Post Incident Review

datanet.co.uk
Private Cloud Solutions

Date: 13th August 2015

Author: Neil Sperring, Technical Director
Case ref: 104-21830 - Distributed denial-of-service (DDoS) attack resulting in a Major Service Outage (MSO)

Contents:
1. Report Aims
2. Customer Impact, Experience & Affected Infrastructure
3. Incident Summaries
4. Root Cause
5. Risk Mitigation, Key Observations & Lessons Learnt

1. Report Aims
This report has been produced by Datanet to provide further detail and clarification of the issues which impacted the Datanet core network, resulting in a loss of services on the 12th August 2015.

2. Customer Impact, Experience & Affected Infrastructure
At approximately 11:30 on 12th August 2015, we became aware of a substantial increase in traffic across our two London data centres and Aspen House, Fleet. This resulted in a loss of multiple services on our core network. The duration of this loss of service was 3 hours 30 minutes and impacted both our connectivity and colocation services.

3. Incident Summaries
11:30 Neil Sperring (NS) and Mike Reed (MR) were made aware of the issues by Brian Money (BM) and Peter Smith (PS) who were taking calls on the Service Desk. NS and MR immediately reviewed the status of our network monitoring system Observium and started to investigate the problem.

11:45 NS and MR identified that one particular co-location customer was maximising the bandwidth available on both the core links to each of our London data centres. Peter Smith (PS) notified the customer of the issue whilst NS and MR investigated blackholing (null interfacing) the customer's subnet at both our London Data Centres.

12:30 NS and MR were successful in blackholing the customer's subnet, however further investigations revealed that the traffic was still saturating our peering and transit provider links in London.

13:00 NS and MR individually contacted each of our peering and upstream transit providers to null the subnets within their networks preventing the traffic reaching us. Within the space of 30 minutes, this restored our transit services and we started to see services come back online and customers were reporting a return of service.

14:00 NS and MR continued to monitor the levels of traffic on the core network and could still see higher than usual volumes of traffic on our LINX Juniper LAN peering at Telecity, London. Having contacted LINX, it became apparent that no level of filtering was available and we took the decision to shut down our port facing the LINX Juniper LAN. As expected, traffic levels on our transit providers increased but remained within operational constraints.

15:00 All services had been restored and were operating as expected.

17:45 The decision was taken by NS and MR to bring back online our LINX Juniper LAN connection and monitor the levels of traffic on this interface. This remained stable and normal levels of traffic were flowing as expected.

13th August 2015 10:00 – Meeting was held internally to analyse our actions taken to address the MSO, understand the lessons learnt should the issue reoccur and agree changes to our procedures in order to respond much more quickly to any future events of this nature.

13th August 2015 15:00 – Major Service Outage (MSO) report generated by NS, agreed by Management Team and published to customers next day.

4. Root Cause

The root cause of the failure was identified as a targeted DDoS attack against a specific Datanet customer. Whilst corrective action was taken, the time taken to realise what was happening, identify the traffic and request assistance from upstream and then to implement the changes within the transit and peering areas of the network could have been executed much quicker.

Note: When a DDoS attack occurs it is industry best practise to identify the source and destination of the traffic and request upstream providers to drop (or null) that traffic.

5. Risk Mitigation, Key Observations & Lessons Learnt

Datanet will continue to use the same NOC monitoring tools we use currently, but will review and modify our procedures so that in the event of a DDoS attack reoccurring on our core network, we will immediately identify the target of the attack and implement measures with our upstream transit providers to null the subnets being affected.

In terms of our peering, we will look to increase, where available, the number of organisations we peer with to more equally balance the traffic between LINX Juniper and LINX Extreme in our separate London data centres. We will also investigate the use of scrubbing services to handle such volumetric attacks in the future.

An update to operational procedures including more understanding and training for our technical staff has already begun and will continue to ensure we respond much quicker and more appropriately in future.