RFO report on Network and DNS outage 27/10/2015

Date of Incident : 27/10/2015

Background

At 12:11pm on Tuesday 27th of October Blacknight experienced a network outage which impacted blacknight.com name servers, shared hosting, shared hosting email, hosted exchange, webmail and our cloud1, cp.blacknight.com control panels.

The issue appeared initially and for some time thereafter to be a huge DDOS attack targeted at ns2.blacknight.com and we treated the issue as such.

Chronology

- 12:12 issue starts.
- 12:15 alerts notify our Network Ops Centre and investigation begins.
- 12:17 engineers based in our Carlow data centre begin working on the issue.
- 12:20 engineers reach out to colleagues in our Dublin data centre.
- 12:21 status post on blacknight.tech published by the engineering team.
- 12:22 Social Media team respond to clients on Twitter, Facebook, and Boards.ie by giving them what information was available.
- 12:30 Engineering still working on the root cause. A denial of service attack targeting an authoritative DNS server on our network is the initial indication.
- 12:40 Engineering blackhole the DNS server to try and bring the network under control.
- 13:00 Engineering continue to work on the issue on site, checking all cabling, logs, console servers etc.
- 13:10 Engineering locate a MAC address flapping on a core access switch.
- 13:20 This switch is removed from production.
- 13:30 Engineering team move to further isolate traffic.
- 13:33 Second core access switch removed from production after it was discovered to be partially dropping certain traffic flows from the network.
- 13:33 Traffic on the network returns to normal.
- 13:50 DNS server placed back in production.
- 13:55 full service restored.

Root cause

After much log analysis and on site testing of network equipment we identified an ASIC in acc-sw01.bk2 which was malfunctioning. Basically at the time of the issue it stopped forwarding Ethernet frames correctly and it caused an internal layer 2 loop within our Top Of Rack aggregation layer. As this layer touches off much of our network in our Dub2 datacentre it had a profound impact.

For reference all routed networks continued to operate as usual. This included cloud1, cloud2, BGP customers, IP Transit customers etc.

Follow up

Following on from this issue we'll be investigating a means to further segregate our DNS infrastructure and to prevent issues like this in the future.

We've had a plan in the pipeline for a while to add ns3.blacknight.com into mix and we've already committed to doing this. In addition we'll be upgrading the acc-swXX.bk2 switches to newer Cisco aggregation layer in the near future.

We'll also push our software providers for a supported migration path for ns2 to remove it from the shared hosting network and into a routed VLAN similar to our plan for ns3.

Resolution

Blacknight put acc-sw02.bk2 back into service on Wednesday 28th of October at 1am. Acc-sw01.bk2 has had the ports associated with the faulty ASIC isolated and is still in service. A further maintenance window will be scheduled to replace both acc-sw01/02 in BK2 in the coming weeks.