Invisible Hijacking

A case study of hijacking millions of IP address invisibly

About Outside Heaven

- We started in 2008
- We rent/manage infrastructures across the globe
- We manage VPN/proxy software solutions

- www.OutsideHeaven.com

What happened

- Spamcop reports started on 21h Jan 2016 for our range about /13 in size
- Average 2-3 reports per day
- From same reporter, and all from Yahoo mail

What we did

- Step 1: Make sure no mail service in the range
- Step 2: Block all mail port
- No affect on the spam cop reporting, reports are still keep coming on the regular bases.

Then…

- We re-announced the range into a different data centre, to a totally different set of server.
- Still..the spam cop reports keep coming

How’s this even possible

- We thought our IP was hijacked, but we checked globe routing history, no unknown announcement.
- Is there a bad guy in our upstream? talked to MTN network team, seems unless whole MTN are bad guy, it is very unlikely.

So…

- We called yahoo, the guy in yahoo showed us this:
- X.X.X.X/18
- But our announcement looks like this:
- X.X.X.X/12
- X.X.X.X/16

How?

- Yahoo receive this /18 announcement from direct peering in DE-CIX of a dead AS(not being seen in globe routing table from 2010)

- It looks like this

- X.X.X.X/16 10310 XXXXX(our AS)

- X.X.X.X/18 10310 17445(hijacked AS) 16637(MTN)

Upstream bad guy?

- Maybe , We bought our service though Afrihost—a secondary reseller of MTN network, although very unlikely, could be someone provided information about our range.
- But technically , no, AS17445 was dead on the internet since 2010.
- MTN are not peering with them

Who is AS17445

- A none-exist Chinese company
- Use Hijacked range
- Use hijacked AS and undelegated AS(one of their AS was from Afrinic free pool)

DE-CIX customer?

- Bought though reseller
- Changed AS number after becoming customer

In Summary

- Become exchange customer
- Direct peering with free mail provider
- announce hijacked range in more specific announcement thought direct peering
- Reaching 90% mail box without being seen in the globe routing table

Prevention?

- Difficult, very in today’s internet
- Difficult to find out due to invisibility in the globe routing table.
- Difficult for large org paying attention to small amount of spam cop reports.
- Difficult for exchange to identify bad customer like this
- Difficult in the peering part as well

How we find out

- We are very sensitive of spamcop/abuse report.
- We pay attention into even very unlikely report.

How we fixed this

- Mostly, social connection to Yahoo and DE-CIX guys.
- So attend meetings:)

The Future

- DECIX promise to check customer’s AS after they changed it in the future.
- Solutions like RPKI would solve this specific problem but of course open to wider debate of the solution.

Questions&Discussion

Lu Heng
h.lu@outsideheaven.com
Outside Heaven