Pakistan Telecom Hijacks YouTube

Or how to SYN-flood DOS yourself while annoying everyone on on the planet

APRICOT Taipei 2008

Martin Brown, Renesys Corp
Earl Zmijewski, Renesys Corp

Overview of 24 February 2008 Hijack

- YouTube announces only 5 small prefixes:
  - A /19, /20, /22, and two /24s
  - The /22 is 208.65.152.0/22
- Pakistan's government decides to block YouTube
- Pakistan Telecom ends up announcing a more specific (208.65.153.0/24) of YouTube's /22
- Most of the Internet goes to Pakistan for YouTube and gets nothing!
- YouTube ends up announcing both the /24 and the two more specific /25s
- PCCW turns off Pakistan Telecom

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Timeline UTC – 24 February 2008

18:47:00	YouTube globally reachable
18:47:45	first evidence of hijacked route propagating in Asia, AS path 3491 17557
18:48:00	several big trans-Pacific providers carrying hijacked route (9 ASNs)
18:48:30	several DFZ providers now carrying the bad route (and 47 ASNs)
18:49:00	most of the DFZ now carrying the bad route (and 93 ASNs)
18:49:30	all providers who will carry the hijacked route have it (total 97 ASNs)

Over one hour later …

20:07:25	YouTube, AS 36561, advertises the /24 that has been hijacked to its providers
20:07:30	several DFZ providers stop carrying the bad route
20:08:00	many downstream providers also drop the bad route
20:08:30	about 40 providers have dropped the hijacked route
20:18:43	YouTube announces two more specific /25 routes
20:19:37	25 more providers now prefer the /25s from 36561
20:50:59	Evidence of prepending: AS path 3491 17557 17557
20:59:39	PCCW disconnects Pakistan Telecom
21:00:00	the world rejoices

We've been here before, but on a larger scale …

Apr 1997	AS 7007
Dec 2005	TTNet (AS 9121)
Jan 2006	Con Edison (AS 27506)

Each of these providers announced parts of the Internet not under their control, resulting in bedlam.

Solutions?

- Replace BGP (go ahead, I'll wait)
  - Pretty Good BGP
  - Secure Origin BGP
  - SBGP
- Filter announcements from your customers
  - Manually
  - Automatically via a RPSL database
- Monitor networks you care about
  - Internet Alert Registry
  - Prefix Hijack Alert System
  - RIPE's MyASN
  - Renesys' Routing Intelligence

Memorable Quotes

- Full technical details published 24 February at www.renesys.com/blog

• "We are not hackers. Why would we do that?" Shahzada Alam Malik, head of the Pakistan Telecommunication Authority, told Associated Press Television News. YouTube's wider problems were likely caused by a "malfunction" elsewhere, he said. — International Herald Tribune, 27 February 2008

• Attempts to log on to the Google-owned site typically timed out. Keynote is unable to uncover the causes of an outage, said Shawn White, Keynote's director of operations, but he added that he would be shocked if one country had the ability to bring down YouTube globally. — CNET, 24 February 2008

Thank You

Martin Brown mabrown@renesys.com
Earl Zmijewski earl@renesys.com