Honeynet Project

Scan of the Month Challenge #30

Steven Sim Kok Leong
steven@beepz.net

Preparation

Before analyzing the log, the downloaded log extracted from the downloaded honeynet-Feb1_FebXX.log.gz has its md5 checksum checked. The checksum matched the one listed on http://www.honeynet.org/scans/scan30/

```
$ md5sum honeynet-Feb1_FebXX.log
8c0070ef51f6f764fde0551fa60da11b  honeynet-Feb1_FebXX.log
```

Short uncomplicated generic shell scripts are written for ease of collecting daily statistics for each type of traffic, specifically to answer Q1. Other commands and shell scripts used will be listed along the way.

extract.sh – Filters relevant traffic from honeynet-Feb1_FebXX.log

e.g. ./extract.sh “INBOUND TCP” 443

```
#!/bin/bash

grep “$1” honeynet-Feb1_FebXX.log | grep “DPT=$2 “ > $2.log
```

day.rate.sh - takes output file from extract.sh as input to compute daily statistic.

e.g. ./day.rate.sh 443.log

Output is ported into Excel for charting.

```
#!/bin/bash
day=1
while [ “$day” -le “27” ]
do
  echo $day: `grep “ $day “ $1|cut -d: -f2|awk ‘{s+=$1} END {print s}’`
  day=`expr $day + 1`
done
```

1. What are the high-level trends in connectivity to/from the honeynet? What was growing/decreasing? How does that match global statistics from DShield and other sources?

A. Protocol Trends

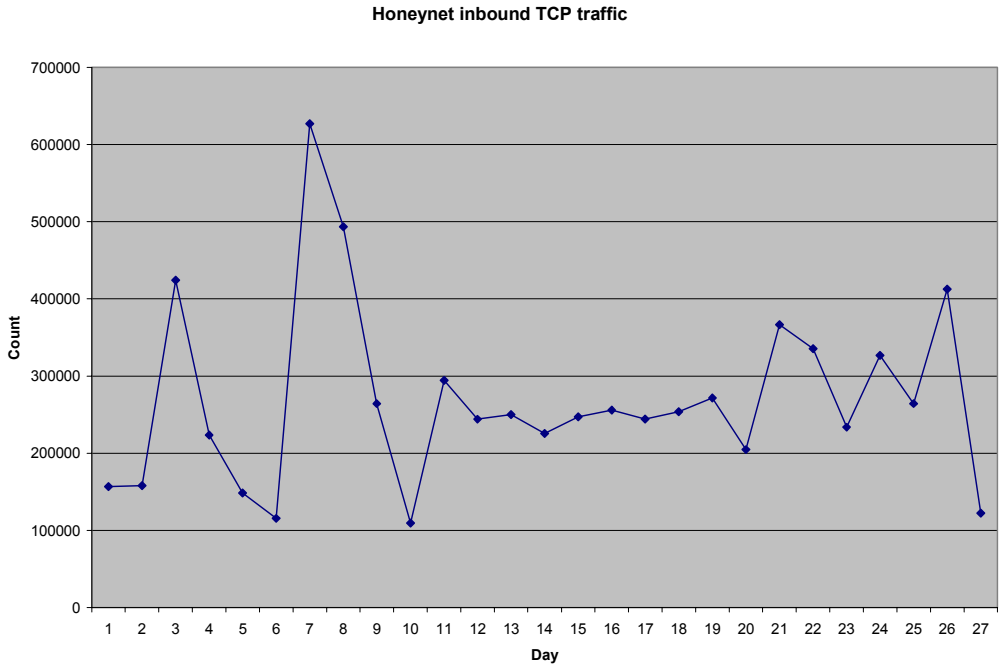
Inbound traffic to the honeynet comprises mainly of TCP traffic with ICMP traffic surpassing that of UDP traffic.

```
$ grep INBOUND honeynet-Feb1_FebXX.log | awk '{print $7}' | sort |
uniq -c
  19602 ICMP:
 244546 TCP:
  18994 UDP:
```

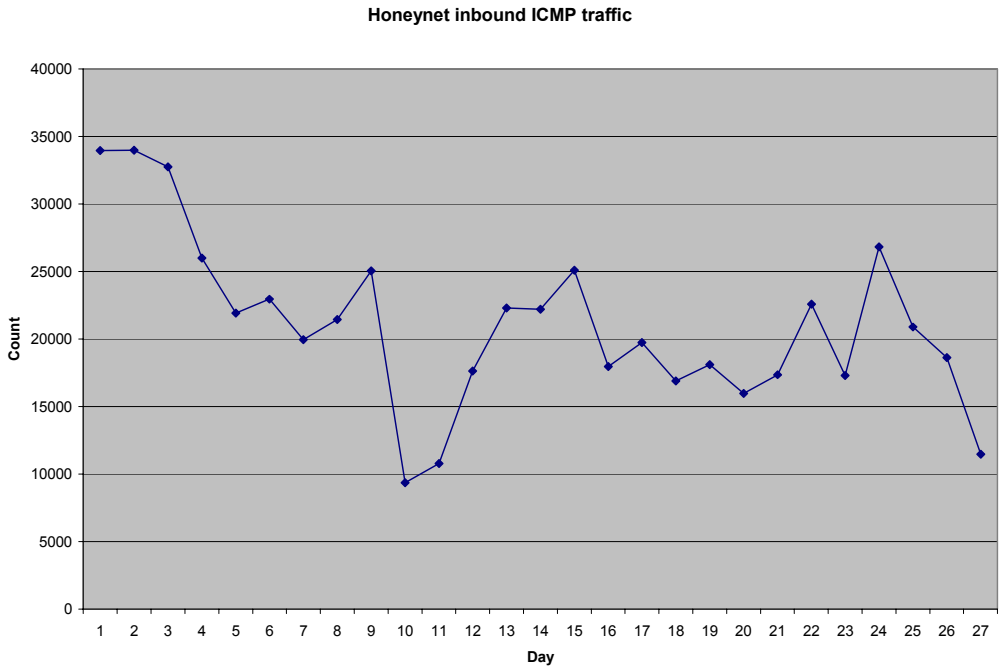
Outgoing traffic to the honeynet comprises primarily TCP traffic followed by UDP traffic. There were however no ICMP traffic from the honeynet. In addition, there were OTHER traffic. Further details will be mentioned on this later in this writeup.

```
$ grep 'OUTG CONN' honeynet-Feb1_FebXX.log | awk '{print $7}' | sort
| uniq -c
      7 OTHER:
   1739 TCP:
    485 UDP:
```

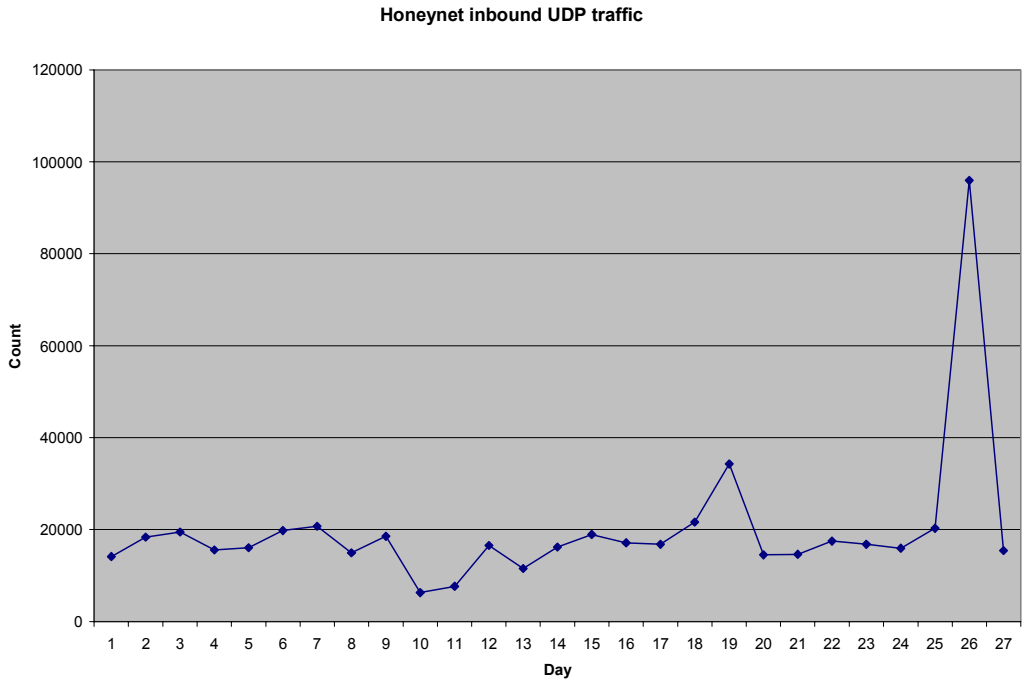
From the graphical representation of daily inbound TCP traffic into the honeynet, the sharp spikes on 3rd Feb and 7th Feb are worth noting. The higher volume of TCP traffic at start-Feb decreases around mid-Feb and rose again towards end-Feb.



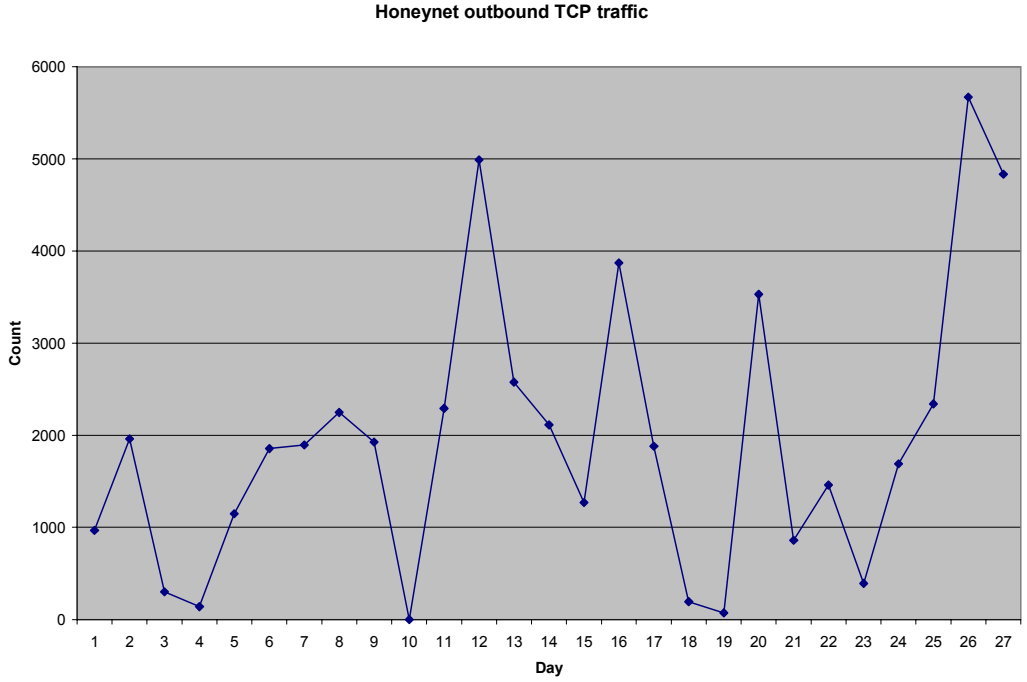
For inbound ICMP traffic into the honeynet, traffic was high on the 1st 3 days of Feb and declined on the average gradually across the month. The big dip in 10th Feb and 11th Feb warrants further scrutiny.



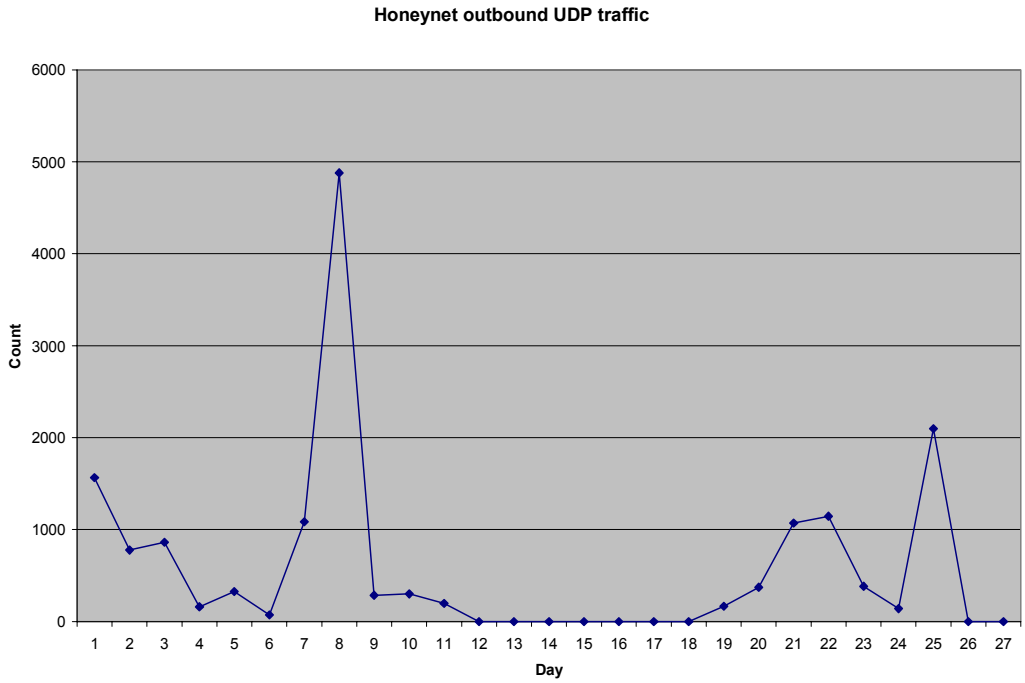
In the trend for inbound UDP traffic, the sharp spike on 26th Feb warrants concern. Beyond that, traffic across Feb is pretty horizontal.



For outbound TCP traffic, the peaks on 12th, 16th, 20th and 26th Feb need to be investigated. Overall, traffic appears to increase towards end-Feb.



For outbound UDP traffic, mid-Feb sees a period of zero UDP outbound activity soon after the big spike on 8th Feb and before the rise near end-Feb.



B. Service trends.

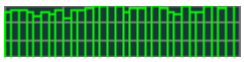
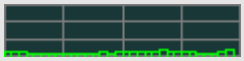
```
Top 10 inbound TCP ports:

  86632 DPT=135
  46439 DPT=445
  26444 DPT=443
  25781 DPT=3127
  15000 DPT=139
  13276 DPT=80
   3427 DPT=6129
   3097 DPT=901
   2791 DPT=1433
   2147 DPT=17300
```

```
Top 10 inbound UDP ports:

   8692 DPT=137
   5905 DPT=1434
   2366 DPT=1026
   1525 DPT=135
    260 DPT=1027
    146 DPT=1812
     28 DPT=111
     18 DPT=31789
     17 DPT=53
     16 DPT=1024
```

Extracting the top 10 ports probed regardless of TCP or UDP, we have

```
Top 10 inbound ports:

  86632 DPT=135
  46439 DPT=445
  26444 DPT=443
  25781 DPT=3127
  15000 DPT=139
  13276 DPT=80
   8692 DPT=137
   5905 DPT=1434
   3427 DPT=6129
   3097 DPT=901
```

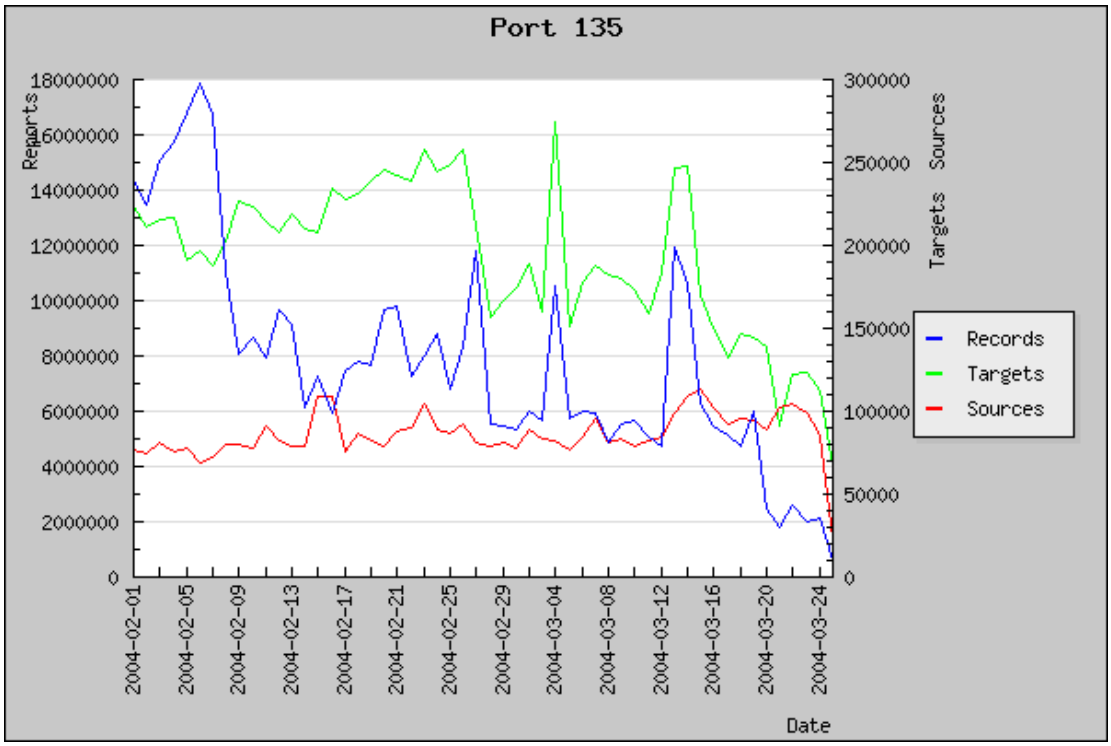
Comparing the top ten of honeynet with that of DShields, there is a very close resemblance in the port numbers with few differences primarily in TCP/443 (honeynet top ten), TCP/901 (honeynet top ten), TCP/1433 (DShield top ten), TCP/21 (DShield top ten). In terms of ranking, the top contenders for 1st, 2nd and 4th spots are similarly TCP/445, TCP/135 and TCP/3127.

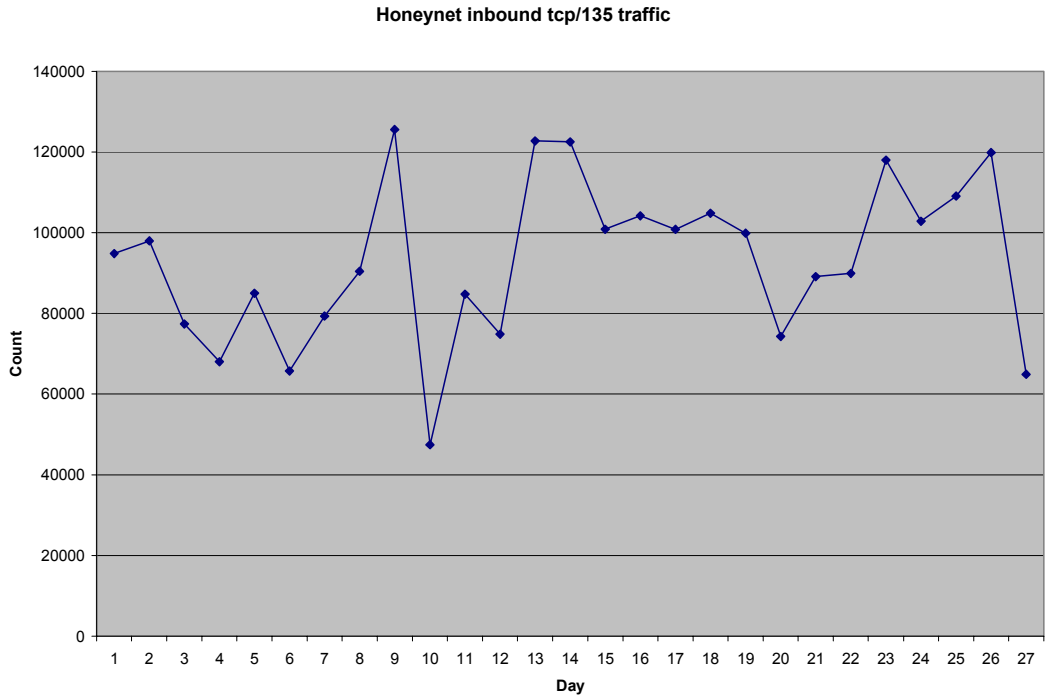
Service Name	Port Number	Activity Past Month	Explanation
microsoft-ds	445		Win2k+ Server Message Block
epmap	135		DCE endpoint resolution
www	80		World Wide Web HTTP
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor
netbios-ns	137		NETBIOS Name Service
ms-sql-m	1434		Microsoft-SQL-Monitor
dameware	6129		Dameware Remote Admin
ms-sql-s	1433		Microsoft-SQL-Server
netbios-ssn	139		NETBIOS Session Service
ftp	21		File Transfer [Control]

Let us scrutinize each of the honeynet top 10 ports closer.

TCP/135

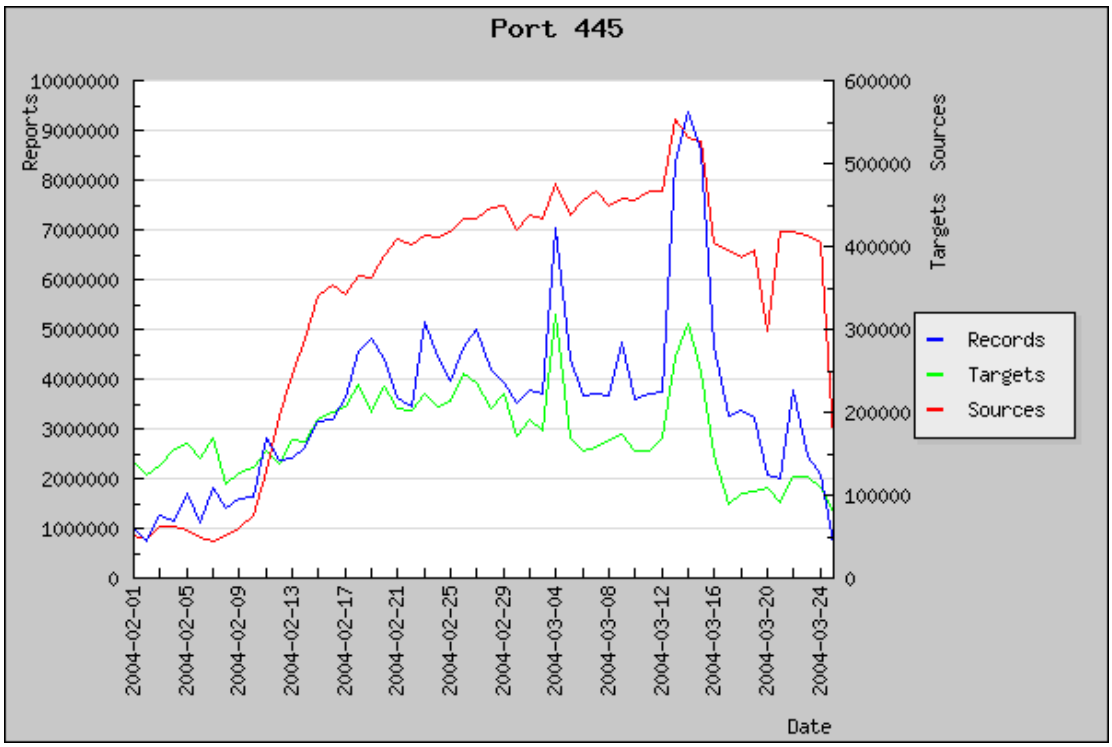
Not much correlation can be noticed for port TCP/135.

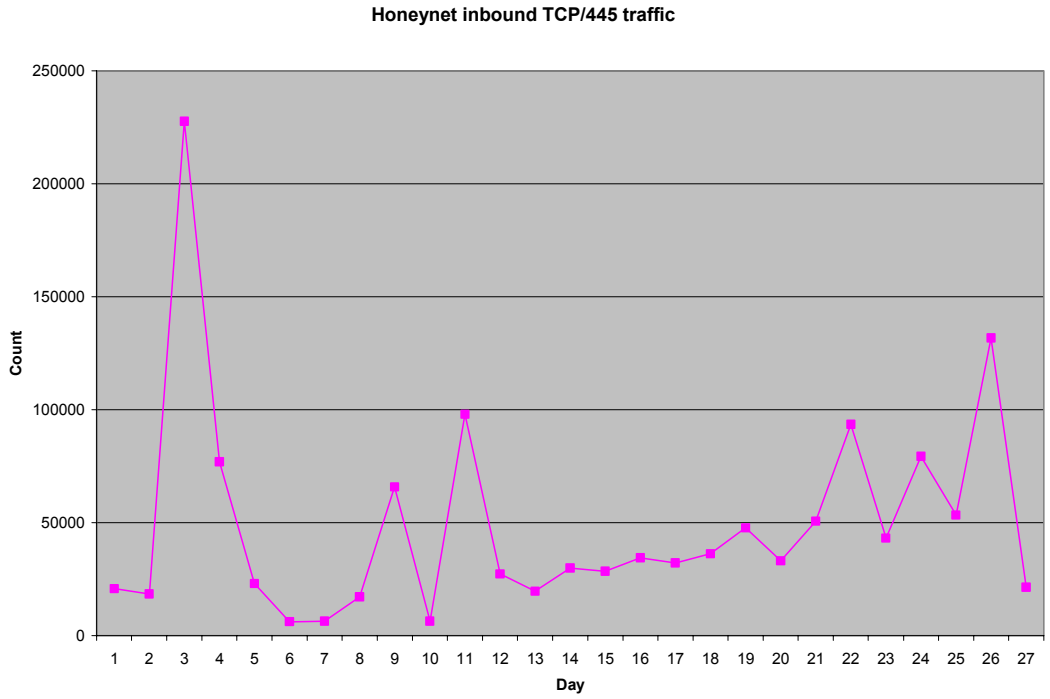




TCP/445

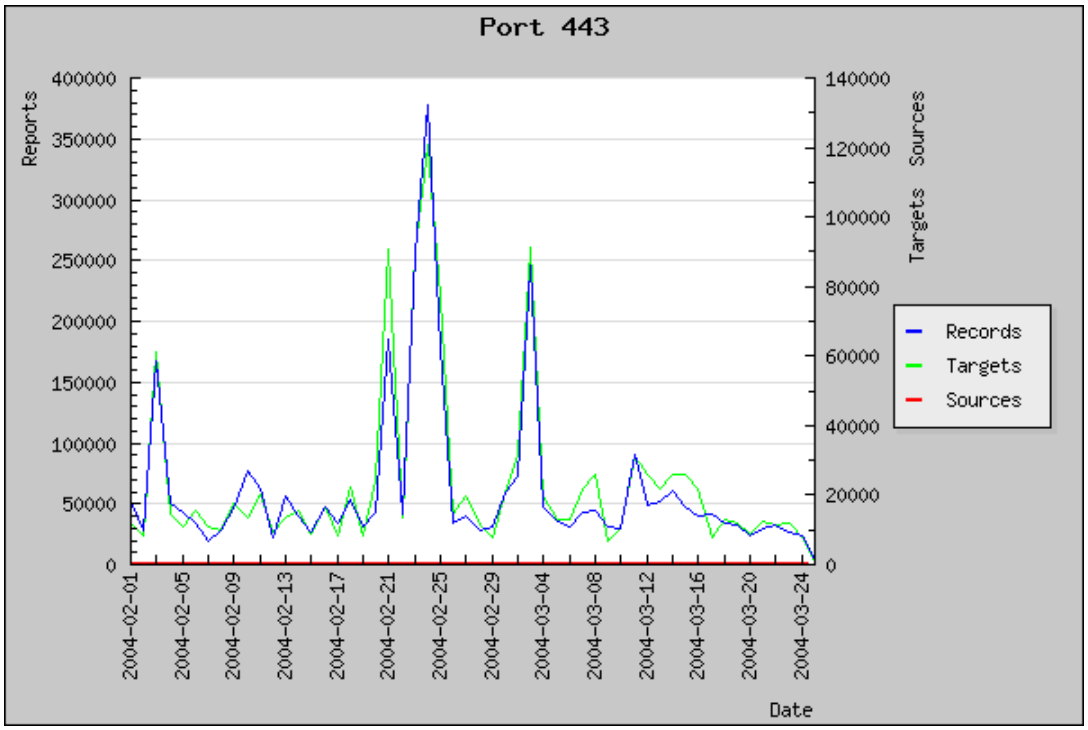
The steady rise across the entire month matches. The spike on 3rd Feb for the honeynet is abnormal.



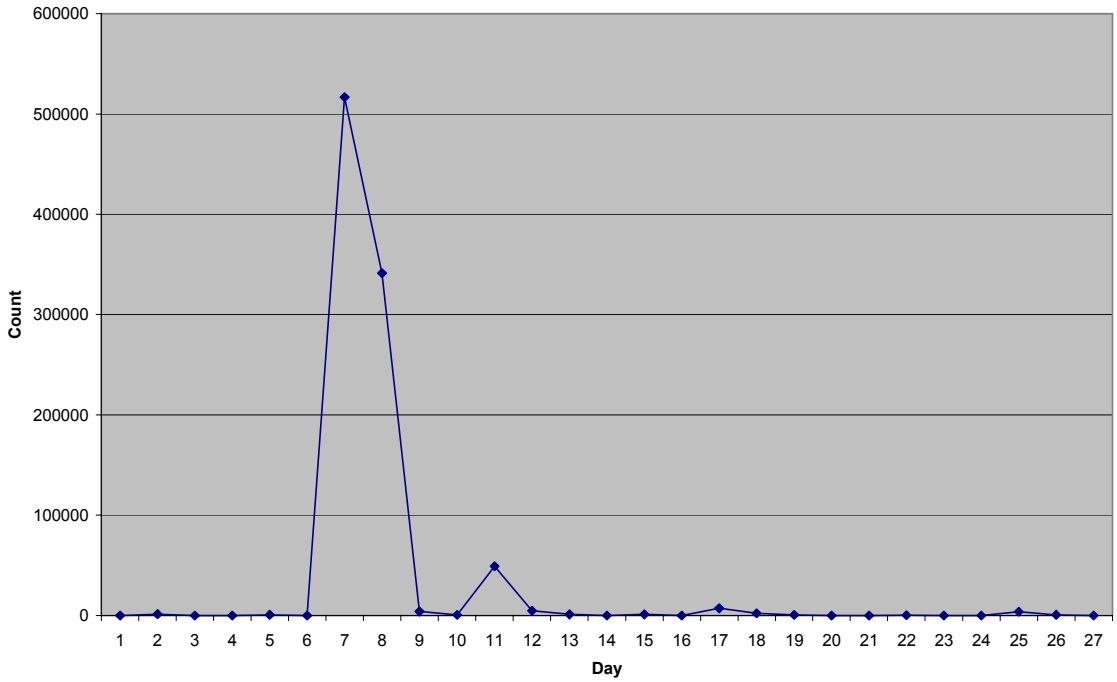


TCP/443

The huge surge in TCP/443 traffic on 7th and 8th Feb is abnormal. There is no associated search reported in DShields. This likely explains why TCP/443 is in the honeynet top 10 but not in the DShields top 10.

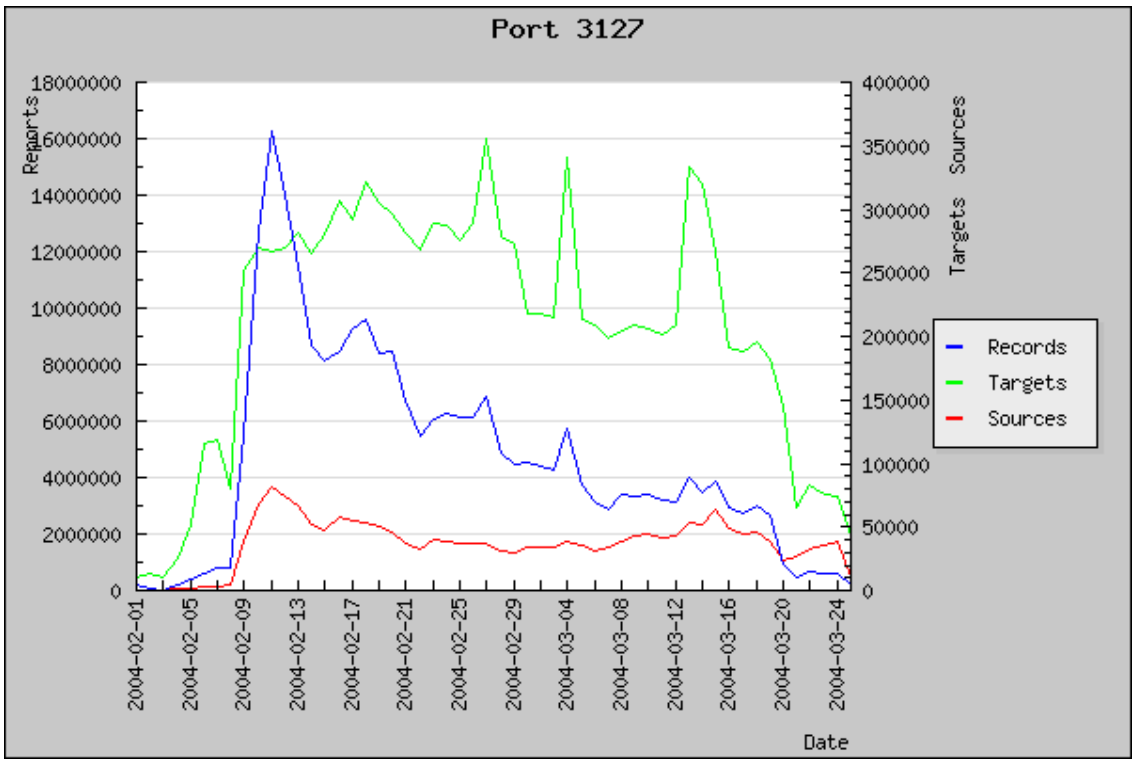


Honeynet inbound TCP/443 traffic

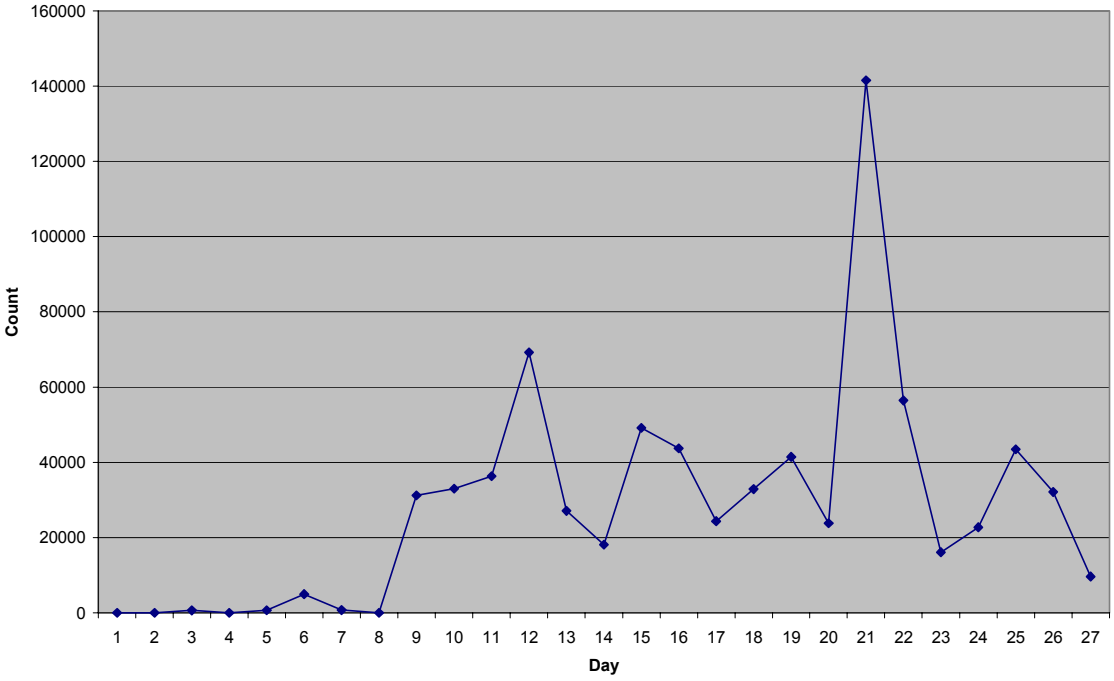


TCP/3127

The peaking around 12th Feb and increase from 9th Feb is similar. However, the peak on 21st Feb needs to be investigated.

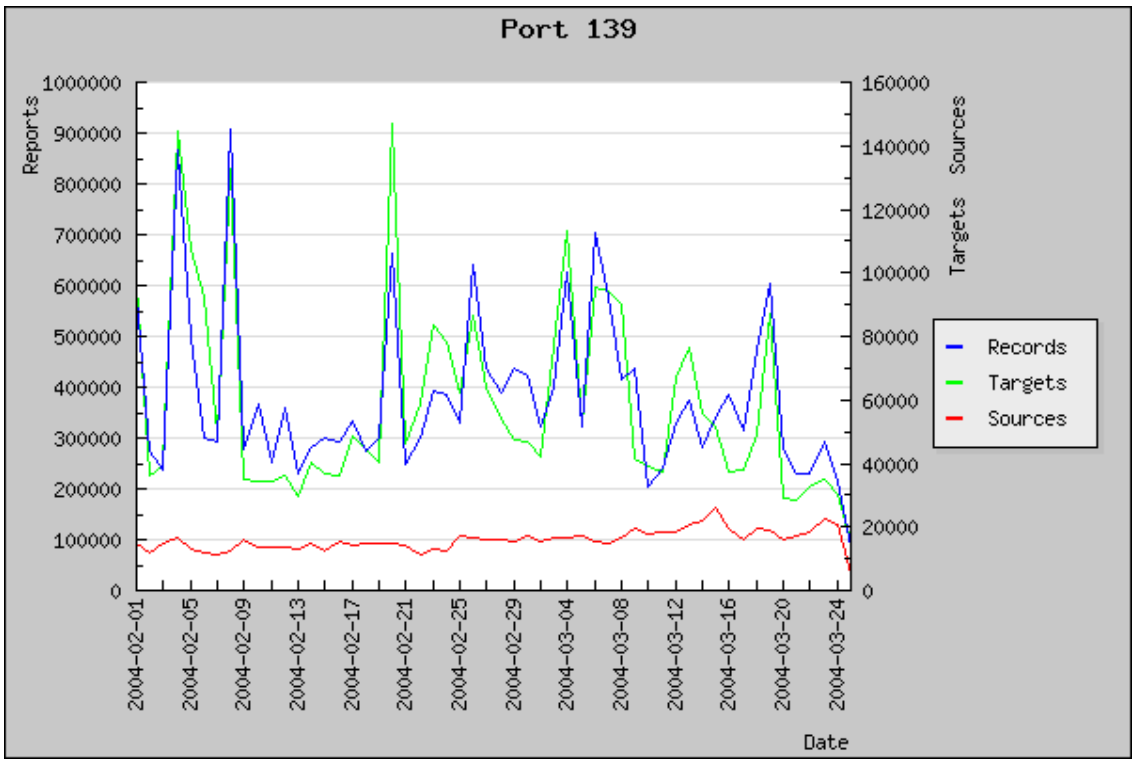


Honeynet inbound TCP/3127 traffic

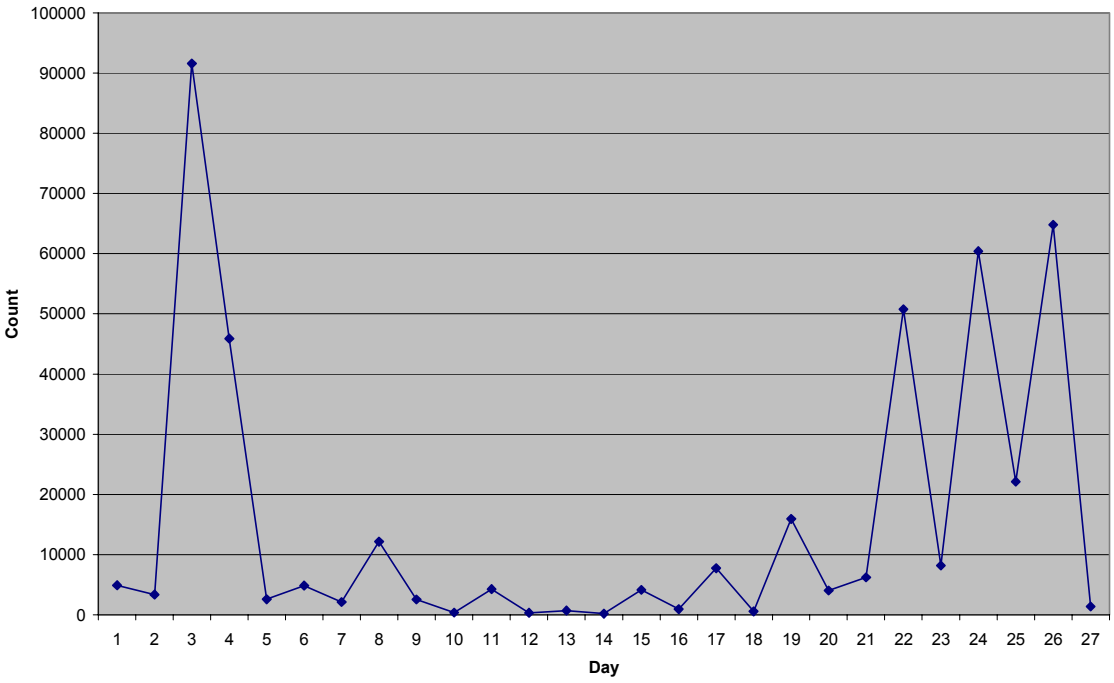


TCP/139

There appears to be quite a fair bit of resemblance with peaks near 3rd, 22nd, 24th and 26th Feb.

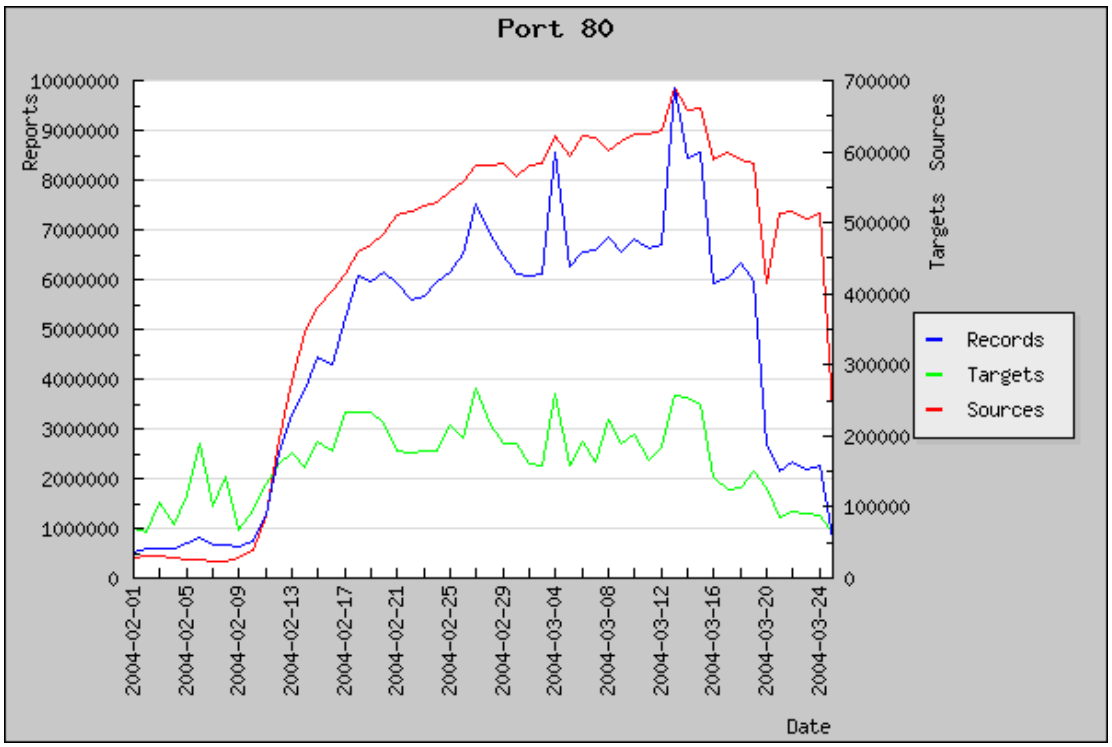


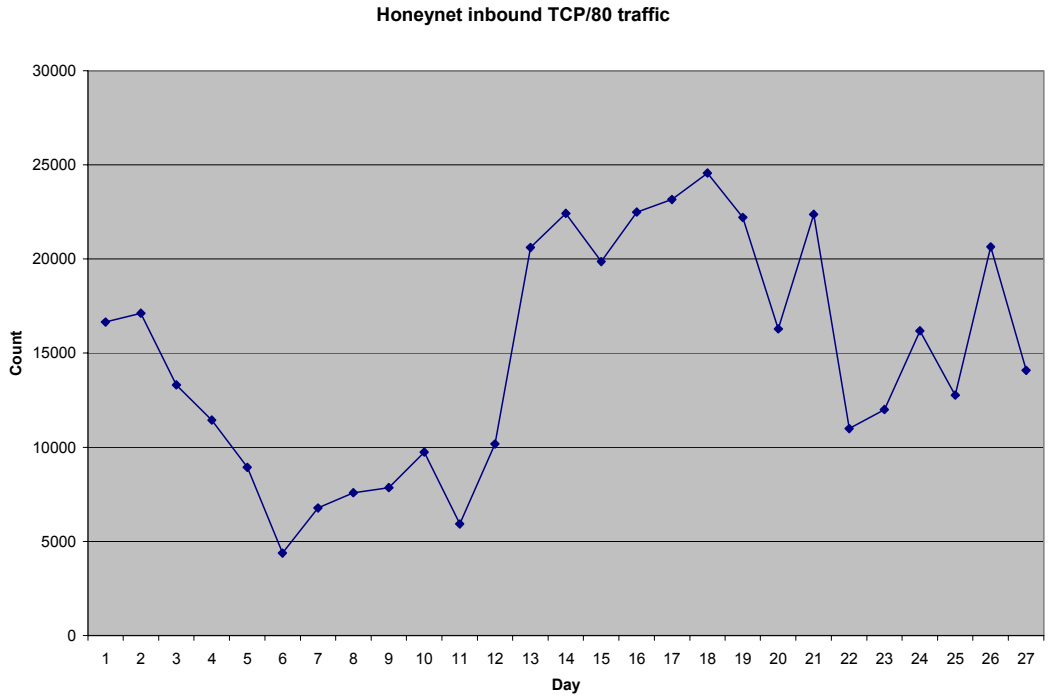
Honeynet inbound TCP/139 traffic



TCP/80

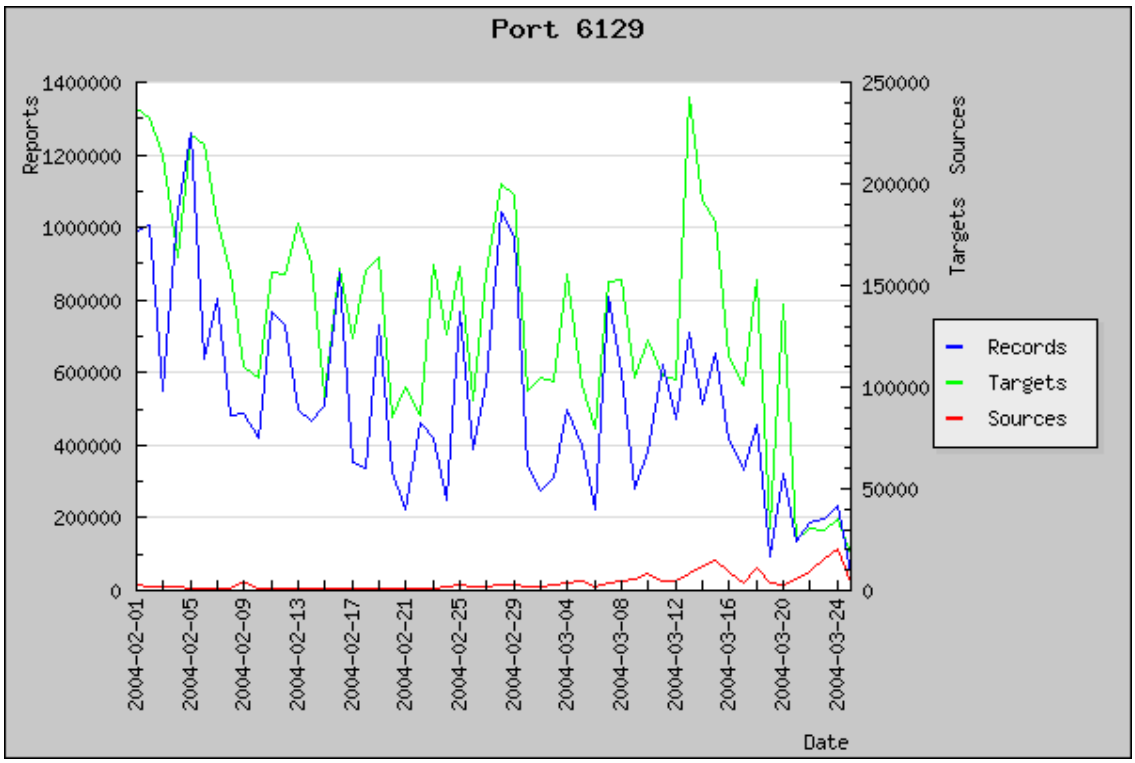
Very strong resemblance in the increase from 11th Feb onwards as well as the dip near 22nd Feb.



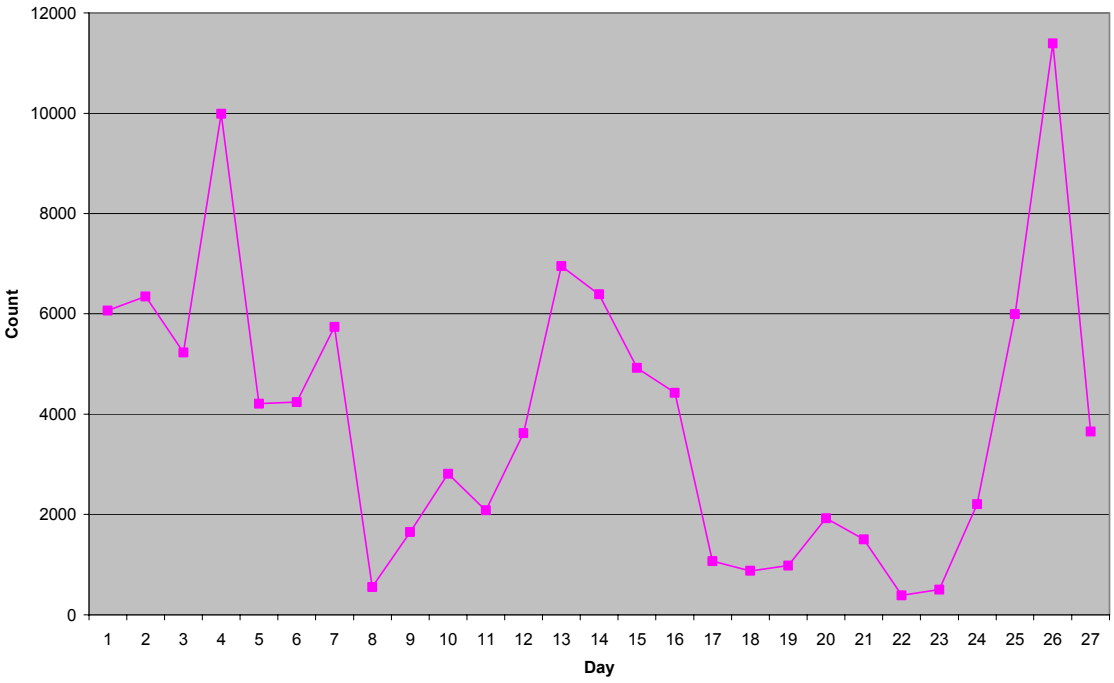


TCP/6129

Very strong resemblance with the peak near 4th Feb, trough near 8th Feb, peaks near 15th Feb and 26th Feb.

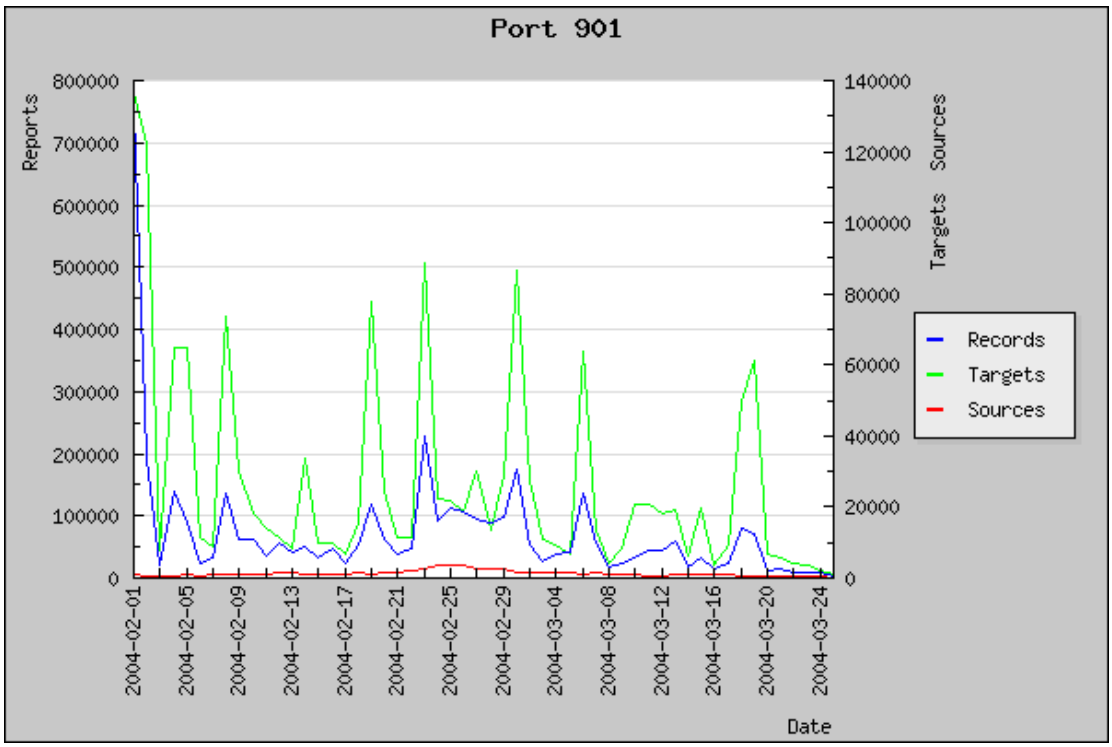


Honeynet inbound TCP/6129 traffic

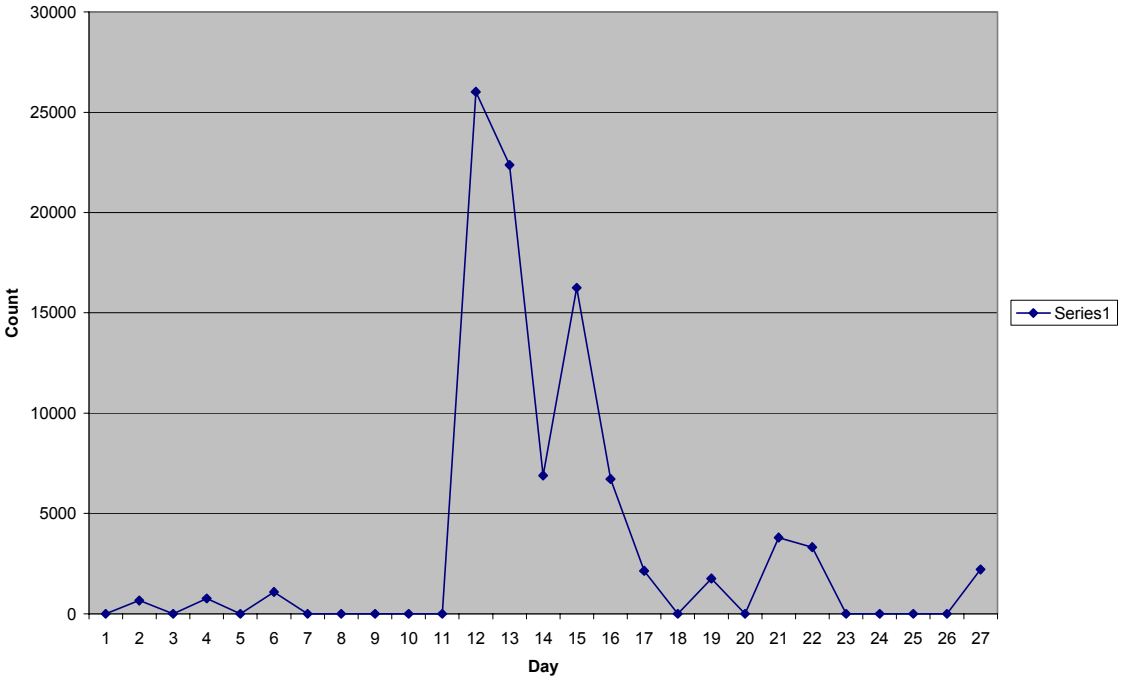


TCP/901

This traffic comes in sporadic bursts, need to check out the surges on 12th, 13th and 14th Feb.

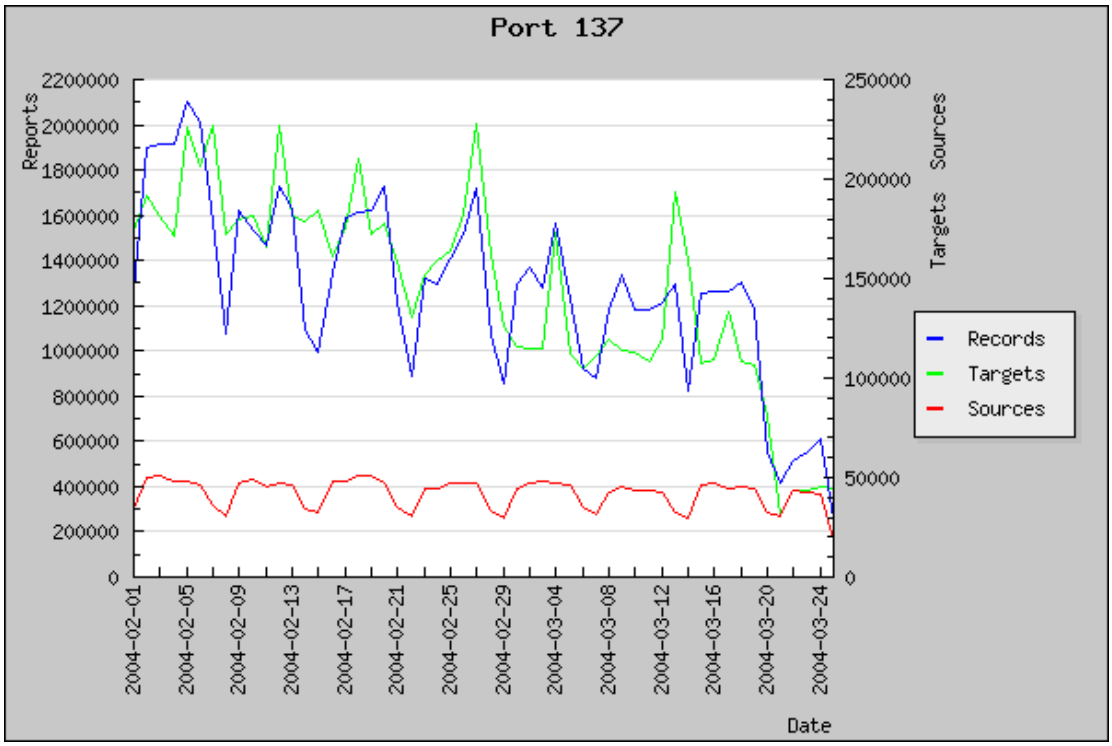


Honeynet inbound TCP/901 traffic

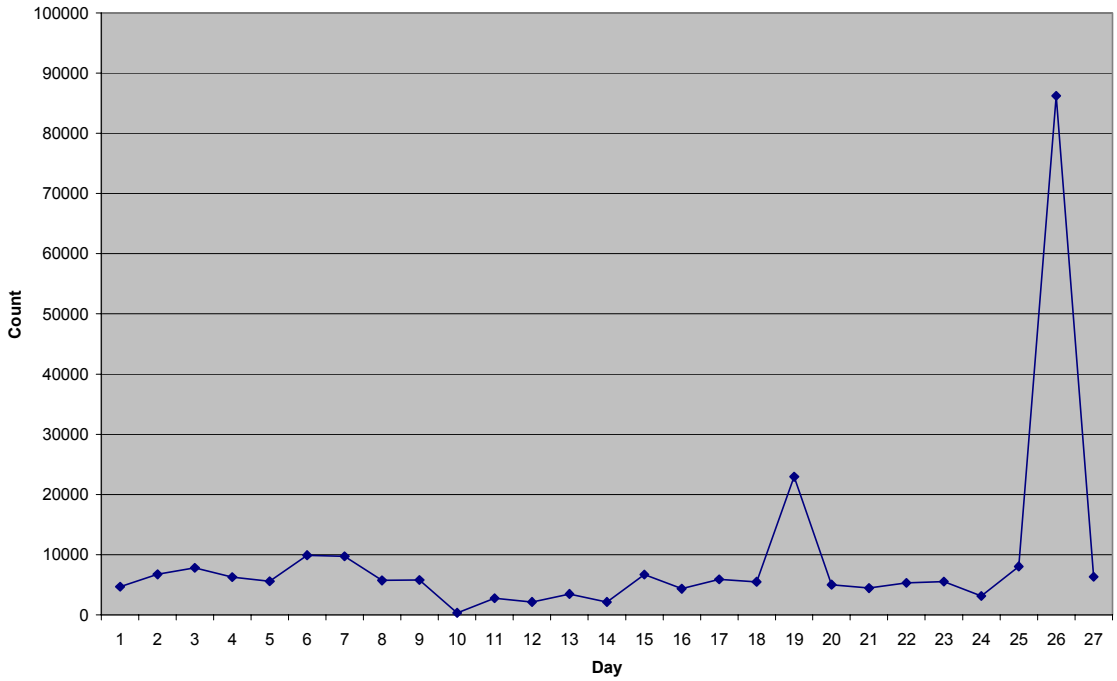


UDP/137

This traffic appears as a decreasing trend in DShield with stable number of sources. The same traffic looks pretty horizontal at the honeynet except on 26th Feb where there was a spike.

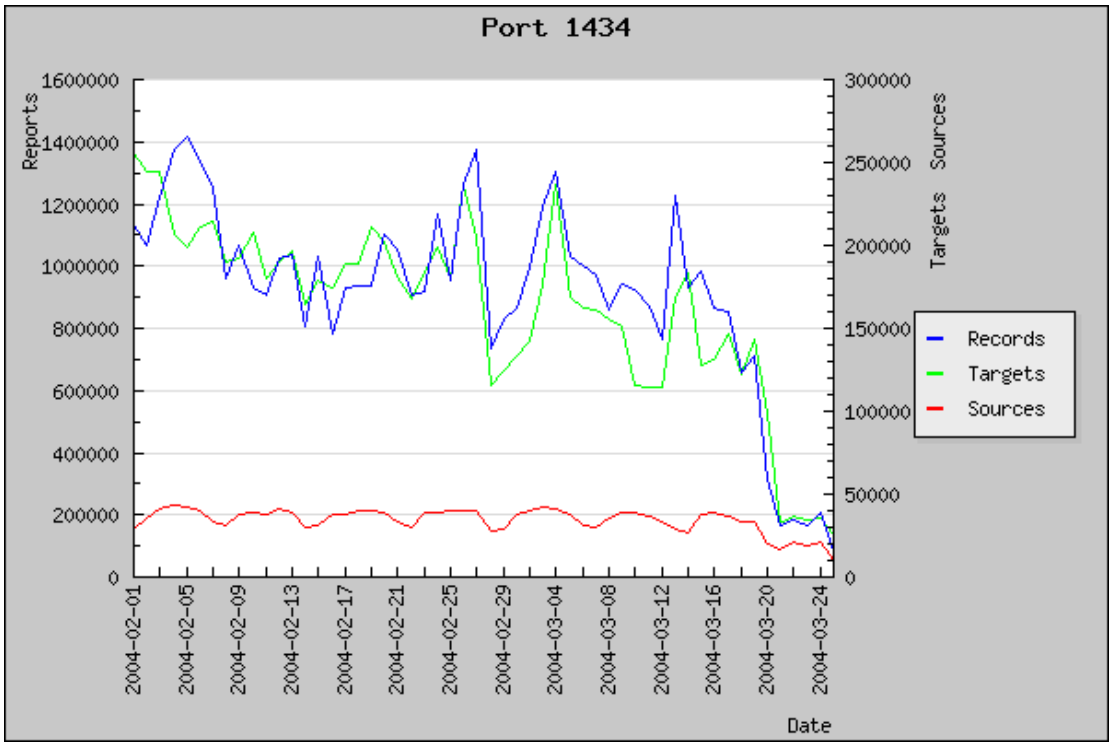


Honeynet inbound UDP/137 traffic

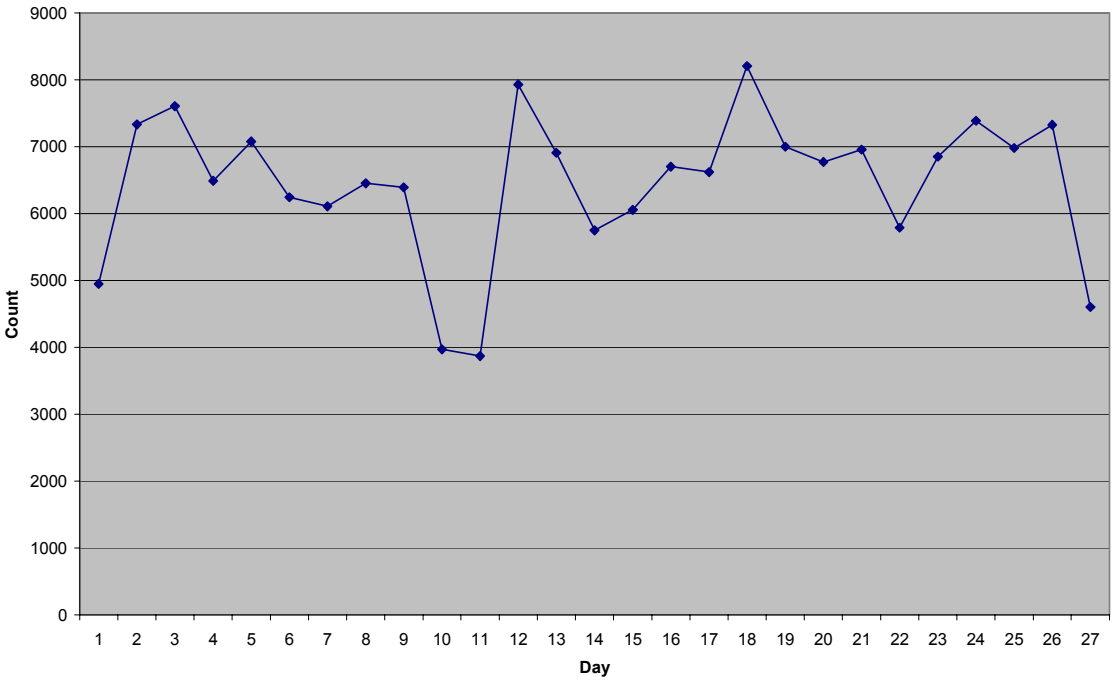


UDP/1434

The dip in traffic in the Honeynet on 10th and 11th Feb looks abnormal. DShield posted a surge near end-Feb which is not observed in honeynet.



Honeynet inbound UDP/1434 traffic



2. What possible evidence of malware is there? what types? what are the malware trends you can observe?

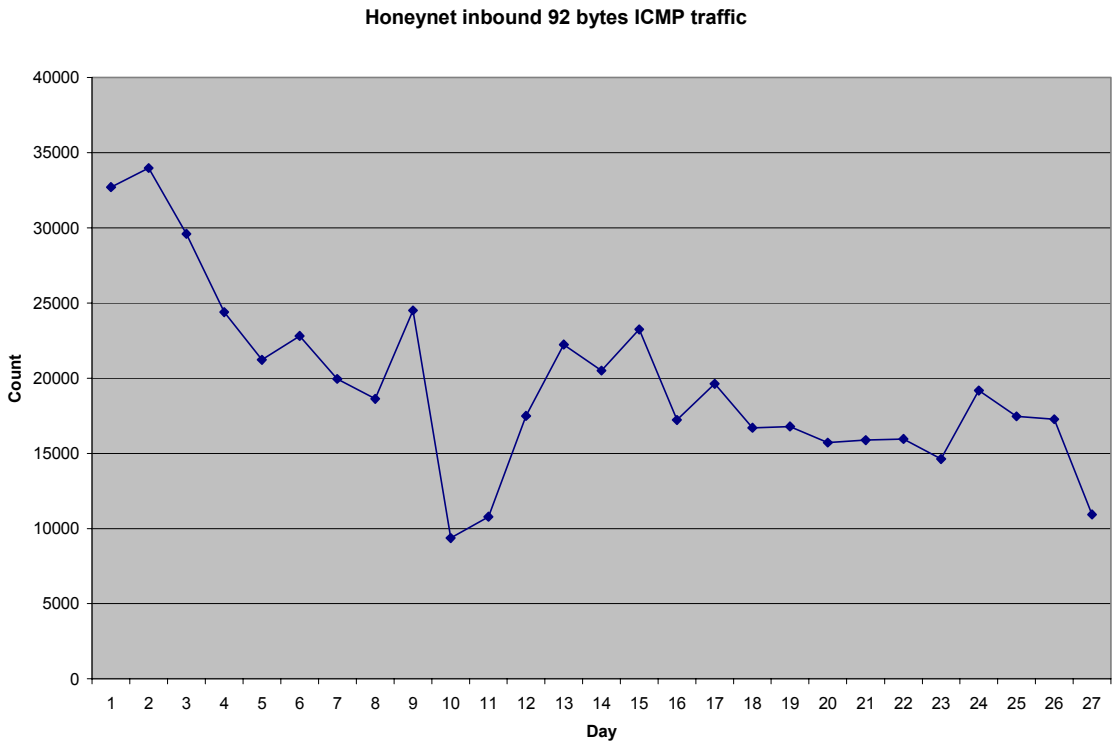
A. Nachi worm and variants

The nachi worm generates a few network behaviors including sending ICMP type 8 code 0 packets of length 92 bytes as well as scanning of TCP/139 of targets with 48 byte packets, beyond exploiting TCP/135. Port TCP/4444 is used as the backdoor.

As noticed from Q1. top 10 ports, TCP/139 and TCP/135 are ranked among the top 10 ports.

Since ICMP 92 bytes packets are pretty much unique to the Nachi worm, traffic associated with them is extracted and charted.

```
$ grep ICMP honeynet-Feb1_FebXX.log | grep LEN=92 > icmp.abnormal92
$ ./day.rate.sh icmp.abnormal92
```



This is further evident that Nachi worm is targeting the honeynet. The dip on 10th and 11th Feb is noticeably similar to that reflected for the UDP/1434

chart and somewhat similar to the TCP/135 dip on 10th Feb. More will be mentioned on this later. The Nachi traffic decreases across the month of Feb.

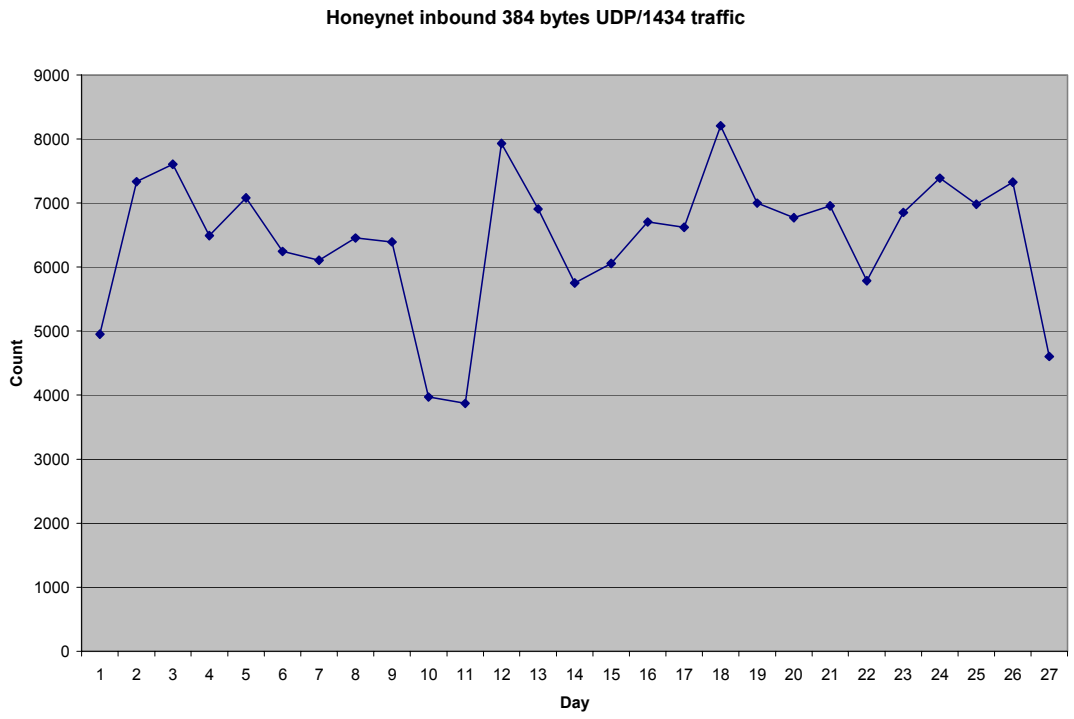
B. Doomjuice worm

MyDoom uses TCP/3127 as preferred port for backdoor if available. Doomjuice worm, also known as Mydoom.C, was found on 9th Feb. It infects machines which are already infected by the original Mydoom. As evident from TCP/3127 chart, there is a marked increase in the number of inbound TCP/3127 probes from 9th Feb. This falls nicely with the discovery of the Doomjuice worm which exploits the same backdoor.

C. MsSQL Slammer worm

Slammer scans and overruns the vulnerability MsSQL service at UDP/1434. The amount of probes targeting this port is still at a consistently high rate. Packet size of 384 bytes is characteristic of such malware traffic. Chart plotted on this traffic shows evidently attempts made by this malware to target the honeynet.

```
$ grep "INBOUND UDP" honeynet-Feb1_FebXX.log | grep "DPT=1434 " | grep
"LEN=384" > inbound.udp.dpt1434.384bytes.log
$ ./day.rate.sh inbound.udp.dpt1434.384bytes.log
```



3. What types of reconnaissance activity you notice? What do you think they were looking for? What are some of the notorious sources of such activity in the files?

A. Dameware worm

There was much speculation on a potential dameware worm since 23rd Jan with the large number TCP/6129 probes. A buffer overflow vulnerability was already published on 22nd Dec 2003 on CERT/CC. Such reconnaissance could be to find vulnerable systems installed with dameware to compromise. The Details on the vulnerability found at http://www.kb.cert.org/vuls/id/909678

The following are the top 10 notorious sources of the TCP/6129 scan.

```
$ cat inbound.tcp.dst.port.6129 | sed 's/DF//g' | awk '{print $12}'
| sort | uniq -c | sort -rn | head
     94 SRC=210.105.40.67
     87 SRC=195.167.19.135
     72 SRC=68.59.101.217
     55 SRC=24.17.237.70
     54 SRC=66.12.221.142
     54 SRC=64.231.82.204
     48 SRC=68.146.149.94
     48 SRC=24.84.102.20
     48 SRC=24.151.74.255
     46 SRC=172.176.191.158
```

B. Witty worm

The recent Witty worm exploits the ICQ parsing vulnerability on certain versions of ISS RealSecure network sensor, server sensor and desktop protector. Because RealSecure network sensor uses TCP/901 for event monitoring, the increase in TCP/901 probes could reflect attempts to identify the whereabouts of such sensors to compromise. Traffic trend shows a surge of such reconnaissance traffic on 12th, 13th and 15th on the honeynet.

The following are the top 10 notorious sources of the TCP/901 scan.

```
$ cat inbound.tcp.dst.port.901 | sed 's/DF//g' | awk '{print $12}'
| sort | uniq -c | sort -rn | head
     97 SRC=131.247.237.79
     94 SRC=151.141.85.61
     91 SRC=153.104.189.234
     89 SRC=24.186.123.213
     89 SRC=151.141.61.120
     85 SRC=164.107.109.84
     71 SRC=68.164.42.178
     71 SRC=4.13.227.219
     70 SRC=218.144.113.159
     69 SRC=24.25.37.160
```

4. What are the different scan patterns (sequential, etc) you can notice? Do you think all come from different attack tools? Any long term ("low and slow") scanning activity?

Taking the top notorious source SRC=210.105.40.67 in the TCP/6129 scan, it can be noticed that the scan is sequential with sequentially-increasing source port SPT numbers and sequentially-increasing target IP addresses. From the time between probes, this is a fast sequential SYN scan.

```
Feb  7 21:43:54 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.64 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=53870 DF PROTO=TCP SPT=15269 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:54 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.67 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=54638 DF PROTO=TCP SPT=15272 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:55 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.70 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=55406 DF PROTO=TCP SPT=15275 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:55 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.69 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=55150 DF PROTO=TCP SPT=15274 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:56 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.72 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=55918 DF PROTO=TCP SPT=15277 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:56 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.73 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=56174 DF PROTO=TCP SPT=15278 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:56 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.71 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=55662 DF PROTO=TCP SPT=15276 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
Feb  7 21:43:56 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=210.105.40.67 DST=11.11.11.75 LEN=44
 TOS=0x00 PREC=0x00 TTL=113 ID=56686 DF PROTO=TCP SPT=15280 DPT=6129 WINDOW=8192 RES=0x00 SYN URGP=0
```

Taking the source SRC=24.17.237.70 in the TCP/6129 scan, there is a random delay within scans at two segmented periods, the first occurring from 00:00:02 hrs while the other occurring from 10:34:08 hrs. Also noticeable is that the first scan targeted IP addresses in increments of 5 between 11.11.11.95 till 11.11.11.125. The source port is fixed at 220. In addition, the packet length is different. Thus likely a different attack tool from above. I would regard this scan as moderately low and slow.

```
Feb  1 00:00:02 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.95 LEN=40
TOS=0x00 PREC=0x00 TTL=113 ID=27095 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:00:24 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.100 LEN=40
 TOS=0x00 PREC=0x00 TTL=113 ID=31168 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:00:46 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.105 LEN=40
 TOS=0x00 PREC=0x00 TTL=113 ID=35169 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:01:09 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.110 LEN=40
 TOS=0x00 PREC=0x00 TTL=113 ID=39230 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:01:36 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.115 LEN=40
 TOS=0x00 PREC=0x00 TTL=114 ID=43270 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:02:00 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.120 LEN=40
 TOS=0x00 PREC=0x00 TTL=113 ID=47327 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 00:02:21 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.125 LEN=40
 TOS=0x00 PREC=0x00 TTL=113 ID=51354 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 10:34:08 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.64 LEN=40
TOS=0x00 PREC=0x00 TTL=113 ID=23293 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 10:34:21 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.67 LEN=40
TOS=0x00 PREC=0x00 TTL=113 ID=25708 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 10:34:30 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.69 LEN=40
TOS=0x00 PREC=0x00 TTL=114 ID=27317 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 10:34:35 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.70 LEN=40
TOS=0x00 PREC=0x00 TTL=113 ID=28109 PROTO=TCP SPT=220 DPT=6129  WINDOW=16384 RES=0x00 SYN URGP=0
Feb  1 10:34:39 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.17.237.70 DST=11.11.11.71 LEN=40
TOS=0x00 PREC=0x00 TTL=113 ID=28909 PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
```

By grepping at the TCP flags, SYN FIN Christmas tree scan was not detected.

5. What other common internet noise types do you see?

One common internet noise is DNS lookups.

```
Feb  1 09:06:16 bridge kernel: Legal DNS: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67 DST=22.22.22.40 LEN=71 TOS
=0x00 PREC=0x00 TTL=64 ID=24007 DF PROTO=UDP SPT=4250 DPT=53 LEN=51
Feb  1 09:06:16 bridge kernel: Legal DNS: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67 DST=22.22.22.40 LEN=71 TOS
=0x00 PREC=0x00 TTL=64 ID=24052 DF PROTO=UDP SPT=4251 DPT=53 LEN=51
Feb  1 09:06:17 bridge kernel: Legal DNS: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67 DST=22.22.22.40 LEN=71 TOS
=0x00 PREC=0x00 TTL=64 ID=24052 DF PROTO=UDP SPT=4252 DPT=53 LEN=51
Feb  1 09:06:17 bridge kernel: Legal DNS: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67 DST=22.22.22.40 LEN=71 TOS
=0x00 PREC=0x00 TTL=64 ID=24103 DF PROTO=UDP SPT=4253 DPT=53 LEN=51
Feb  1 09:06:17 bridge kernel: Legal DNS: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67 DST=22.22.22.40 LEN=71 TOS
=0x00 PREC=0x00 TTL=64 ID=24103 DF PROTO=UDP SPT=4254 DPT=53 LEN=51
```

6. Any unidentified/anomalous traffic observed? Please suggest hypothesis for why it is there and what it indicates.

Anomaly 1:

When answering question 1, it was noticed that there were 7 packets of outgoing traffic from the honeynet categorized under "OUTG CONN OTHERS". Such packets were shown to have a PROTO=2 in the logs. PROTO 2 is IGMP for multicast traffic. It is unusual because it originates from honeypot 11.11.11.67. It occurred at two different periods 3rd Feb and 19th Feb. With a TTL of 1, the multicast is limited within the same subnet as 11.11.11.67.

```
Feb  3 13:43:51 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.0.2 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb  3 13:45:06 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb  3 13:45:11 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb  3 13:45:11 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb 19 12:11:00 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb 19 12:11:01 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb 19 12:11:04 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
```

Looking at traffic before and after, such multicast traffic appears to be associated with the netbios broadcasts originating from 11.11.11.67.

```
Feb  3 13:42:01 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=11.11.11.65 LEN=77 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=2278 DPT=514 LEN=57
Feb  3 13:42:14 bridge kernel: OUTG CONN UDP: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.65 LEN=81 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=2278 DPT=514 LEN=61
Feb  3 13:42:19 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=61.152.102.26
DST=11.11.11.80 LEN=92 TOS=0x00 PREC=0x00 TTL=107 ID=58868 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=1770
Feb  3 13:43:08 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=202.155.34.166
DST=11.11.11.89 LEN=404 TOS=0x00 PREC=0x00 TTL=116 ID=29117 PROTO=UDP SPT=3824 DPT=1434 LEN=384
Feb  3 13:43:47 bridge kernel: Legal Broadcast: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
Feb  3 13:43:47 bridge kernel: Legal Broadcast: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb  3 13:43:51 bridge kernel: Legal Broadcast: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb  3 13:43:51 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=224.0.0.2 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb  3 13:44:34 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=24.207.17.99
DST=11.11.11.110 LEN=92 TOS=0x00 PREC=0x00 TTL=115 ID=31999 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=65050
Feb  3 13:45:06 bridge kernel: OUTG CONN OTHER: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=224.0.1.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Feb  3 13:45:07 bridge kernel: Legal Broadcast: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
Feb  3 13:45:07 bridge kernel: Legal Broadcast: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0 SRC=11.11.11.67
DST=11.11.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
```

Anomaly 2

There appears to be UDP packets initiated from within the honeynet specifically from 11.11.11.67 and specifically targeting UDP/514 on 11.11.11.65, UDP/55247 on 218.38.159.132, UDP/33223 on 216.82.64.254 and UDP/34980 on 158.205.180.50.

11.11.11.67 appears to be deliberating syslog traffic towards 11.11.11.65. Sending syslog traffic to the syslog server on 11.11.11.65 looks legitimate, judging from multiple occurrences from the log. However, the question here is why was the syslog traffic dropped? A hypothesis was that the syslog service on 11.11.11.65 was down at these periods.

What is more notable is the attempted traffic outbound from 11.11.11.67.

```
Feb  1 21:46:29 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=218.38.159.132 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137
DPT=55247 LEN=237
Feb  3 13:42:01 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=11.11.11.65 LEN=77 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=2278
DPT=514 LEN=57
Feb  8 07:00:16 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=11.11.11.65 LEN=73 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=4833
DPT=514 LEN=53
Feb  8 10:54:01 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=11.11.11.65 LEN=82 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=4914
DPT=514 LEN=62
Feb  8 12:01:03 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=11.11.11.65 LEN=157 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=4916
DPT=514 LEN=137
Feb 21 07:06:18 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=216.82.64.254 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137
DPT=33223 LEN=237
Feb 25 09:45:24 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=158.205.180.50 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137
DPT=34980 LEN=237
```

Looking at the traffic before and after such occurrences, above traffic, there were noticeably attempts by external IP addresses (218.38.159.132) in scanning the honeynet IP addresses. 1.11.11.67 has responded on behalf thus reaching the 20 attempts threshold.

```
Feb  1 21:46:27 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=218.38.159.132 DST=11.11.11.84 LEN=78 TOS=0x00 PREC=0x00 TTL=51 ID=33443 DF
PROTO=UDP SPT=55243 DPT=137 LEN=58
Feb  1 21:46:27 bridge kernel: OUTG CONN UDP: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=218.38.159.132 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP
SPT=137 DPT=55243 LEN=237
Feb  1 21:46:27 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=218.38.159.132 DST=11.11.11.87 LEN=78 TOS=0x00 PREC=0x00 TTL=51 ID=33488 DF
PROTO=UDP SPT=55245 DPT=137 LEN=58
Feb  1 21:46:27 bridge kernel: OUTG CONN UDP: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=218.38.159.132 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP
SPT=137 DPT=55245 LEN=237
Feb  1 21:46:28 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=218.38.159.132 DST=11.11.11.89 LEN=78 TOS=0x00 PREC=0x00 TTL=51 ID=33620 DF
PROTO=UDP SPT=55246 DPT=137 LEN=58
Feb  1 21:46:28 bridge kernel: OUTG CONN UDP: IN=br0 PHYSIN=eth1 OUT=br0 PHYSOUT=eth0
SRC=11.11.11.67 DST=218.38.159.132 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP
SPT=137 DPT=55246 LEN=237
Feb  1 21:46:29 bridge kernel: INBOUND UDP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=218.38.159.132 DST=11.11.11.90 LEN=78 TOS=0x00 PREC=0x00 TTL=51 ID=33632 DF
PROTO=UDP SPT=55247 DPT=137 LEN=58
Feb  1 21:46:29 bridge kernel: Drop udp after 20 attempts IN=br0 PHYSIN=eth1 OUT=br0
PHYSOUT=eth0 SRC=11.11.11.67 DST=218.38.159.132 LEN=257 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=UDP SPT=137 DPT=55247 LEN=237
```

Anomaly 3

A fair bit of traffic was dropped on 10th and 11th Feb, which explains the noticeable dips in the traffic charts of inbound 92 bytes ICMP, UDP/1434 and TCP/135 traffic.

```
Feb 10 13:50:22 bridge kernel: INBLOCK: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=4.22.106.52 DST=11.11.11.105 LEN=92
TOS=0x00 PREC=0x00 TTL=112 ID=17103 PROTO=ICMP TYPE=8 CODE=0 ID=21241 SEQ=46667
Feb 10 13:50:46 bridge kernel: INBLOCK: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1 SRC=205.230.103.253 DST=11.11.11.100
LEN=92 TOS=0x00 PREC=0x00 TTL=118 ID=57942 PROTO=ICMP TYPE=8 CODE=0 ID=33697 SEQ=42893
Feb 10 14:00:28 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=00:02:b3:65:c9:71:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.69 DST=11.11
.11.65 LEN=69 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1024 DPT=514 LEN=49
Feb 10 14:00:33 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.69 DST=11.11
.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
Feb 10 14:00:33 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.69 DST=11.11
.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb 10 14:00:34 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=00:02:b3:65:c9:71:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.69 DST=11.11
.11.65 LEN=67 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1025 DPT=514 LEN=47
Feb 10 14:00:34 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.69 DST=11.11
.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
…
Feb 11 10:03:32 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
Feb 11 10:03:32 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb 11 10:03:34 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=96 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=76
Feb 11 10:04:46 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb 11 10:06:46 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=221
Feb 11 10:08:46 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=78 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=137 DPT=137 LEN=58
Feb 11 10:09:01 bridge kernel: INBLOCK: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:b0:d0:87:85:c3:08:00 SRC=11.11.11.67 DST=11.11
.11.255 LEN=214 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=194
```

1-2 pm on 10th sees 2 counts of INBLOCKs.
2-3 pm on 10th sees 151 counts of INBLOCKs.
10-11 am on 11th sees 28 counts of INBLOCKs.
11-12 pm on 11th sees 6 counts of INBLOCKs.

From the log, the INBLOCKs occurred close to what appears to be a restart of the ports. A guess could be that the bridge faced some difficulties in handling the traffic load and had to be re-initialised. Incidentally 8th Feb saw the highest surge in inbound TCP/443 and outgoing UDP traffic (refer to Q1 charts).

```
Feb 10 13:51:02 bridge kernel: eth0: 0 multicast blocks dropped.
Feb 10 13:51:03 bridge kernel: br0: port 2(eth0) entering disabled state
Feb 10 13:51:03 bridge kernel: eth1: 0 multicast blocks dropped.
Feb 10 13:51:03 bridge kernel: br0: port 1(eth1) entering disabled state
Feb 10 13:51:05 bridge kernel: br0: port 2(eth0) entering listening state
Feb 10 13:51:20 bridge kernel: br0: port 2(eth0) entering learning state
Feb 10 13:51:35 bridge kernel: br0: port 2(eth0) entering forwarding state
Feb 10 13:51:35 bridge kernel: br0: topology change detected, propagating
Feb 10 13:52:24 bridge kernel: br0: port 2(eth0) entering disabled state
Feb 10 13:52:24 bridge kernel: device eth0 left promiscuous mode
Feb 10 13:52:24 bridge kernel: br0: port 1(eth1) entering disabled state
Feb 10 13:52:24 bridge kernel: device eth1 left promiscuous mode
```

Anomaly 4

ICMP type 8 code 0 packets of size 92 bytes smell of nachi worm. Since Nachi runs on windows platforms, the TTL would be counting from 128. However, sieving through the log, such ICMP packets with TTL counting from 256 is detected from 2 IP addresses within the network 148.243.211.0. It would seem either that 148.243.211.0 network comprises of non-Windows-based systems or the TTL was deliberately set as such.

```
Feb  6 18:06:19 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.247 DST=11.11.11.64 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=27691
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=47552
Feb  6 18:06:19 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.247 DST=11.11.11.67 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=27694
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=48320
Feb  6 18:06:19 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.247 DST=11.11.11.69 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=27696
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=48832
Feb  6 18:06:19 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.247 DST=11.11.11.70 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=27697
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=49088
…
Feb 13 02:14:15 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.60 DST=11.11.11.95 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=37372
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=35433
Feb 13 02:14:15 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.60 DST=11.11.11.100 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=37377
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=36713
Feb 13 02:14:15 bridge kernel: INBOUND ICMP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=148.243.211.60 DST=11.11.11.105 LEN=92 TOS=0x00 PREC=0x00 TTL=243 ID=37384
PROTO=ICMP TYPE=8 CODE=0 ID=256 SEQ=37993
```

7. Was the honeypot compromised during the observed time period? How do you know?

The honeypot was compromised during the observed time period. Since the honeypot should be not initiating any unsolicited traffic outbound, any such traffic (which would exclude identd and UDP responses) implies that the honeypot is compromised. Such traffic can be captured by extracting the SYN packets originating from the honeynet outbound.

Hackers or worms usually waste no time upon gaining access to download tools or rootkits from external storage sites via web or FTP downloads. Thus, the honeypot should be compromised on 7th Feb at around 1628 hrs.

```
$ grep "OUTG CONN TCP" honeynet-Feb1_FebXX.log | sed 's/DF//g' |grep -v ACK | grep SYN |
grep -v DPT=113 | awk '{print $1,$2,$3,$13,$14,$18,$22,$23,$25,$26,$27,$28,$29,$30}'
Feb 7 16:28:50 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 06:52:55 SRC=11.11.11.67 DST=62.211.66.12 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 06:53:56 SRC=11.11.11.67 DST=62.211.66.12 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 06:54:47 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 06:55:20 SRC=11.11.11.67 DST=62.211.66.12 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 07:08:02 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 07:09:20 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 07:14:07 SRC=11.11.11.67 DST=193.230.153.133 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 07:14:41 SRC=11.11.11.67 DST=193.230.153.133 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 07:25:37 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 07:34:30 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:50:11 SRC=11.11.11.67 DST=64.161.61.115 TTL=64 DPT=1291 WINDOW=5840 SYN URGP=0
Feb 8 10:56:35 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:56:38 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:56:44 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:56:56 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:57:20 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:57:25 SRC=11.11.11.67 DST=195.27.176.155 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 10:58:08 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:01:20 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:46:51 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:46:54 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:47:00 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:47:12 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:47:36 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:48:24 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:48:27 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:48:33 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:48:45 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:49:09 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:51:45 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 11:56:19 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:01:03 SRC=11.11.11.67 DST=216.254.0.38 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 12:08:49 SRC=11.11.11.67 DST=62.211.66.12 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:10:27 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:15:14 SRC=11.11.11.67 DST=66.187.232.40 TTL=64 DPT=21 WINDOW=5840 SYN URGP=0
Feb 8 12:19:41 SRC=11.11.11.67 DST=195.27.176.155 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:24:08 SRC=11.11.11.67 DST=195.27.176.155 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:36:41 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 12:36:44 SRC=11.11.11.67 DST=207.66.155.21 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
Feb 8 13:46:48 SRC=11.11.11.67 DST=64.161.61.115 TTL=64 DPT=1051 WINDOW=5840 SYN URGP=0
Feb 9 12:06:02 SRC=11.11.11.67 DST=64.161.61.115 TTL=64 DPT=3184 WINDOW=5840 SYN URGP=0
```

```
  Count Source          Target port
     33 SRC=11.11.11.67 DPT=80
      6 SRC=11.11.11.67 DPT=21
      1 SRC=11.11.11.67 DPT=3184
      1 SRC=11.11.11.67 DPT=1291
      1 SRC=11.11.11.67 DPT=1051
```

8. If you'd obtain such firewall logs from a production system, what source IPs or groups of such IPs you'd focus on as a highest threat?

The source IPs I would focus on as the highest threat would be. Inbound traffic from both these IP addresses has the closest proximity to when the honeypot started initiating outbound traffic.

A. 61.120.200.227

This IP address has been attempting connections to TCP/80 and TCP/443 within the honeynet since Feb 7 15:42:06 until Feb 7 16:50:37. It is likely a scan of potential vulnerabilities for HTTP and HTTPS and the period of scan falls nicely where the first outbound SYN packet was sent from the honeynet.

```
Feb 7 16:28:50 SRC=11.11.11.67 DST=209.63.57.10 TTL=64 DPT=80 WINDOW=5840 SYN URGP=0
```

B. 66.60.166.84

This IP address has been attempting connections to TCP/80 and TCP/443 from Feb 7 16:20:23 until Feb 8 07:32:31, again in close proximity to the honeypot initiated traffic.

9. What honeypot systems were attacked the most? What ports were open on each of them? Why do you think machines with close IP addresses were attacked differently?

11.11.11.75 was attacked the most.

```
$ grep "INBOUND" honeynet-Feb1_FebXX.log | sed 's/DF//g' | awk '{print $13}' | sort |
uniq -c | sort -rn
  30730 DST=11.11.11.75
  14445 DST=11.11.11.80
  13303 DST=11.11.11.100
  13265 DST=11.11.11.105
  12981 DST=11.11.11.67
  12909 DST=11.11.11.110
  12523 DST=11.11.11.90
  11653 DST=11.11.11.71
  11579 DST=11.11.11.87
  11286 DST=11.11.11.70
  11107 DST=11.11.11.69
  11088 DST=11.11.11.115
  10915 DST=11.11.11.73
  10772 DST=11.11.11.72
  10656 DST=11.11.11.82
  10398 DST=11.11.11.81
  10270 DST=11.11.11.125
  10169 DST=11.11.11.95
  10011 DST=11.11.11.83
```

Below is the set of TCP ports opened on each honeypot. It is derived by looking at the source port of outgoing TCP ACK traffic. Such TCP traffic with ACK flag set could only be sent from the honeypot as a response to incoming SYN or PSH traffic.

```
$ grep "OUTG CONN TCP" honeynet-Feb1_FebXX.log | sed 's /DF//g' | grep ACK | awk
'{print $13,$21}' | sort | uniq -c | sort -rn | awk '{print $2,$3}' |sort | sed
's/SRC=//g' | sed -e 's/SPT=//g'
11.11.11.67 139
11.11.11.67 443
11.11.11.67 80
11.11.11.69 21
11.11.11.69 443
11.11.11.69 80
11.11.11.71 21
11.11.11.71 443
11.11.11.71 80
11.11.11.72 21
11.11.11.72 443
11.11.11.72 80
11.11.11.73 139
11.11.11.73 21
11.11.11.73 3128
11.11.11.73 443
11.11.11.73 80
11.11.11.75 21
11.11.11.75 443
11.11.11.75 80
11.11.11.80 139
11.11.11.80 21
11.11.11.80 443
11.11.11.80 80
```

For UDP service ports, outgoing UDP responses (apart from syslogging) from the honeynet would imply a UDP service running at the honeypot.

```
$ grep "OUTG CONN UDP" honeynet-Feb1_FebXX.log | sed 's/DF//g' | awk '{print $13,$21}' | sort |
uniq -c | sort -rn | awk '{print $2,$3}' | sed 's/SRC=//g' | sed 's/SPT=//g'
11.11.11.67 137
11.11.11.67 4916
11.11.11.67 2277
11.11.11.67 4912
11.11.11.67 4833
11.11.11.67 1026
11.11.11.67 4914
11.11.11.67 4831
11.11.11.67 4834
11.11.11.67 4827
11.11.11.67 1050
11.11.11.67 4713
11.11.11.67 1070
11.11.11.67 4925
11.11.11.67 4915
11.11.11.67 4709
11.11.11.67 4829
11.11.11.67 4711
11.11.11.67 2278
```

I think machines with close IP addresses are attacked differently because firstly because of the varying services running on them and secondly because of the vulnerabilities detected during the scans performed on these services. Exploits are usually tailored based on the applicable vulnerabilities. A guess is that 11.11.11.75 might have more vulnerabilities on its web services.

Bonus Question: Provide some high-level metrics about the data (such as most frequently targeted ports, etc) and make some conclusions based on them.

Please refer to Question 1 answer.

References

http://www.dshield.org
http://www.incidents.org
http://www.honeynet.org