# Incident Report

## Interxion DSL Disconnections 17/09/16

**Report Date: 19th September 2016**

**Introduction:**

This report details the incident of DSL services which connect through our Interxion core router, disconnecting on the 17th September 2016 at approximately 13:47.

**Series of events:**

On the 17th September we started to receive correspondence from some customers reporting that their connections were offline. Initial reports started coming into the desk shortly after the disconnections had occurred, from 13:54 onwards.

After handling the initial reports, our Support agents submitted a case for our NOC to review. At 14:51, the initial feedback from our NOC engineer was that there was instability experienced on some interfaces on the side of the DSL platform handled by Interxion. Stability had since returned but our NOC engineer was continuing to monitor closely.

Some customers who had reported the issue had seen services come back online from approximately 14:10 onwards and users continued to reconnect into the afternoon. Reboots of equipment on site were reconnecting services which hadn't come back online automatically.

Upon further investigation, it has since been confirmed that the disconnections were caused by a large DDOS attack aimed at a subscriber on our network. A routing protocol was then torn down on multiple interfaces on the Interxion DSL platform due to extremely high CPU levels caused from handling the additional load. The first disconnections were seen at 13:47 before stability returned at 14:07 once the DDOS attack had passed.

It appears that in this scenario, the DDOS protection policies we run over our network did not catch the attack. There are a few bespoke scenarios where this can occur and therefore we are introducing a 2nd protection system to run alongside the current one, which monitors for attacks such as this differently. Therefore moving forward, should the protection policies which were in place fail to pick up an attack, the alternative protection will do so, eliminating the chance of a repeat scenario.

In addition to the alternative DDOS protection being implemented, we are also in the process of upgrading the key hardware which was involved during this incident. Whilst by no means was this scenario caused by a piece of hardware not behaving as expected, further upgrades and increased capability would will still be beneficial and reduce impact in any load related scenario moving forward.

We apologise for any inconvenience or disruption caused by this incident.