SENATE INQUIRY INTO 2016 CENSUS

RESPONSE OF VOCUS COMMUNICATIONS LIMITED TO THE SUBMISSION OF IBM AUSTRALIA LIMITED

18 OCTOBER 2016

Vocus Communications | ABN 96 084 115 499 | vocus.com.au
Level 12, 60 Miller Street, North Sydney, NSW 2060

Introduction

Vocus Communications Limited (**Vocus**) is an ASX listed telecommunications company delivering services across Australia and New Zealand. One of the services which Vocus provides is IP Transit services and DDoS protection services.

Vocus was an upstream supplier of Nextgen Networks Pty Ltd (**Nextgen**) and provided IP Transit Services and DDoS protection services to Nextgen which it resupplied to IBM Australia Limited (**IBM**) for use in relation to the eCensus website.

There are several comments by IBM in its submission to the Senate's Inquiry into 2016 Census (**IBM Submission**) which Vocus does not agree with. Vocus appreciates the opportunity to respond to those comments. Vocus' response is limited to the comments of IBM which related directly to Vocus or its services.

Vocus response to IBM Submission

DDoS attack magnitude

At paragraph 12 of the IBM Submission, IBM submits that the fourth DDoS attack was '*of significant size and had the effect of causing the site to become unresponsive and unavailable to the public…'*

Vocus does not agree that the fourth DDoS attack was the cause of the site becoming unresponsive. The fourth attack comprised of attack traffic which peaked at 563Mbps which is not considered significant in the industry, and lasted 14 minutes. See report from Arbor Networks which indicates that it is materially below the mean attack size (https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf).

Such attacks would not usually bring down the census website which should have had relevant preparations in place to enable it to cater for the expected traffic from users as well as high likelihood of DDoS attacks.

Events leading up to the shutdown of the eCensus website

The cause of the census website being unreachable was IBM employee's falsely identifying normal traffic patterns as data exfiltration, and manually turning off their Internet gateway routers (see paragraph 17 of IBM Submission) which IBM took approximately 3 hours to configure and bring the website back up again (see paragraphs 19 and 87 of IBM Submission). It is not clear from paragraph 17 of IBM Submission what 'miscarry' took place which triggered IBM's decision to shut down access to the site.

With respect to paragraph 13, as noted above, the traffic coming through the Singapore link amounted to a total of 563Mbps, and not of a size to cause the census website to become unresponsive, had appropriate network security measures been implemented by IBM. In addition, it is incorrect for IBM to represent that DDoS attack traffic travels through a single link, in this case, the Vocus Singapore peering link. Referring to IBM's technical description of DDoS attacks at paragraphs 61 to 64 of the IBM Submission, Vocus adds that the devices ('botnets') can be located anywhere in the world, including inside Australia. Furthermore, the Island Australia approach does not consider the reality of overseas network operators connecting to Australian service providers inside Australian borders. In fact, during the fourth DDoS attack, Vocus had blocked the vast majority of DDoS traffic, only passing on a small percentage of the total traffic from botnet hosts in Asia and Australia.

Once Vocus was made aware of the fourth DDoS Attack, it implemented a static null route to block additional DDoS traffic at its international border routers within 15 minutes.

Testing and implementation of Island Australia

On 1 August 2016, Vocus advised Nextgen that it did not provide geo-blocking. In its discussions with Nextgen regarding appropriate DDoS protection strategies, Vocus was in fact requested to disable its DDoS protection product covering the eCensus IP space. If Vocus DDoS protection product was left in place the eCensus website would have been appropriately shielded from DDoS attacks. Vocus disagrees with the assessment that these DDoS protection measures were inappropriate due to the eCensus "unique traffic profile" (see paragraph 77 of IBM Submission). The final measure agreed with Nextgen was that Vocus would implement Remote Triggered Black Hole (**RTBH**) route advertisements with international carriers that support RTBH.

Vocus was not, at any time prior to 9 August 2016, invited to participate in any testing of IBM's DDoS mitigation strategy, or given any detail of what testing was undertaken. In fact, Vocus was not informed of IBM's DDoS mitigation strategy, Island Australia or its specific requirements, until after the fourth attack. As a result, any assumption that Vocus was required to, or had implemented Island Australia or geo-blocking including, without limitation, as mentioned at paragraphs 14, 16, 82, 83, 92, 94, 95 and 96 are inaccurate. It follows that the 'error' which IBM submits at paragraphs 13 and 95 of the IBM Submission that Vocus had committed is inaccurate as Vocus was not, prior the fourth attack, advised of Island Australia.