# Background Traffic to Network 36.0.0.0/8

November 2010

Geoff Huston
George Michaelson
APNIC R&D
research@apnic.net

APNIC is now regularly examining the unused state of IPv4 address blocks before they are passed over for general allocation. Experiments are undertaken with these address blocks by advertising a route to the address block, and recording all incoming traffic received in response to the routing advertisements. This document reports on the results of this experiment in the identification of the patterns of such "background" traffic that is being directed to the address block 36.0.0.0/8.

APNIC expresses its appreciation for the generous assistance provided by NTT and Merit in undertaking this series of experiments.

## Experiment Details

In collaboration with APNIC, AS237 (Merit) exclusively announced 36.0.0.0/8 for the period from 24 October 2010 until 2 November 2010. The data collector was unfiltered, and the data collection system was entirely passive, and no packets were generated in response to the incoming traffic. For the last 24 hours the announcement overlapped with a parallel announcement of 36.0.0.0/8 from NTT Japan.

## Traffic Profile

Figure 1 shows the traffic profile for network 36.0.0.0/8.

*(The graph utility used here does not make this adequately clear, but in the following figures the red trace is the total traffic, the blue trace is TCP, the green trace is UDP, the violet trace is ICMP and the cyan trace is all other protocols.)*

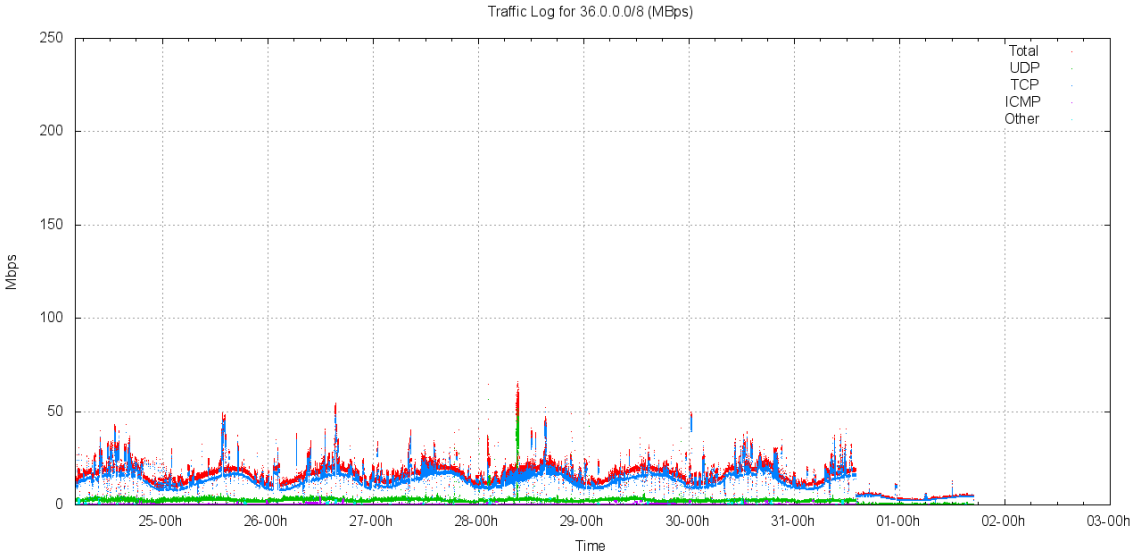


*Figure 1 – Traffic profile for 36.0.0.0/8*

This traffic profile is similar to the profile that was recorded for other /8 address blocks recently allocated to APNIC, including 49.0.0.0/8 and 101.0.0.0/8. The address block 36/8 attracts some 12 – 25Mbps of incoming traffic. Of this, some 83% of the traffic is TCP and 15% is UDP, with the remainder being predominately ICMP.

The traffic shows a pronounced diurnal pattern, which most visible in the TCP component of the traffic. There is no clear weekday / weekend delineation.

In terms of protocol distribution, the distribution of incoming bytes in these two address blocks are shown in Table 1. This table also includes previously collected data concerning the protocol distribution in 49.0.0.0/8, 14.0.0.0/8 and 223.0.0.0/8.

| Protocol | Proportion of Traffic<br>36.0.0.0.8 | 101.0.0.0/8 | 49.0.0.0/8 | 14.0.0.0/8 | 223.0.0.0/8 |
|---|---|---|---|---|---|
| **TCP** | 82.8% | 76.0% | 81.5% | 66.2% | 71.4% |
| **UDP** | 14.5% | 22.7% | 17.4% | 25.6% | 27.6% |
| **ICMP** | 2.0% | 0.9% | 1.1% | 8.0% | 0.9% |
| **Other** | 0.7% | 0.4% | 0.0% | 0.2% | 0.1% |

*Table 1. Distribution of Traffic by Protocol*

Of note here is that the incoming traffic in network 36.0.0.0/8 has a slightly lower component of TCP traffic, and a corresponding higher UDP component compared to two of the other three network blocks, although it is most similar in profile to 49.0.0.0/8.

Also of note in terms of traffic profile, incoming TCP traffic in network 36.0.0.0/8 shows a marked diurnal pattern, while the UDP traffic levels do not show such a marked diurnal pattern.

The second view of the overall traffic profile is by packet count rather than traffic (byte) counts. The packet profile of incoming traffic in this network block is shown in the following figure.

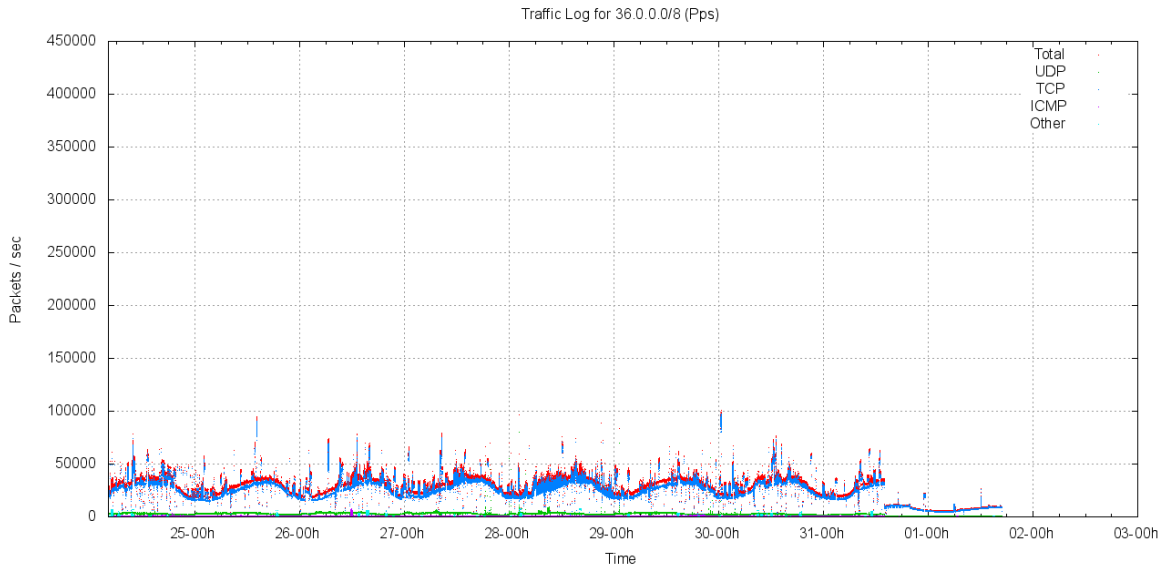


*Figure 2 – Packet profile for 36.0.0.0/8*

The 36/8 network block attracts between 25,000 and 45,000 packets per second, where 87% of the incoming packets are TCP, between 14.2% are UDP, 6.1% are ICMP and the remaining packets represent 4.6% of the total.

In terms of protocol distribution, the distribution of incoming bytes in these two address blocks are shown in Table 2. This table also includes previously collected data concerning the protocol distribution in 49/8, 14/8 and 223/8 for comparison.

| Protocol | Proportion of Packets<br>36.0.0.0/8 | 101.0.0.0/8 | 49.0.0.0/8 | 14.0.0.0/8 | 223.0.0.0/8 |
|---|---|---|---|---|---|
| **TCP** | 88.4% | 83.1% | 86.9% | 50.0% | 50.0% |
| **UDP** | 9.2% | 16.1% | 14.2% | 36.5% | 35.7% |
| **ICMP** | 1.7% | 0.7% | 6.1% | 9.9% | 13.9% |
| **Other** | 0.7% | 0.2% | 4.6% | 3.6% | 0.3% |

*Table 2. Distribution of Packets by Protocol*

The third form of traffic profile is in terms of packet size distribution. TCP packets are predominately 62 octet SYN packets (16,504M of the 18,271M TCP packets (90%) were TCP SYN packets).

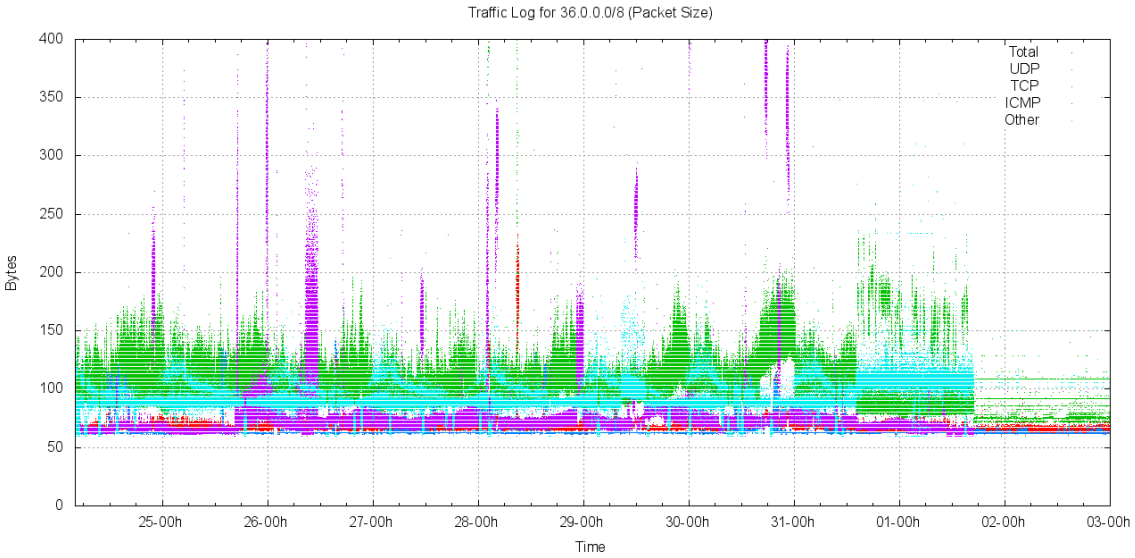


*Figure 3 – Packet size distribution for 36.0.0.0/8*

Of note in the data collected is the ICMP and "other protocol" extended bursts of larger packet sizes.

## Distribution of Traffic Across /16s

The following figure shows the distribution of traffic across the /8 address block, divided up into each of the 256 /16 address blocks. Figure 4 shows this distribution for 36.0.0.0/8.

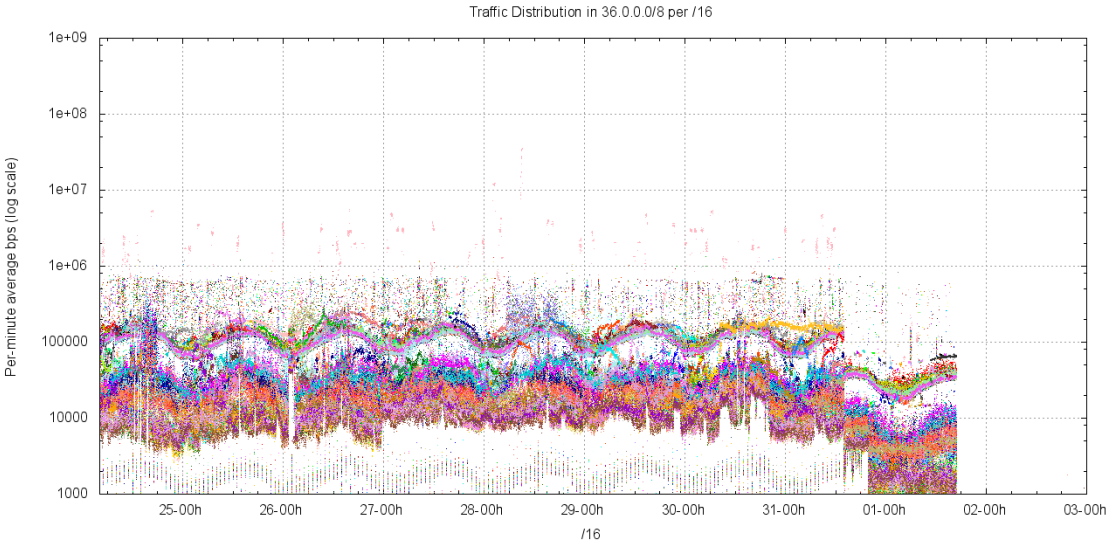


*Figure 4 – Traffic distribution per /16 for 36.0.0.0/8*

In almost all cases the level of incoming traffic lies between 10Kbps to 200Kbps, with a visible diurnal component. There is a "banding" into two traffic profiles: the low /9 exhibits an average traffic level of some 110Kbps per /16, while the high /9 exhibits an average traffic level of 15kbps, consistent with the scanning behaviour of the conficker virus, as seen in other /8s tested in 2010 by APNIC.

The distribution of average traffic levels for each of the /16s in net 36/8 is shown in the following figure.

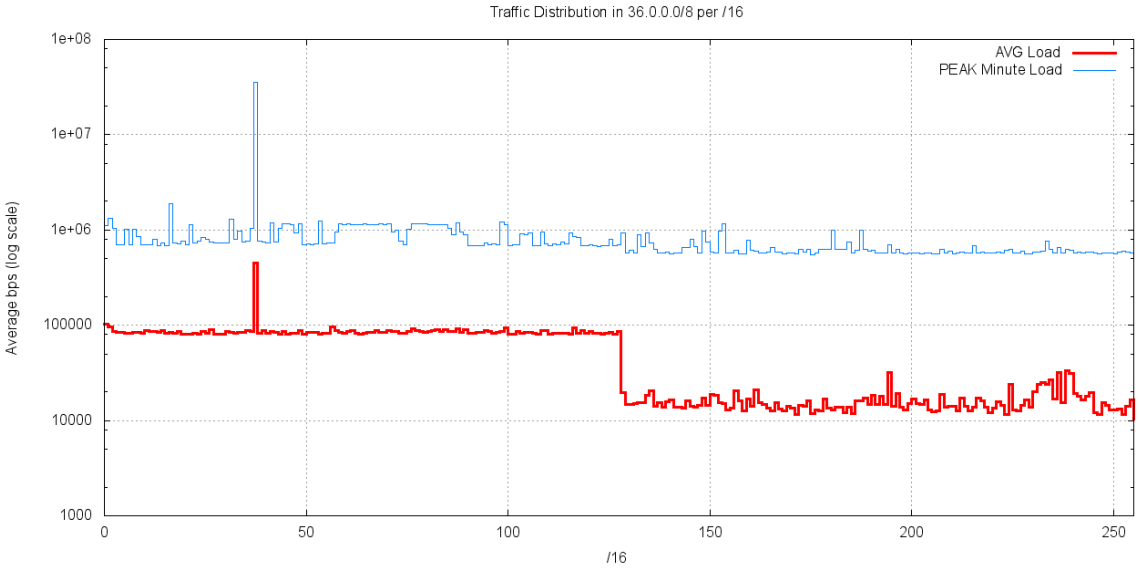


*Figure 5 – Average Traffic load per /16 for 36.0.0.0/8*

This data collection shows a pronounced break in the "middle" of the address block. The low half of the address block (36.0.0.0/9) has an average traffic load of 100Kbps per /16, while the upper half of the block (36.128.0.0/9) has an average traffic load of 20Kbps. The peak traffic point lies at 36.37.0.0/16.

There is only one /16 that appear to show an anomalously high levels of traffic, namely 36.37.0.0/16. No other /16 appears to present anomalous activity in this experiment.

## Distribution of Traffic

The following figure shows the distribution of traffic levels per /24 in network 36.0.0.0/8.

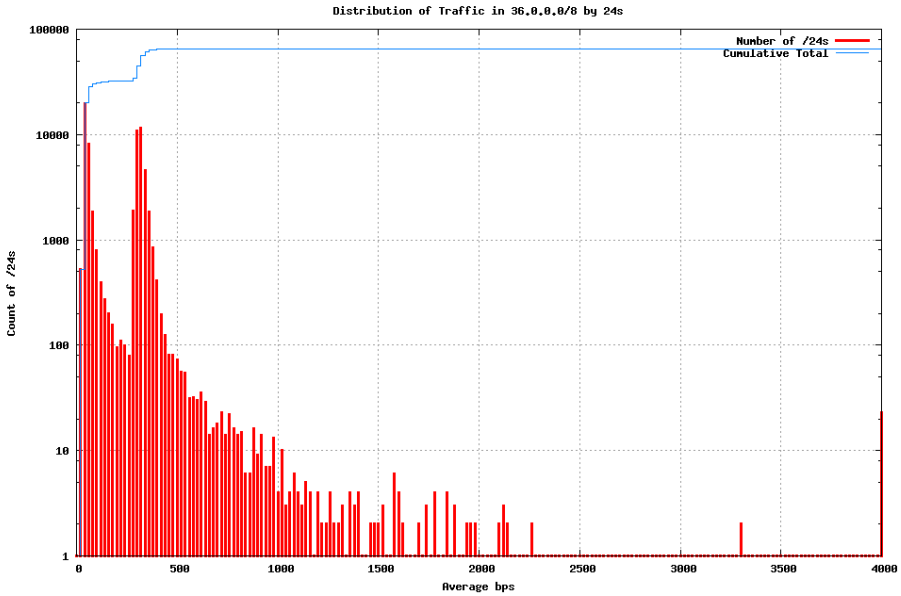


*Figure 6 – Traffic profile for 36.0.0.0/8 by /24s*

The second peak in this distribution at 400bps per /24 is due to Conficker scanning across the low /9 of the address block. It appears that the Conficker scanning traffic element is common across the entire IPv4 address range, and this additional traffic component directed to TCP port 445 in the low /9 of this two address block is not an anomaly that warrants any particular action in terms of reservation of addresses from allocations or assignments.

Using a threshold value of a average incoming traffic rate of more than 10Kbps per /24, corresponding to 40 bits per second per address, or approximately 1 packet on average every 20 seconds per address, then there are 5 /24s in 36.0.0.0/8 that exceed this level of traffic.

| /24 Prefix | Avg Traffic |
|---|---|
| 36.37.38.0/24 | 380 Kbps |
| 36.194.54.0/24 | 18 Kbps |
| 36.0.0.0/24 | 15 Kbps |
| 36.56.249.0/24 | 14 Kbps |
| 36.224.105.0/24 | 11 Kbps |

*Table 3 – Traffic profile for highest traffic /24s in 36.0.0.0/8*

However, with the exception of 36.0.0.0/24 none of these networks have a sustained incoming traffic profile at that rate, but received the traffic in short bursts (as shown, for example, in the profile recorded for 36.194.54.0/24 below). The network 36.37.38.0/24 is notable because of the short (1 – 2 minute) bursts of incoming traffic in the order of 2 Mbps – 5 Mbps that were recorded over the experiment period.

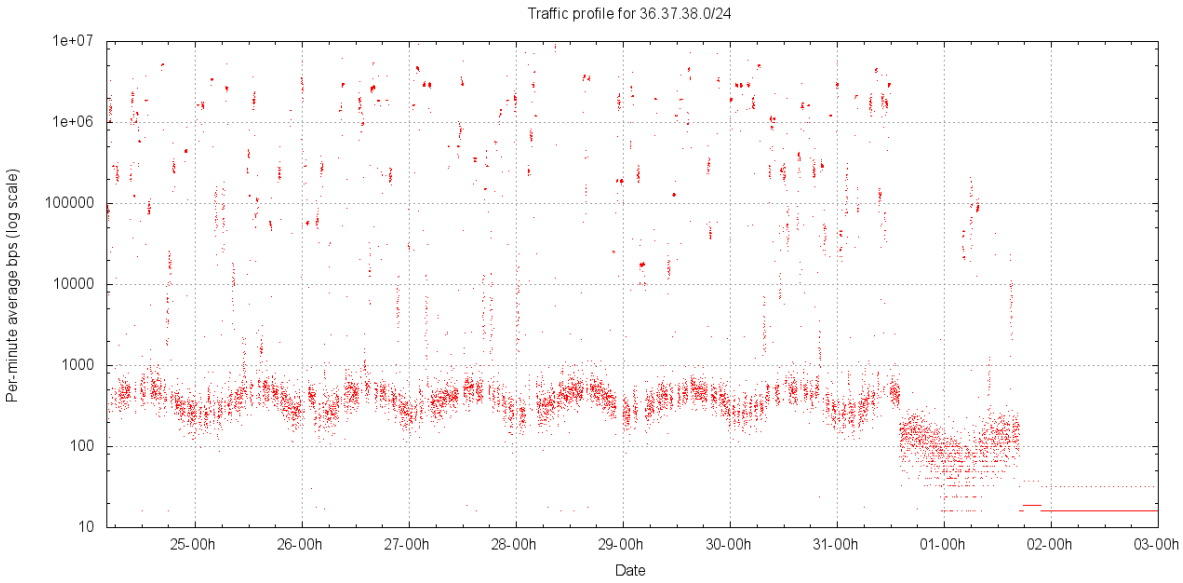


*Figure 7 – Traffic profile for 36.37.38.0/24 (per minute average incoming traffic)*

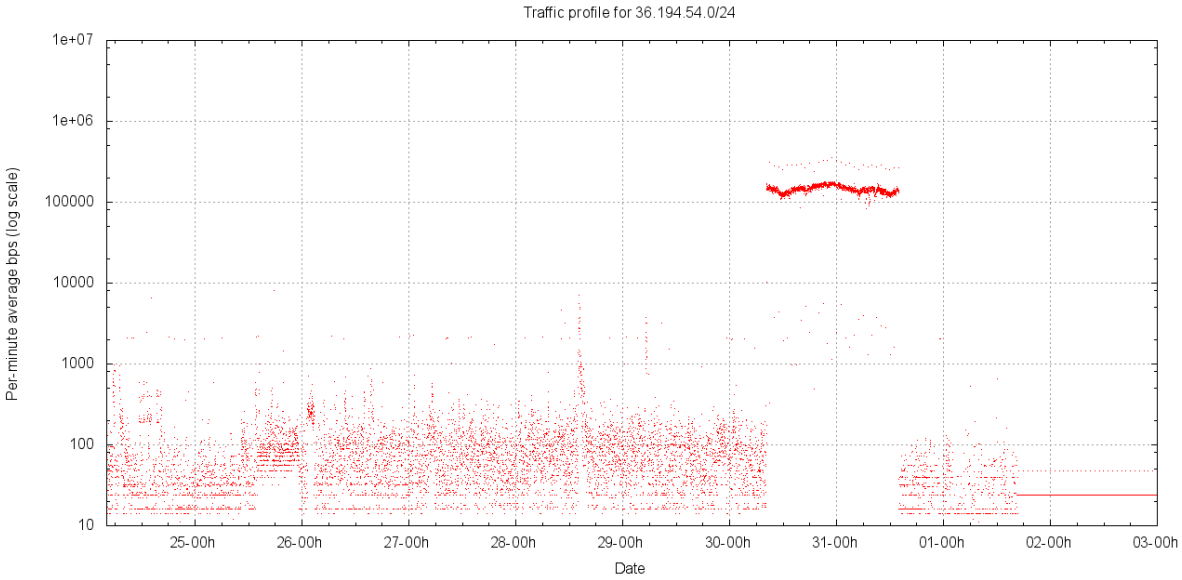


*Figure 8 – Traffic profile for 36.194.54.0/24 by /24s (per minute average incoming traffic)*

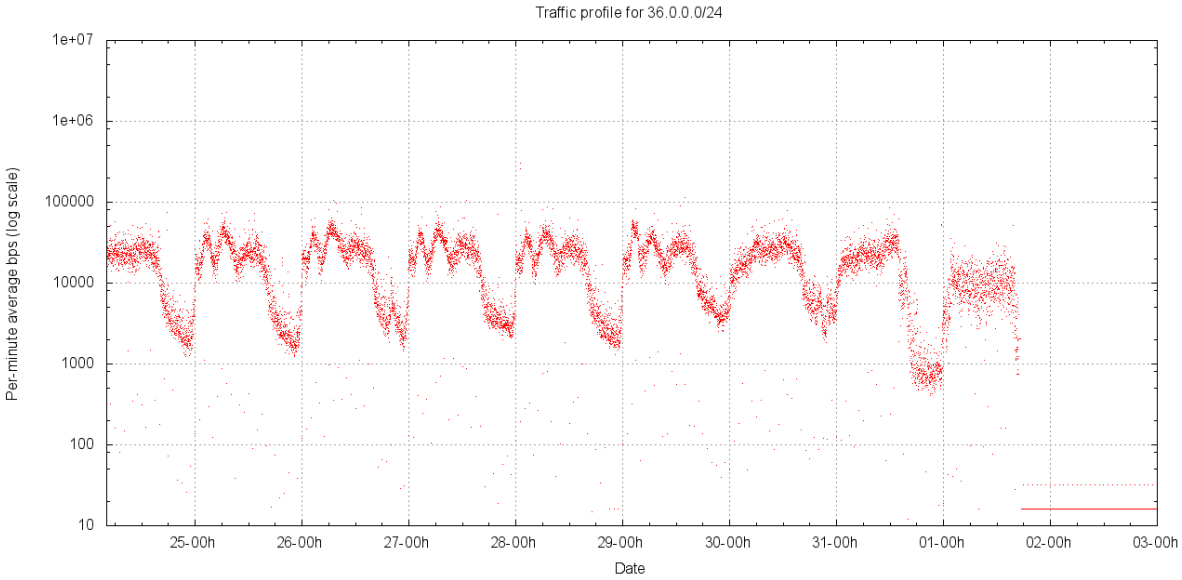


*Figure 9 – Traffic profile for 36.0.0.0/24 (per minute average incoming traffic)*

## Conclusions

It is recommended that 2 /24 prefixes be withheld from regular allocation or assignment from 36.0.0.0/8 for a period of 3 months, allowing a second round of testing of these particular prefixes at that time.

These withheld prefixes are:

**36.0.0.0/24**
**36.37.38.0/24**