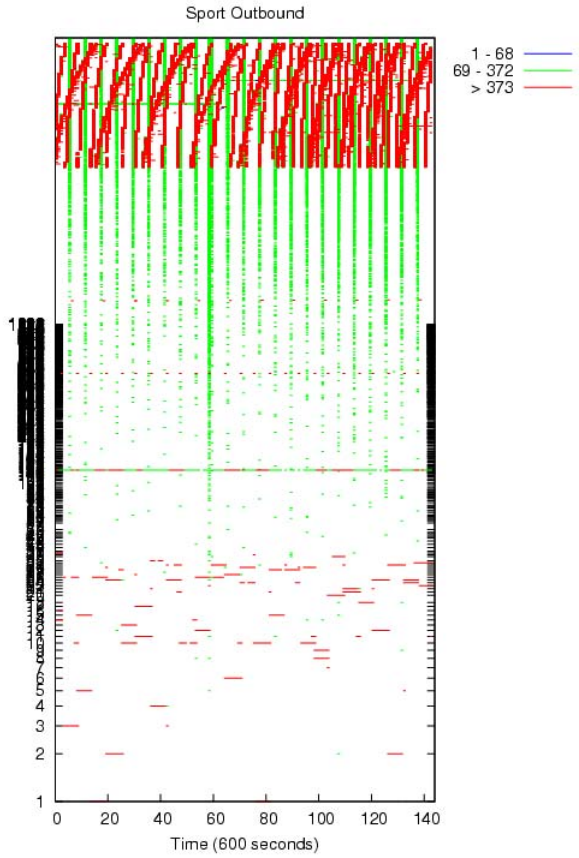
02/17


Dport Inbound
1 - 135
136 - 1348
> 1349
1024
500
53
7
0
20
40
60
80
100
120
140
Time (600 seconds)

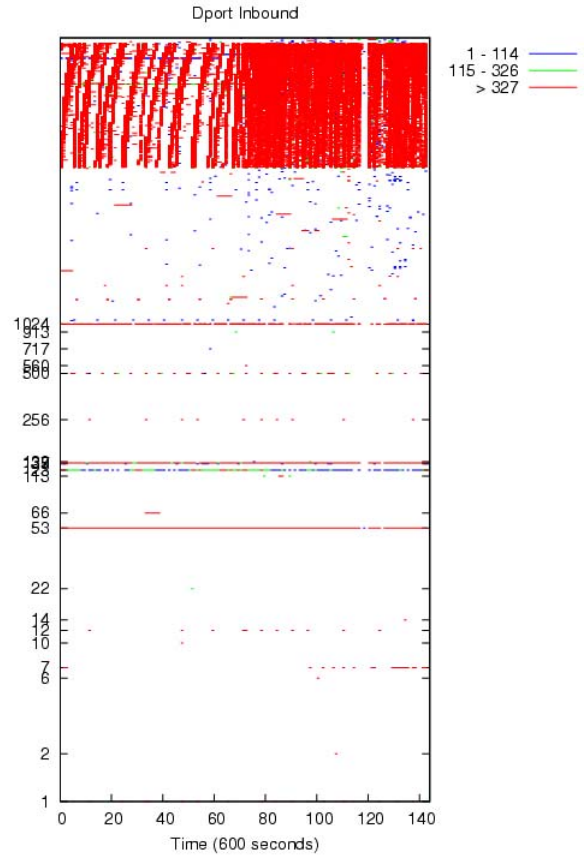

Sport Outbound
1 - 68
69 - 466
> 467
1
2
3
4
0
20
40
60
80
100
120
140
Time (600 seconds)

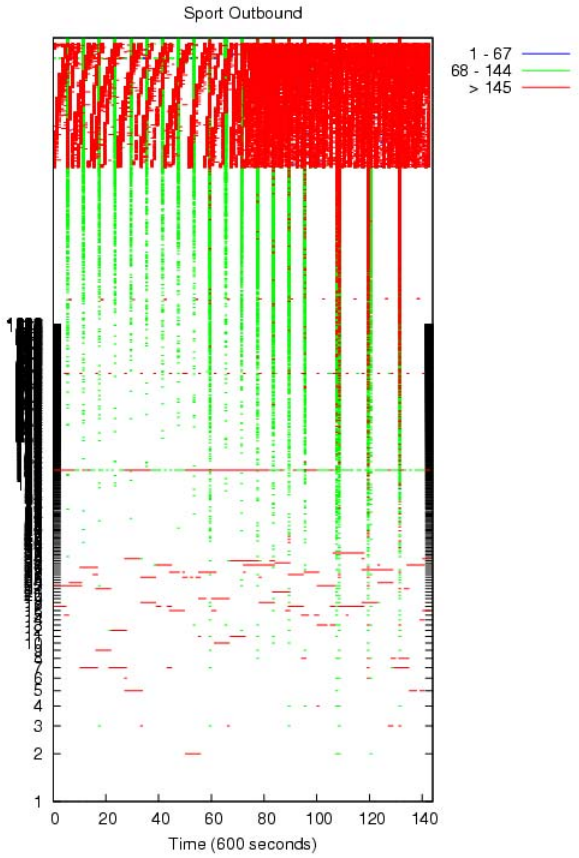
02/18


Dport Inbound
1 - 130
131 - 1341
> 1342
1024
783
500
445
53
22
7
0
20
40
60
80
100
120
140
Time (600 seconds)

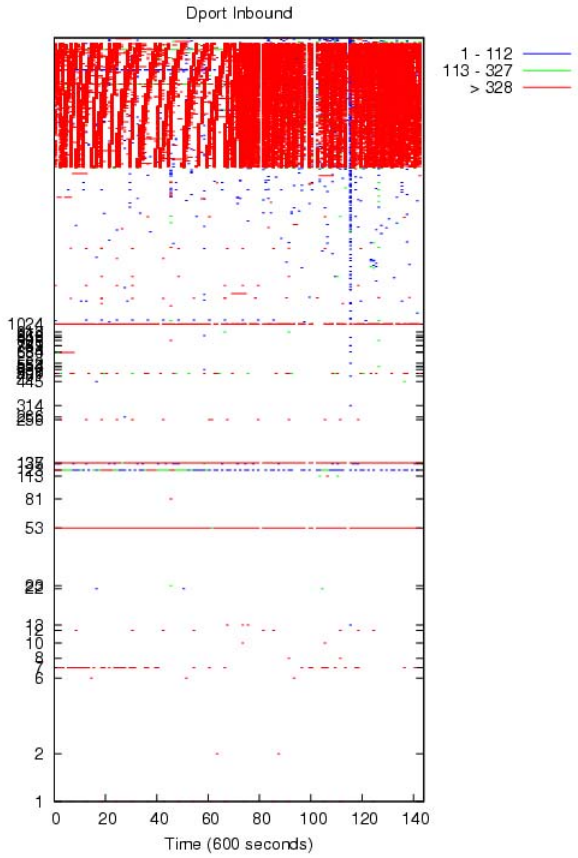

Sport Outbound
1 - 68
69 - 372
> 373
1
2
3
4
0
20
40
60
80
100
120
140
Time (600 seconds)

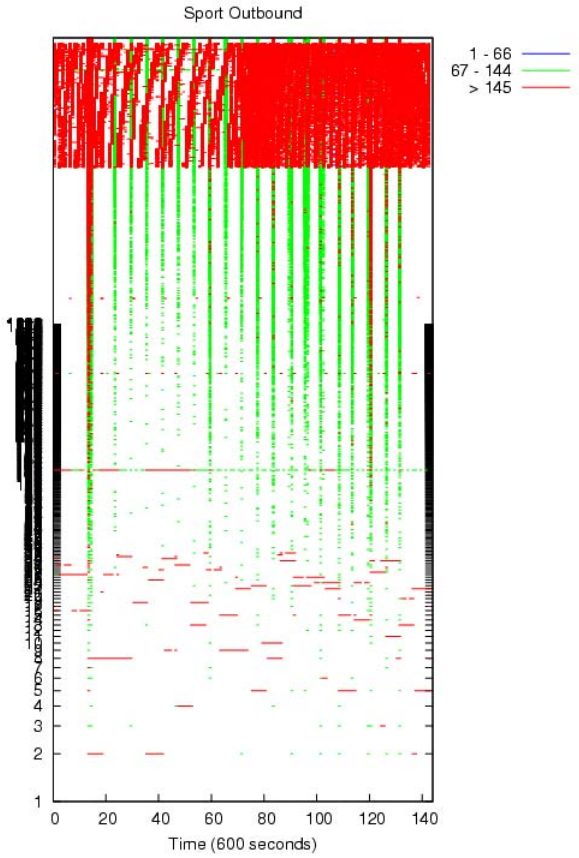
02/19


Dport Inbound
1 - 114
115 - 326
> 327
1024
913
717
560
500
256
143
66
53
22
14
12
10
7
6
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

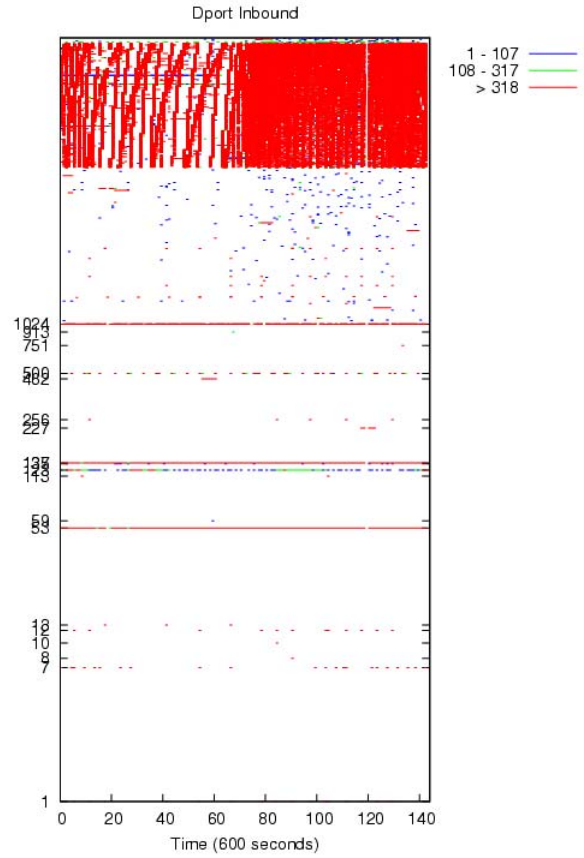

Sport Outbound
1 - 67
68 - 144
> 145
6
5
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

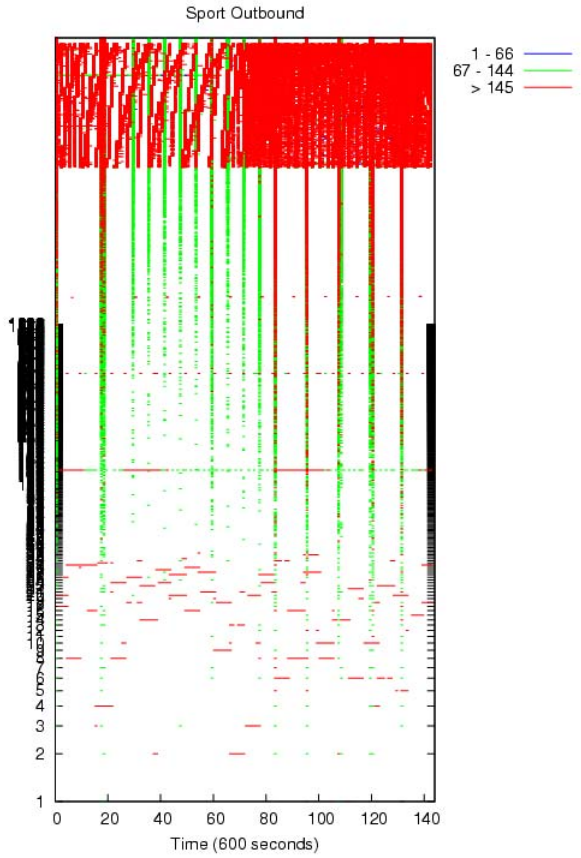
02/20


Dport Inbound
1 - 112
113 - 327
> 328
1024
445
314
137
81
53
25
22
18
10
8
7
6
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)


Sport Outbound
1 - 66
67 - 144
> 145
6
5
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

02/21


Dport Inbound
1 - 107
108 - 317
> 318
1024
913
751
589
482
256
227
135
128
118
59
53
18
10
8
7
1
0
20
40
60
80
100
120
140
Time (600 seconds)


Sport Outbound
1 - 66
67 - 144
> 145
6
5
4
3
2
1
0
20
40
60
80
100
120
140
Time (600 seconds)

VPN Issue Summary

- Heavy activity appeared “normal” for this server but the server was not a known mail server
- US-CERT highlighted activity to agency

VPN Issue Resolution

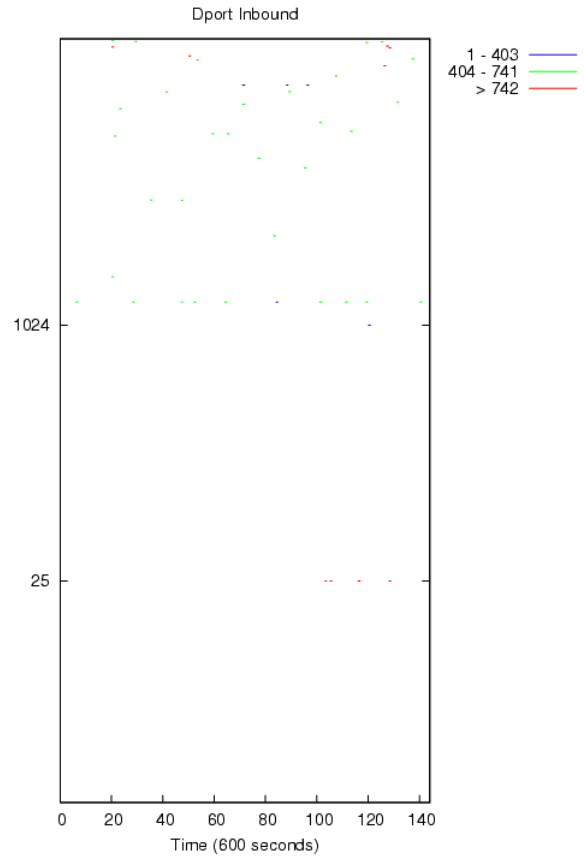
- The agency's ISP said this was legitimate mail traffic
- The traffic should have been traversing over an encrypted VPN tunnel
- Instead the traffic was seen by Einstein going out across the Internet
- The ISP worked to restore the VPN tunnel functionality but only a very small amount of data was transmitted

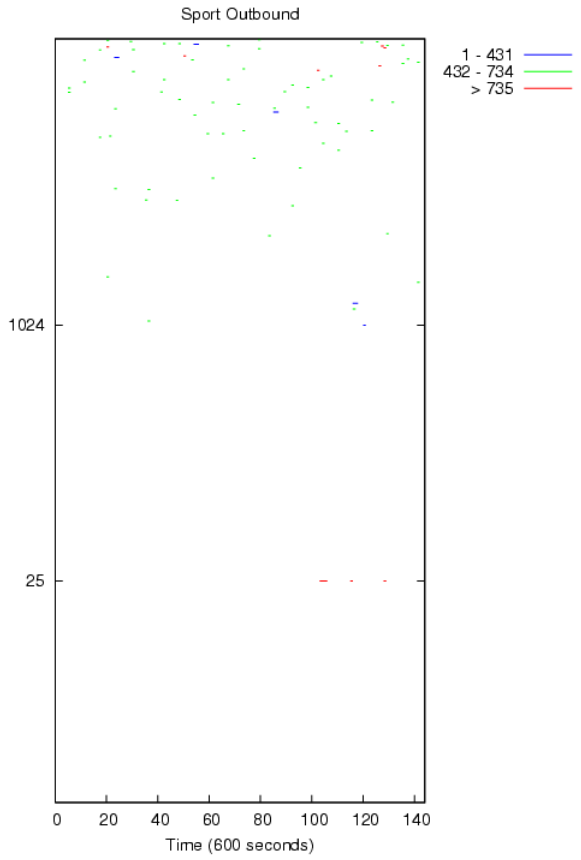
New Mail Servers

Background

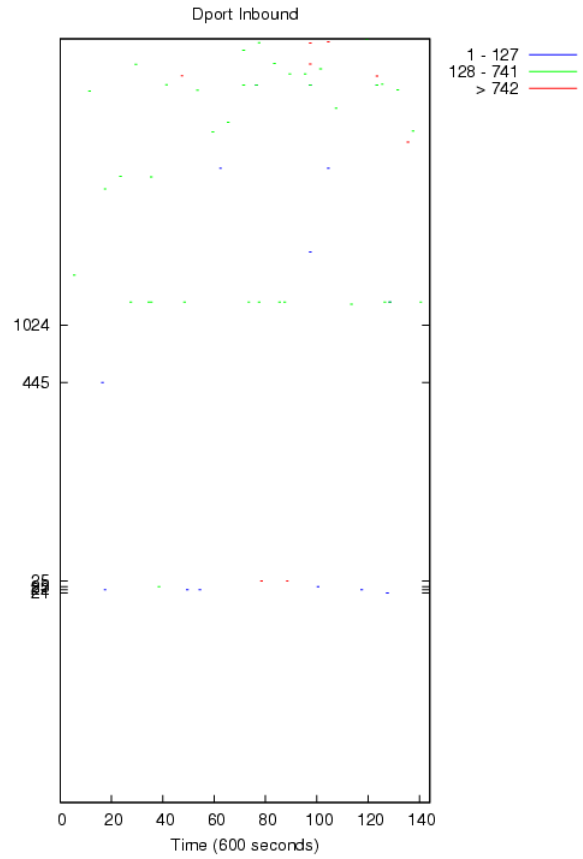
- Agency server exploded in activity level
- Increase from 5 flows per day to an excess of 14,000 flows per day
- This jump started on 2/23/2008

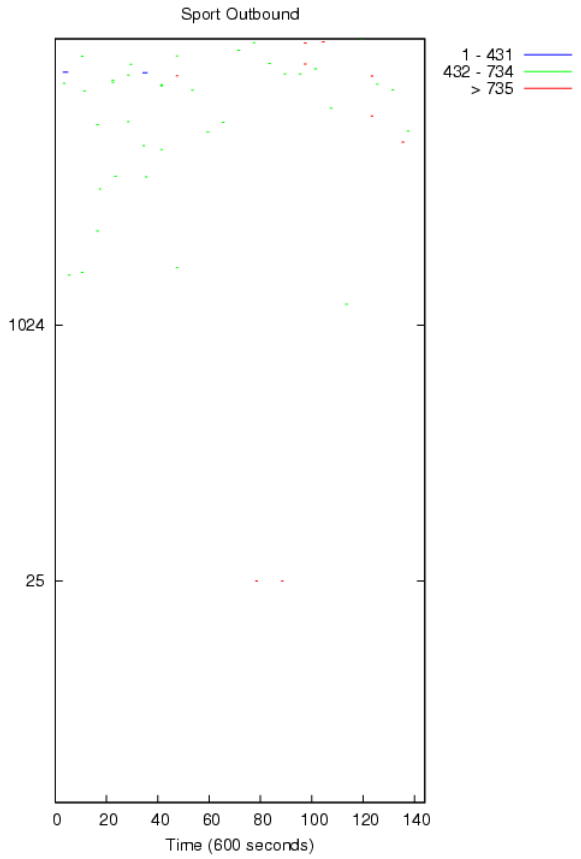
02/21


Dport Inbound
1 - 403
404 - 741
> 742
1024
25
0
20
40
60
80
100
120
140
Time (600 seconds)

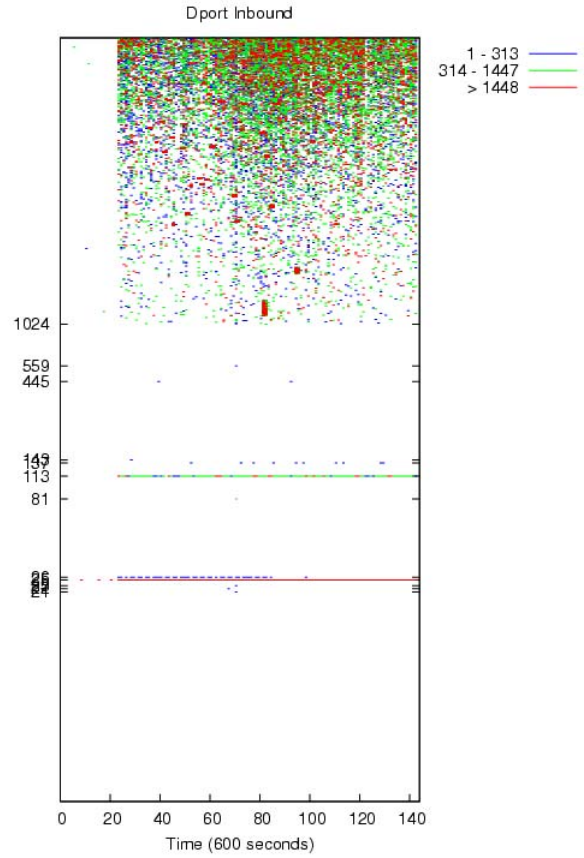

Sport Outbound
1 - 431
432 - 734
> 735
1024
25
0
20
40
60
80
100
120
140
Time (600 seconds)

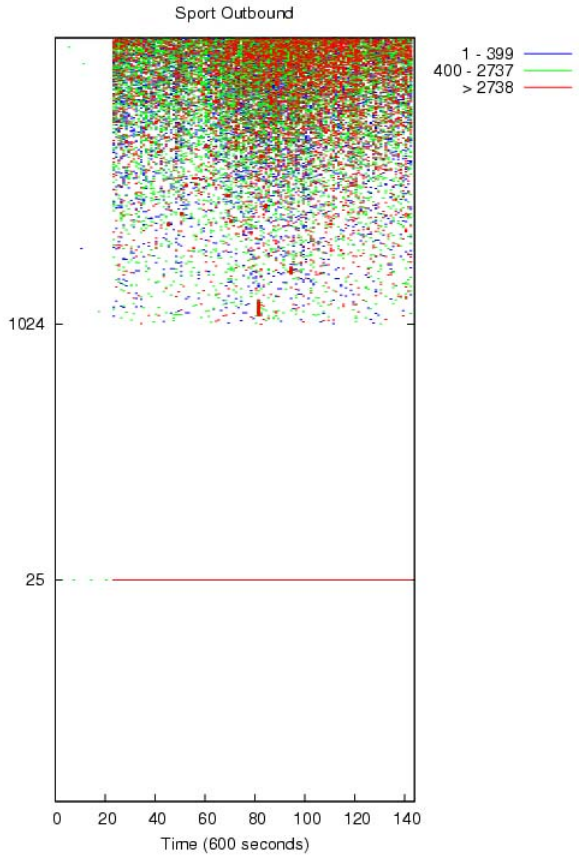
02/22


Dport Inbound
1 - 127
128 - 741
> 742
1024
445
0
20
40
60
80
100
120
140
Time (600 seconds)

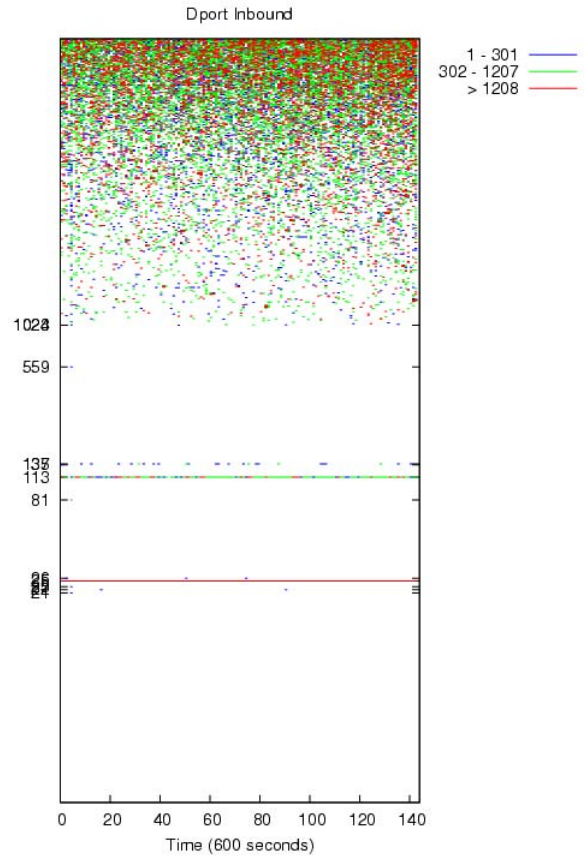

Sport Outbound
1 - 431
432 - 734
> 735
1024
25
0
20
40
60
80
100
120
140
Time (600 seconds)

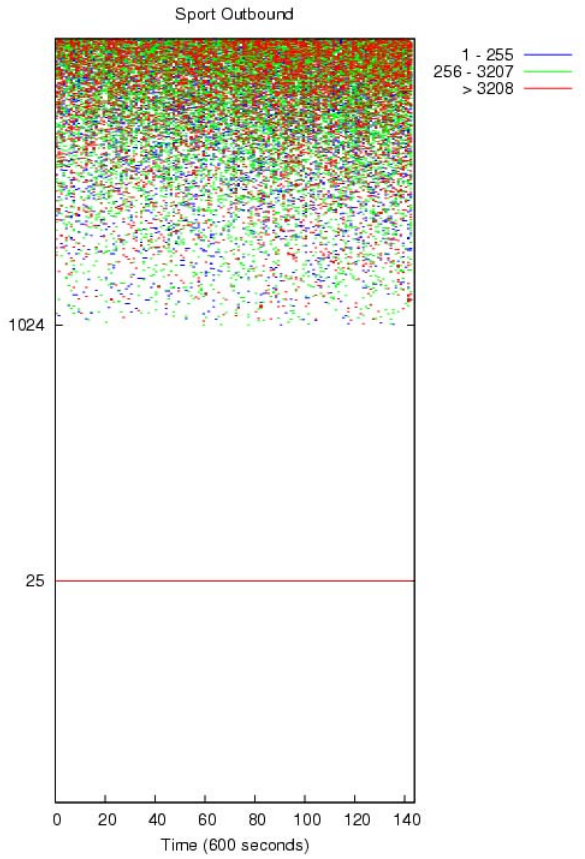
02/23


Dport Inbound
1 - 313
314 - 1447
> 1448
1024
559
445
113
81
0
20
40
60
80
100
120
140
Time (600 seconds)

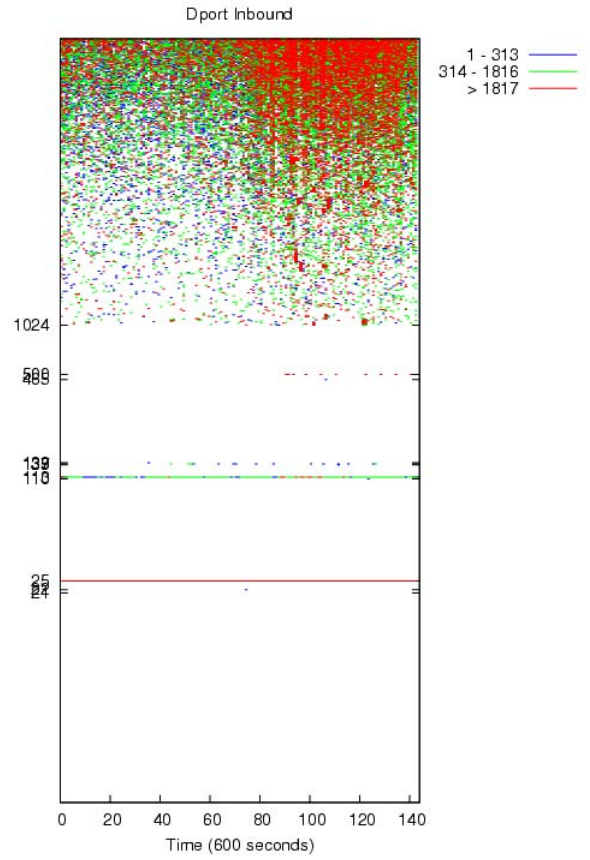

Sport Outbound
1 - 399
400 - 2737
> 2738
1024
25
0
20
40
60
80
100
120
140
Time (600 seconds)

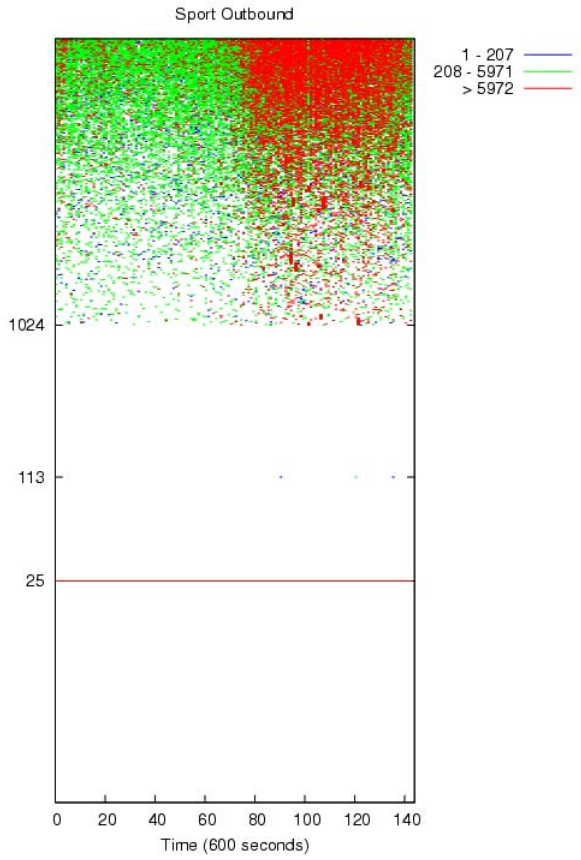
02/24


Dport Inbound
1 - 301
302 - 1207
> 1208
1024
559
137
113
81
25
0
20
40
60
80
100
120
140
Time (600 seconds)

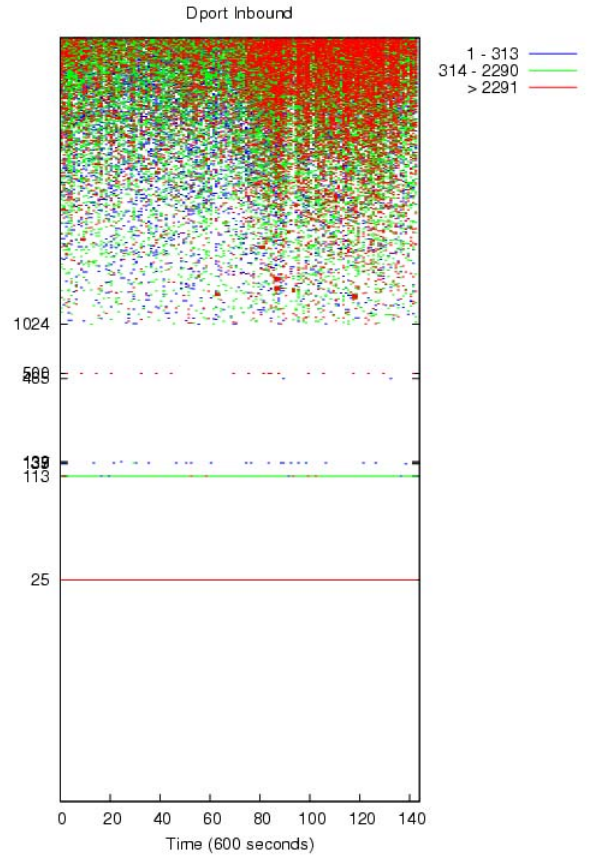

Sport Outbound
1 - 255
256 - 3207
> 3208
1024
25
0
20
40
60
80
100
120
140
Time (600 seconds)

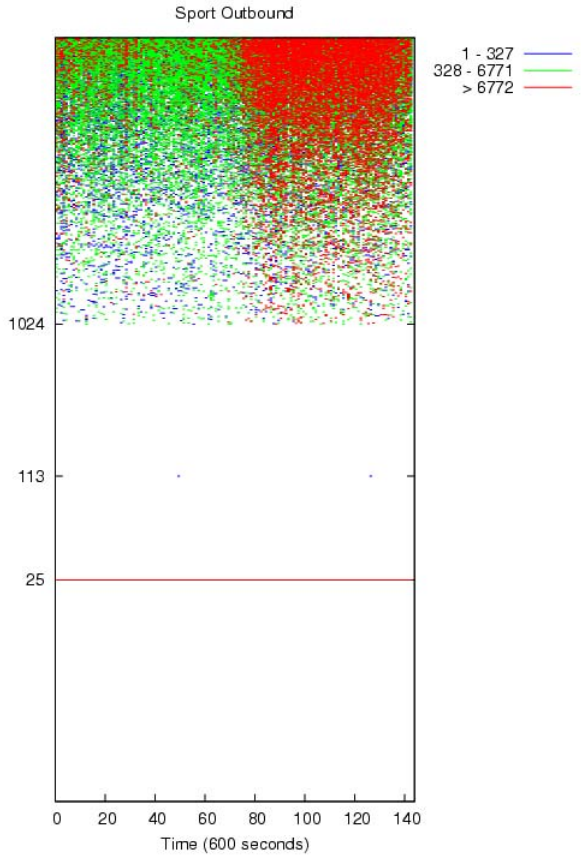
2/25


Dport Inbound
1 - 313
314 - 1816
> 1817
1024
113
25
0
20
40
60
80
100
120
140
Time (600 seconds)

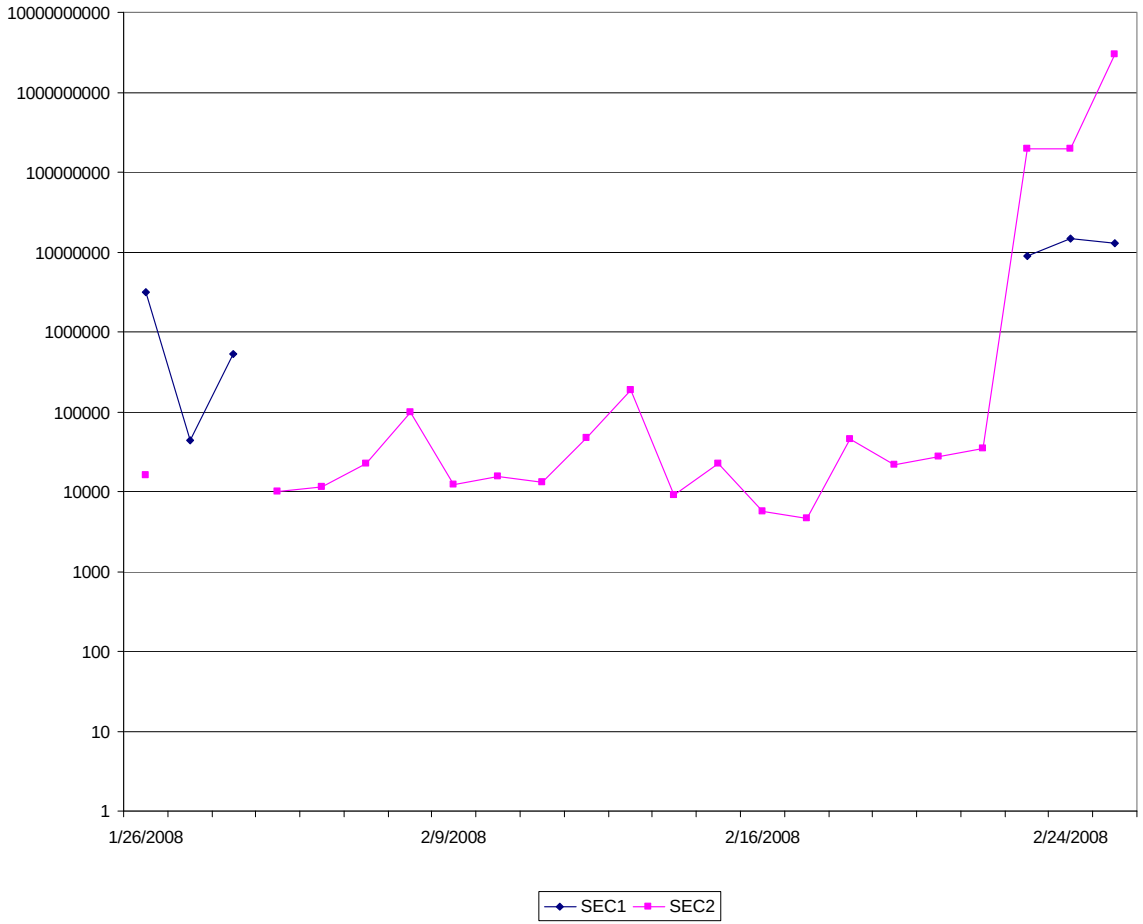

Sport Outbound
1 - 207
208 - 5971
> 5972
1024
113
25
0
20
40
60
80
100
120
140
Time (600 seconds)

2/26


Dport Inbound
1 - 313
314 - 2290
> 2291
1024
113
25
0
20
40
60
80
100
120
140
Time (600 seconds)


Sport Outbound
1 - 327
328 - 6771
> 6772
1024
113
25
0
20
40
60
80
100
120
140
Time (600 seconds)

Byte volume


10000000000
1000000000
100000000
10000000
1000000
100000
10000
1000
100
10
1
1/26/2008
2/9/2008
2/16/2008
2/24/2008
SEC1
SEC2

New Servers Summary

- Agency servers showed low traffic volume and then a sudden increase in traffic
- Continued monitoring showed significant spike in byte volume

New Servers Resolution

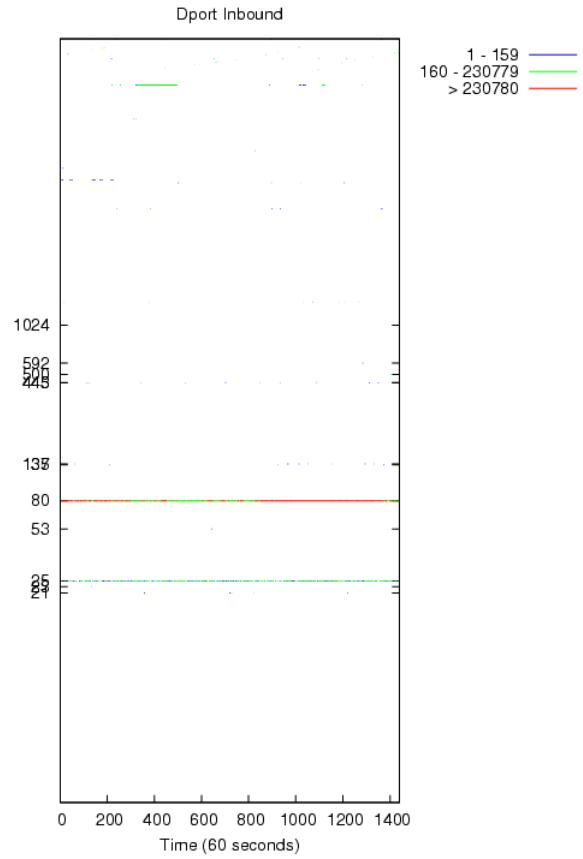
- Agency reported that they had stood up two new mail servers in two locations

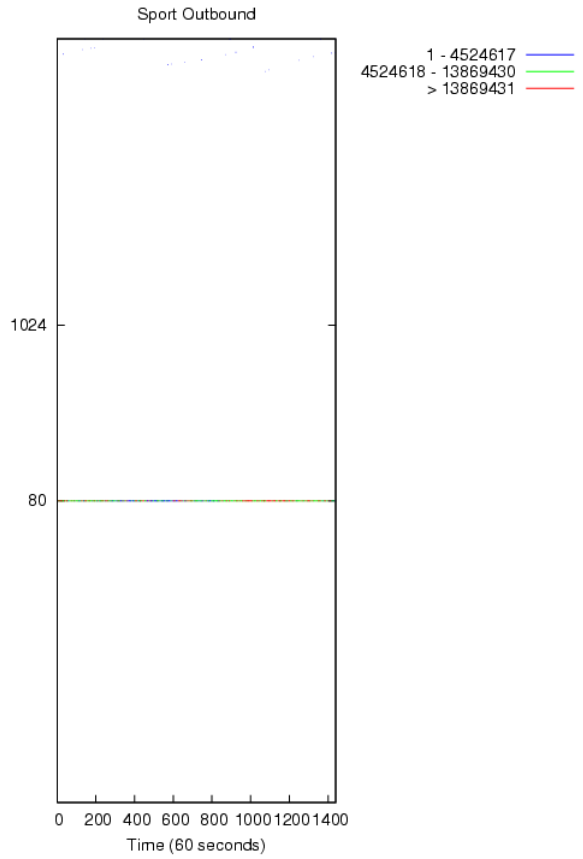
Misconfiguration

Background

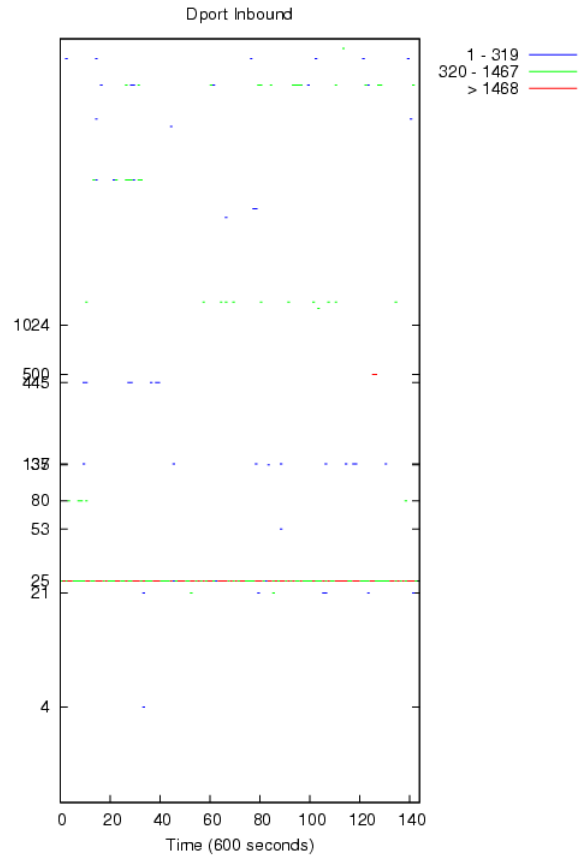
- On 03/10, an agency host initiated SMTP connections with 75 external mail servers within a 1 minute period
- The host was not a known SMTP server and had exhibited very limited SMTP traffic in the past
- The only exception was a similar short burst of activity on 2/8/2008

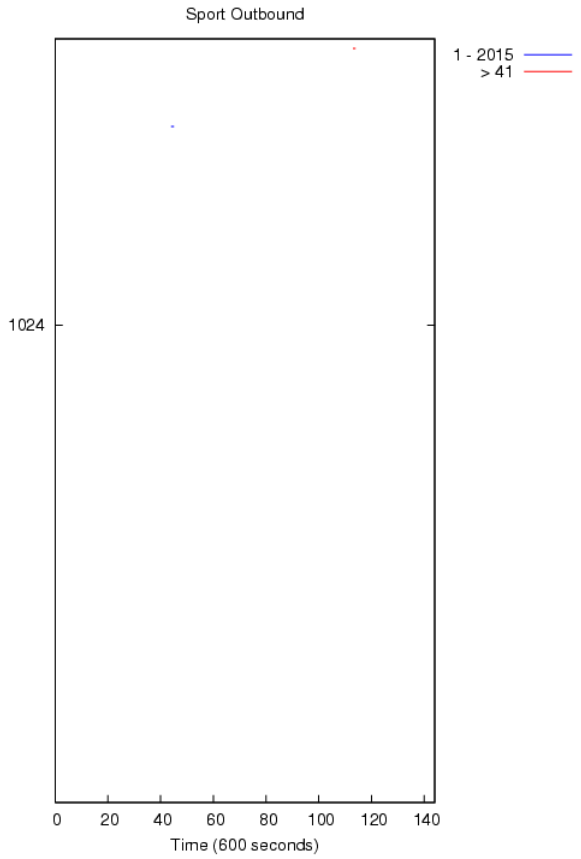
01/25


Dport Inbound
1 - 159
160 - 230779
> 230780
1024
592
500
445
135
80
53
25
0 200 400 600 800 1000 1200 1400
Time (60 seconds)

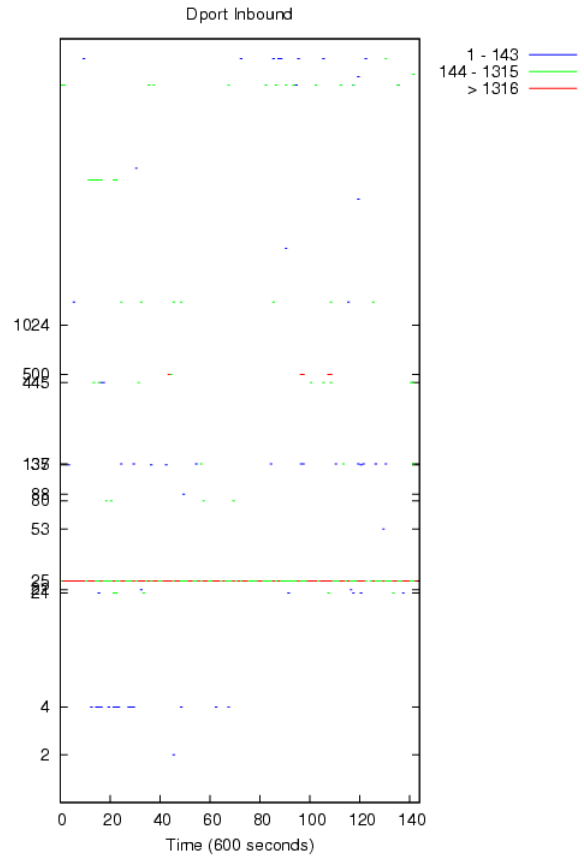

Sport Outbound
1 - 4524617
4524618 - 13869430
> 13869431
1024
80
0 200 400 600 800 1000 1200 1400
Time (60 seconds)

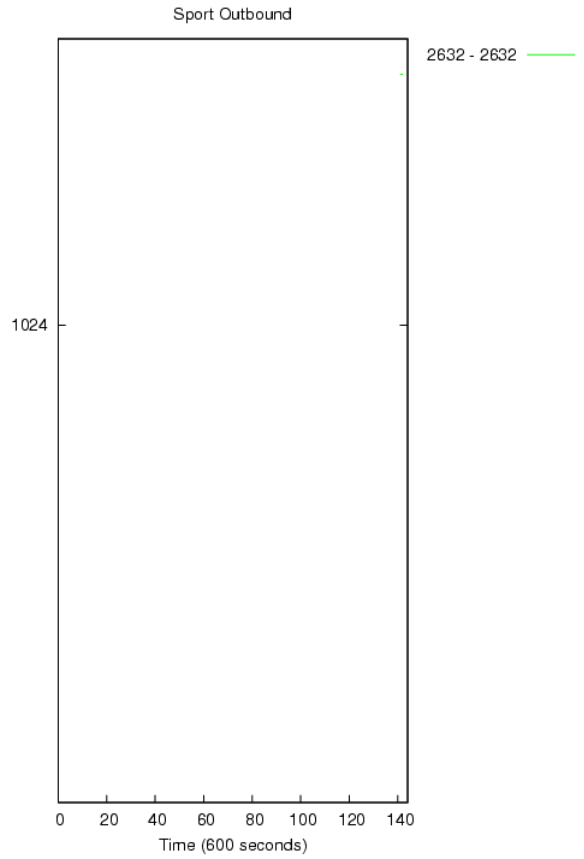
01/31


Dport Inbound
1 - 319
320 - 1467
> 1468
1024
500
445
135
80
53
25
21
4
0
20
40
60
80
100
120
140
Time (600 seconds)

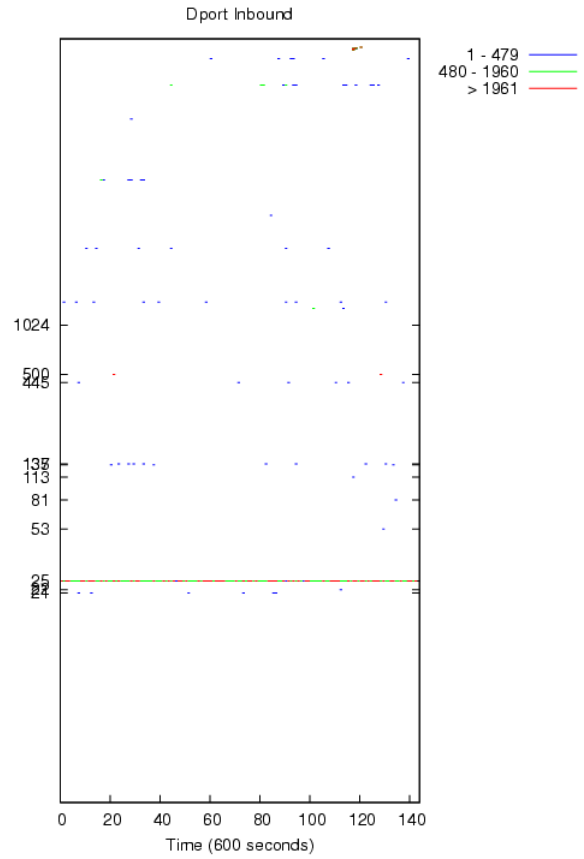

Sport Outbound
1 - 2015
> 41
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

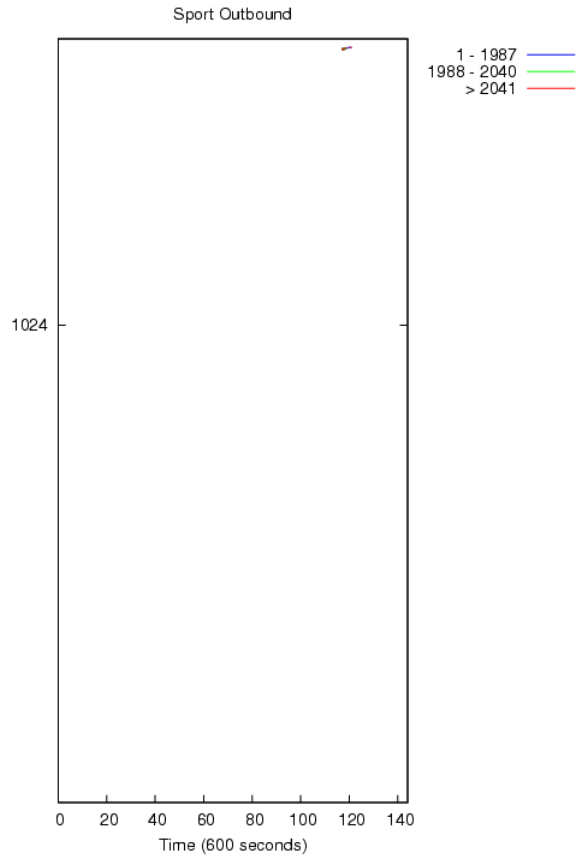
02/06


Dport Inbound
1 - 143
144 - 1315
> 1316
1024
500
445
135
88
80
53
25
24
4
2
0
20
40
60
80
100
120
140
Time (600 seconds)

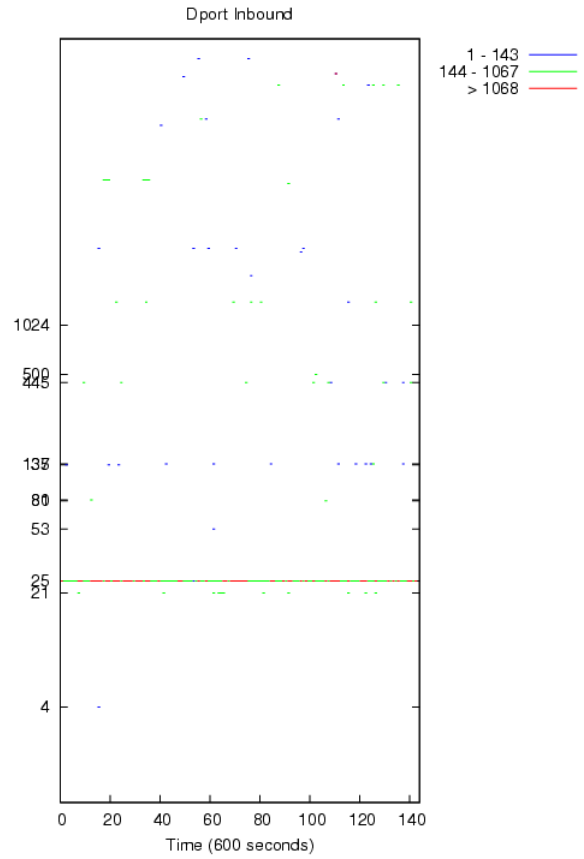

Sport Outbound
2632 - 2632
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

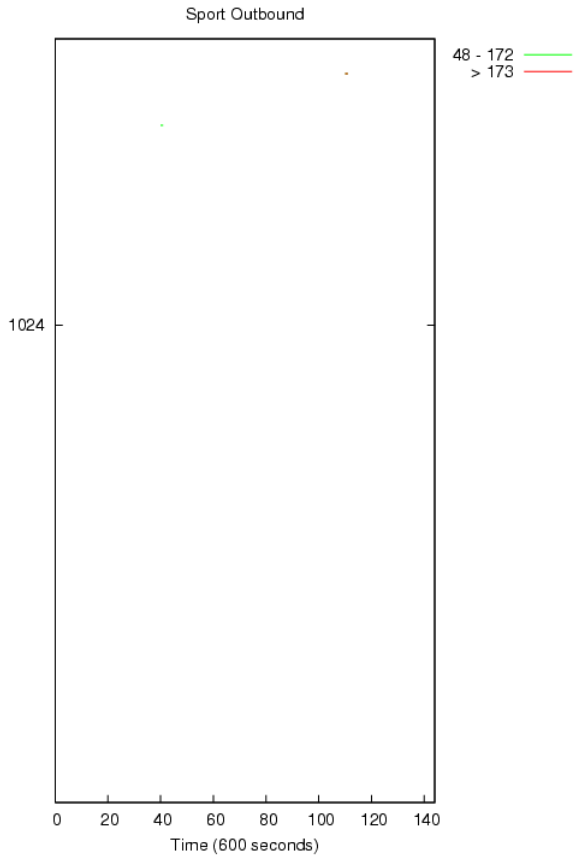
02/08


Dport Inbound
1 - 479
480 - 1960
> 1961
1024
500
445
137
113
81
53
25
0
20
40
60
80
100
120
140
Time (600 seconds)

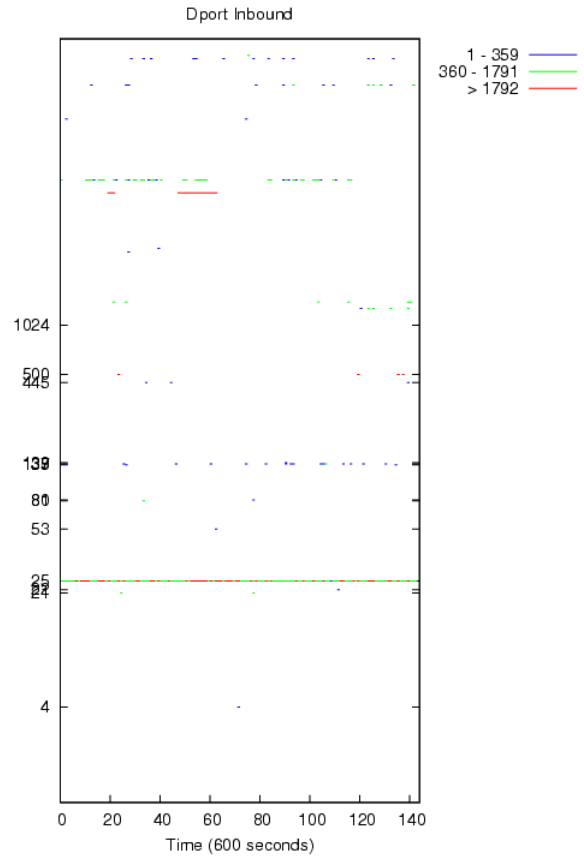

Sport Outbound
1 - 1987
1988 - 2040
> 2041
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

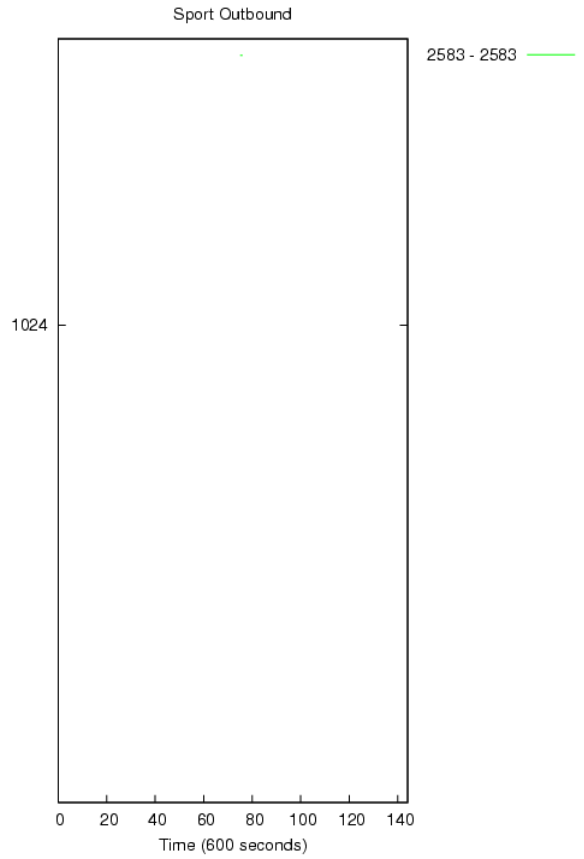
02/11


Dport Inbound
1 - 143
144 - 1067
> 1068
1024
500
445
135
80
53
25
21
4
0
20
40
60
80
100
120
140
Time (600 seconds)

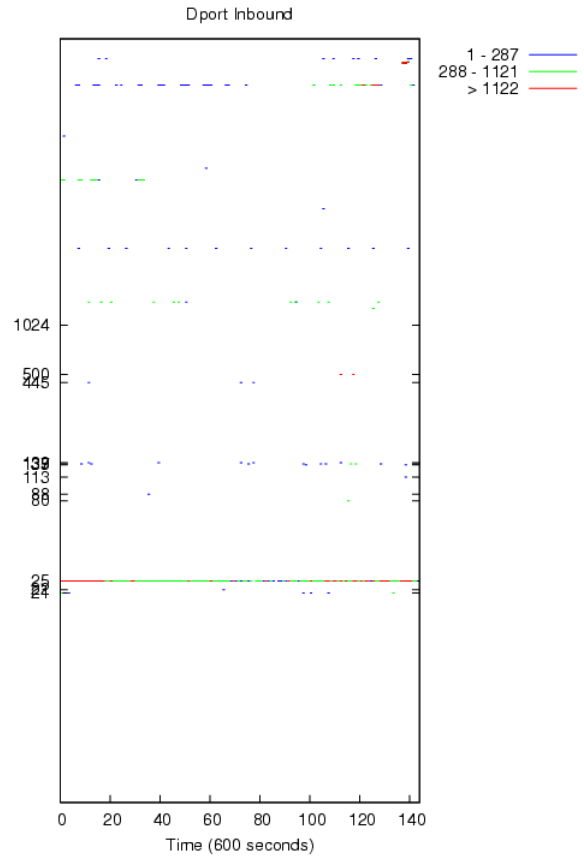

Sport Outbound
48 - 172
> 173
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

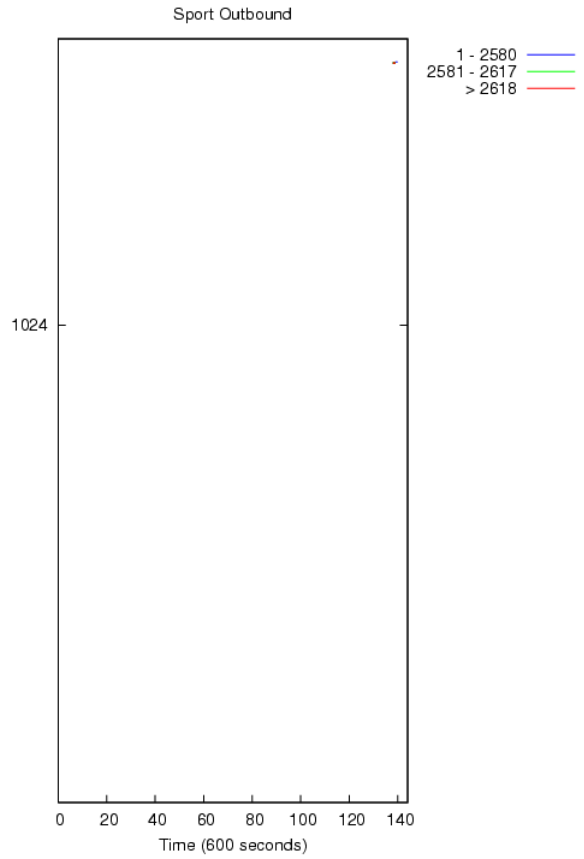
02/13


Dport Inbound
1 - 359
360 - 1791
> 1792
1024
500
445
139
80
53
25
4
0
20
40
60
80
100
120
140
Time (600 seconds)


Sport Outbound
2583 - 2583
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

03/10

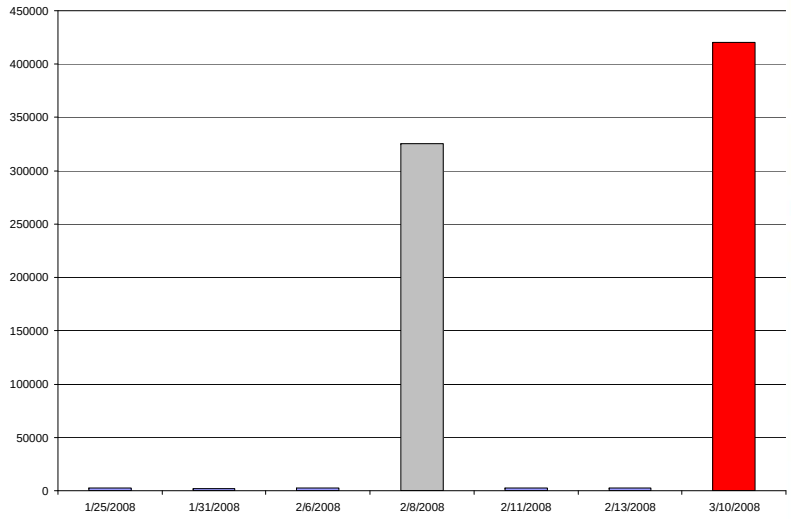

Dport Inbound
1 - 287
288 - 1121
> 1122
1024
500
445
139
113
88
80
25
24
0
20
40
60
80
100
120
140
Time (600 seconds)


Sport Outbound
1 - 2580
2581 - 2617
> 2618
1024
0
20
40
60
80
100
120
140
Time (600 seconds)

Client/Server activity

03/10

- 111 clients connecting inbound
- 76 servers connecting outbound



Misconfiguration Summary

- Visualization did not show significant increase in activity
- Client/server activity showed significant volume

Agency Resolution

- The modified SMTP config sent all outbound mail to their mail appliance for inspection and distribution
- Configuration was lost therefore mail did not pass through the appliance
- SMTP went out directly from host identified in Rogue Server
- Agency made configuration change

Summary

- Rogue Server has identified new servers, errors in mail routing, and network misconfigurations (VPN)
- Rogue Server techniques could potentially be applied to other applications
- Network architecture is learned through flow analysis and no knowledge of the network is necessary

Contact Info

- **Technical comments or questions**
  - US-CERT Security Operations Center
  - Email: soc@us-cert.gov
  - Phone: +1 888-282-0870
- **Media inquiries**
  - US-CERT Public Affairs
  - Email: media@us-cert.gov
  - Phone: +1 202-282-8010
- **General questions or suggestions**
  - US-CERT Information Request
  - Email: info@us-cert.gov
  - Phone: +1 703-235-5111
- **For more information, visit** http://www.us-cert.gov

Questions?