Invisible Hijacking Follow up

A case study of hijacking millions of IP address invisibly

Lu Heng
h.lu@outsideheaven.com
Outside Heaven

Outside Heaven

- We started in 2008
- We rent/manage infrastructures across the globe
- We manage VPN/proxy software solutions
- www.OutsideHeaven.com larus.world for software solutions:)

What happened

- Someone 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

Questions and Issue raised during private discussion after my lighting talk

Let’s talk about them first

Whois database-Afrinic

- as-block: AS36864 - AS37887
- descr: *** ASN Block ***
- remarks:
- remarks: These AS numbers are assigned by AfriNIC
- remarks: to Network Operators in Africa and the
- remarks: Indian Ocean Regions.
- remarks:
- remarks: More information:
- remarks: http://www.iana.org/assignments/as-numbers
- remarks:
- org: ORG-AFNC1-AFRINIC
- admin-c: TEAM-AFRINIC
- tech-c: TEAM-AFRINIC
- mnt-by: AFRINIC-DB-MNT

Whois DB RIPE

- aut-num: AS37268
- as-name: DYNALTD
- admin-c: RM17728-RIPE
- tech-c: RM17728-RIPE
- descr: DynaNetworks LTD
- remarks: For information on "status:" attribute read https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources
- status: OTHER
- mnt-by: MNT-DYNANETWORKSLTD
- import-via: AS6777 from AS15169 accept ANY
- import-via: AS6777 from AS8075 accept ANY
- export-via: AS6777 to AS15169 announce AS37268
- export-via: AS6777 to AS8075 announce AS37268
- created: 2013-09-18T09:13:16Z

Other DB(lacnic,apnic,arin)

- All return correct results(undelegated Afrinic AS)
- Same goes for AS17445, only RIPE DB has entry in which the other 4 DBs all shows it is undelegated.

- aut-num: as17445
- as-name: Afrox
- descr: afrox MIS
- admin-c: RM17864-RIPE
- tech-c: RM17864-RIPE
- remarks: For information on "status:" attribute read https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources
- status: OTHER
- mnt-by: MNT-AFROX
- created: 2015-12-10T19:33:26Z
- last-modified: 2016-01-07T11:52:01Z
- source: RIPE

User awareness

- unreachable websites for varies reason are common in our business.
- Changing IP for customer is also common practise.
- Report for single unreachable website will never reach network team due to the volume of reports we receive everyday.

Routing viewers

- Service like RIPE routing history does not see such announcement as yahoo does not share what they see.
- Essentially the only person who in fact seeing is the direct peerer of the hijacker.

Thank you Yahoo and DECIX

- Yahoo’s detailed report to DECIX was really helpful
- DECIX’s promote responds and active in contacting different parties are also really helped.
- Total over 100 Email exchanges between many people to solve this problem

Hijacker ARE NOT HIDING, THEY ARE RUNNING IT LIKE REAL BUSINESS!

Questions and Discussions

Lu Heng
H.Lu@outsideheaven.com
Outside Heaven