Minor Prefix Hijack experience

Joel Jaeggli
Fastly

Timeline

May 7 2018

~17:50 UTC AS132116 announces to their peers

151.101.1.0/24
151.101.65.0/24
151.101.129.0/24
151.101.193.0/24

Probably this is in Delhi

ಠ~ಠ

Timeline

17:57 - First Customer notice they can reach their anycast offset from GCE.

Mad rush ensues

20:00 - 21:00 15169 / 8075 confirm they have suppressed the errant peer.

02:30 UTC - AS132116 confirms that they have removed the announcement.

Resolution

On May 8, 2018, at 8:03 AM, XXXXXX XXXXXXXX <supportani@aninetwork.in> wrote:

Dear Sir,

We had found the issue after that we removed the IP pool from our network , so you are requested to please start our BGP session on priority basis.

Regards,
XXXX XXXX

…

This is a lie.

Anatomy of Fastly Anycast Advertisements

151.101.0.0/16 - backing anycast

- 151.101.0.0/22 - http1 anycast
  - 151.101.0.0 - 151.101.3.255 customer offset
- 151.101.4.0/22 - unicast1 prefix
- …
- 151.101.64.0/22 - http2 anycast
- 151.101.128.0/22 - http3 anycast
- 151.101.192.0/22 - http4 anycast

Anatomy - conclusions

So…

These prefixes are spaced so that fat-fingering or targeting one, likely won't wipe out the others.

So we can reasonably conclude that regardless of how the leaked that they were specifically targeted.

Non-malicious theory would be traffic scrubbing or shaping service that injects more specific routes internally and that they have sufficiently poor filtering that they leaked to peers.

Non-Global Visibility

We didn’t see this leak via any transit providers.

We didn’t see it from bgpmon

We did see it from internal monitors in the cloud providers that accepted it.

We don’t really know how many other providers accepted it.

The amount of visible impact is not sufficient to intuit for traffic loss from other ISPs.

132116 has a limited number of visible peers.

Observations about Prevention

This would have been prevented by origin validation.

> We don’t sign our prefixes

It would also have been prevented by a filter based on 132116’s IRR object.

Lack of visibility is a challenge

The fact that no major transit providers apparently carried the prefix is nice, (great even), but points to that not being necessary for significant impact.