PSD GROUP
Tailored Technology and Communication Solutions
CCC IT SOLUTIONS | SCHOOLCARE | LOGI-CALL | BROADBAND4

Suite 5, Hillfields House,
Castleman Way, Hampshire,
BH24 3BA

t: 0333 240 2622
e: sales@psdgroup.co.uk
www.psdgroup.co.uk

BROADBAND4 CONNECTIVITY ISSUE 30/04/21

The Issue

PSD Group monitoring alerted engineers to a drop in outbound connectivity to a number of customers on our platform starting at 0842 on 30th April 2021.

PSD Group engineers immediately started to investigate using live information being gathered by our monitoring system to ascertain some commonality between the alerts.

Traffic levels appeared to return to normal around 0857 and engineers continued investigations, which at first glance presented as 100% CPU usage on core routing devices delivering services to our Education Customers. This dropped to normal levels as services appeared to be restored.

A further occurrence of this issue was observed between 1106 and 1116 and 1512 and 1541. Each time high CPU on core Firewall Devices with a corresponding alteration in the traffic profile on primary transit links.

Dara gathered during the incident was analysed on the evening of the 30th, to try and further isolate the root cause. It was surmised that an increase in backup platform traffic may have contributed to the issue, as this was the only obvious correlation, however this was discounted after further investigation over the bank holiday.

As the root cause was not fully confirmed, alterations were made to our monitoring platform to provide more detail on certain metrics to ascertain a root cause.

No further incidents were observed over the Weekend and the Bank Holiday, with traffic levels remaining normal.

Monitoring identified a further incident on 1353 on Tuesday 4th May following a similar pattern as the previous incident which concluded at 1420.

Engineers immediately investigated the issue, using the new monitoring metrics and observed a Distributed Denial of Service Attack (DDoS) directed towards a single customer IP Address. This traffic was “blackholed” and traffic issues were observed as returning to normal, along with the CPU load on the firewalls.

The network remained stable after the Blackholing of the traffic on our primary transit link.

Minor packet loss was observed on the morning of the 5th May, with attack traffic (albeit a smaller volume) being presented on our secondary peering link, ALL IP traffic to the customer IP was dropped whilst an investigation took place.

Suite 5, Hillfields House,
Castleman Way, Hampshire,
BH24 3BA

t: 0333 240 2622
e: sales@psdgroup.co.uk
www.psdgroup.co.uk

The Cause

The root cause of the outage was identified as a targeted DDoS Attack directed towards a customer IP.

The customer has investigated and using a mixture of Broadband4 Filtering Logs and on premises classroom management tools, identified an individual who was involved in the arrangement of the DDoS attack, highlighting and confirming this was a targeted attack, as opposed to a random one.

The Resolution

PSD Group are reviewing internal procedures around the triage and quick identification of DDoS attacks and implementing specific processes around the blackholing of offending traffic to reduce the overall impact of a potential attack on the network as a whole.

By their nature and scale DDoS attacks are very hard to completely mitigate, however we will continue to evaluate commercial solutions aimed at attack mitigation.