

The Day the YouTube Died

What happened and what we might do about it

MENOG 3, Kuwait
April 2008

Martin Brown, Renesys Corp
Todd Underwood, 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 announces 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** ~ 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 TTNNet (AS 9121)

Jan 2006 Con Edison (AS 27506)

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

But do hijacks really occur with any regularity?

Examine two US government networks and their more specifics

US owns but does not announce 7.0.0.0/8, 11.0.0.0/8 and others. These networks are “free for the taking” without any impact.

A Sampling of Hijacks				
<u>Prefix</u>	<u>Date(s)</u>	<u>Origination (AS)</u>	<u>Avg Time per Peer (Mins)</u>	<u>Max Peers</u>
7.7.7.0/24	7 March 2008	Posdata Co. Ltd. (AS 18305)	16.4	227
7.7.7.0/24	28 Nov 2007	Bell Canada (AS 577)	4.4	206
7.7.7.0/24	Jan – Sept 2007	Sprint (AS 1239)	months	194
7.0.0.0/8	7 May 2007	Teknoas (AS 42075)	13.7	119
11.1.1.0/24	5 Mar 2008 - ongoing	Helios Net (AS 21240)	weeks	248
11.11.11.0/24	5 Jan 2008	Hutchinson (AS 9304)	69.0	207
11.0.0.0/24	20 Oct 2007	Global Crossing (AS 3549)	28.3	208

Every announcement in this assigned, but unused, space is a hijack.

Solutions?

- Replace BGP (go ahead, I'll wait)
 - Secure Origin BGP
 - SBGP
 - Pretty Good BGP
- 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's Routing Intelligence

Solutions?

- Announce all the /24's
 - Reduce scope of damage
 - Exploding routing tables
 - We currently see 19 globally routed /8s
→ 1,245,184 /24s!
 - Entire routing table would be on the order of
10 million /24s

Downsides/Problems

- Replace BGP — Obvious
 - Limited value unless everyone does it
 - exception Pretty Good BGP
 - Router hardware performance
 - Router support
 - Management
 - Cost

Downsides/Problems

- Filter all routes from customers
 - Good idea, but only mostly helps everyone else
 - Well, reduces likelihood that your customer will hijack Youtube and you'll have to clean up the mess
- Filter all routes from peers
 - Great idea, but
 - Hard to build filter lists that are accurate for big peers
 - Hard to implement really large lists on current generation routers

Downsides/Problems

- Monitor networks you care about
 - Increases Costs: procedures, set up monitoring, handle false positives (Balance against value to reduced downtime)
 - Big question: if **your** customer experienced a hijack, what would your NOC do to help them?
 - Most ASNs are insufficiently connected to the global routing and security community to get prompt action if they **do** take an alert
 - This is solvable. By you.

Downsides/Problems

- Announce all /24s
 - Beside the obvious death and destruction of routers everywhere....
 - Arms race that's already being lost
 - Renesys already sees 12.5% of /25s being “globally routed” (203 of them – see NANOG 41)
 - Even if you “win” you still just limit the damage, and not as much as you hope.

Best current known solution

- Filter your customers (because you should)
- Monitor prefixes you care about
 - Maintain alerts
 - Establish procedures for handling a hijack quickly
- Build contacts within your peers and service providers to get quick responses to bad paths

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
Todd Underwood todd@renesys.com
Earl Zmijewski earl@renesys.com