Università degli Studi di Roma Tre
Dipartimento di Informatica e Automazione
Via della Vasca Navale, 79 – 00146 Roma, Italy

YouTube Hijacking (February 24th 2008) Analysis of BGP Routing Dynamics

A. Antony[1], D. Karrenberg[1], R. Kisteleki[1], T. Refice[2], R. Wilhelm[1]

RT-DIA-123-2008 **February 2008**

(1) Science Group,
RIPE NCC,
Amsterdam, The Netherlands.
{antony,dfk,robert,wilhelm}@ripe.net
(2) Dipartimento di Informatica e Automazione,
Università di Roma Tre,
Rome, Italy.
refice@dia.uniroma3.it

Work partially supported by RIPE NCC (Amsterdam, The Netherlands).

ABSTRACT

On Sunday, 24 February 2008, *Pakistan Telecom* (*AS17557*) started an unauthorized announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, *PCCW Global* (*AS3491*) forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale.

In this report we show how this event was observed by about 300 vantage points (also called *collector peers*) spread over the Internet by the *Routing Information Service* (*RIS*) [5] of *RIPE NCC* [4] and, in general, how to obtain hard data on network events using public available tools developed by the RIS and by the *Compunet Research Group* of *Rome Tre University* [3] .

This document contains information also published as RIPE NCC's document at [6].

1 Event Timeline

Before, during and after Sunday, 24 February 2008 AS36561 (YouTube) announces 208.65.152.0/22. Note that AS36561 also announces other prefixes, but they are not involved in the event.

Sunday, 24 February 2008, 18:47 (UTC) AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.

Sunday, 24 February 2008, 20:07 (UTC) AS36561 (YouTube) starts announcing 208.65.153.0/24. With two identical prefixes in the routing system, BGP policy rules, such as preferring the shortest AS path, determine which route is chosen. This means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.

Sunday, 24 February 2008, 20:18 (UTC) AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.

Sunday, 24 February 2008, 20:51 (UTC) All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen prepended by another 17557. The longer AS path means that more routers prefer the announcement originated by YouTube.

Sunday, 24 February 2008, 21:01 (UTC) AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24. Note that AS17557 was not completely disconnected by AS3491. Prefixes originated by other Pakistani ASes were still announced by AS17557 through AS3491.

2 Event Analysis

We now show how we analyzed the data collected by RIS's collector peers, to understand the hijacking event, using some public available tools developed by the RIS and by the Compunet Research Group of Rome Tre University.

Pakistan aimed to block the YouTube's web site (youtube.com). youtube.com appears in the DNS with three distinct IP addresses: 208.65.153.238, 208.65.153.251 and 208.65.153.253.

First, to find the prefixes originated by YouTube, we searched the routing table dumps of the various RIS's collector peers, by querying the *RISwhois*. This tool (accessible via whois protocol on [9] or through the web interface at [8]) provides a quick look at the most recent set of collector peers' routing tables. Once the hijacking was almost over, RISwhois showed YouTube originating 208.65.152.0/22, 208.65.153.0/24 and 208.65.153.128/25. The /22 was the most widely seen prefixes (by 112 RIS's collector peers). The /24 was observed by 105 peers. The /25 announcement, on the other hand, only reached 21 peers.

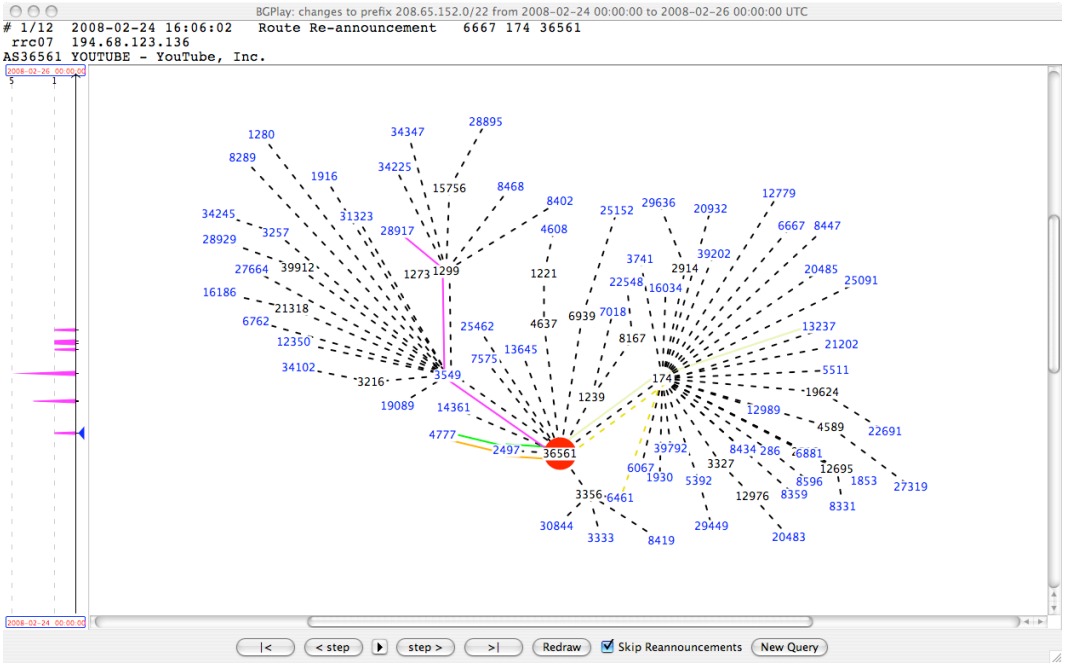
Then, to have a more detailed view of the event, we looked at the BGP messages propagated through the Internet when the event occurred, using the *RIS search* tool [7]. Searching for the period Sunday, 24 February 2008, 18:00 (UTC) to Monday, 25 February 2008, 01:00 (UTC), both AS17557 (Pakistan Telecom) and AS36561 (YouTube) resulted as origin of the /24 prefix.

Finally, to understand the dynamics of the route announcements, withdrawals and the "competition" in BGP between the Pakistani /24 and YouTube announcement, we used the visualization tools *BGPlay* [2] and *BGPath* [1]. These tools were designed and deployed by the Computer Networks Research Group and the former has been integrated into the RIS service portfolio. Next sections show BGPlay and BGPath snapshots illustrating the state of the network at some key points in time.

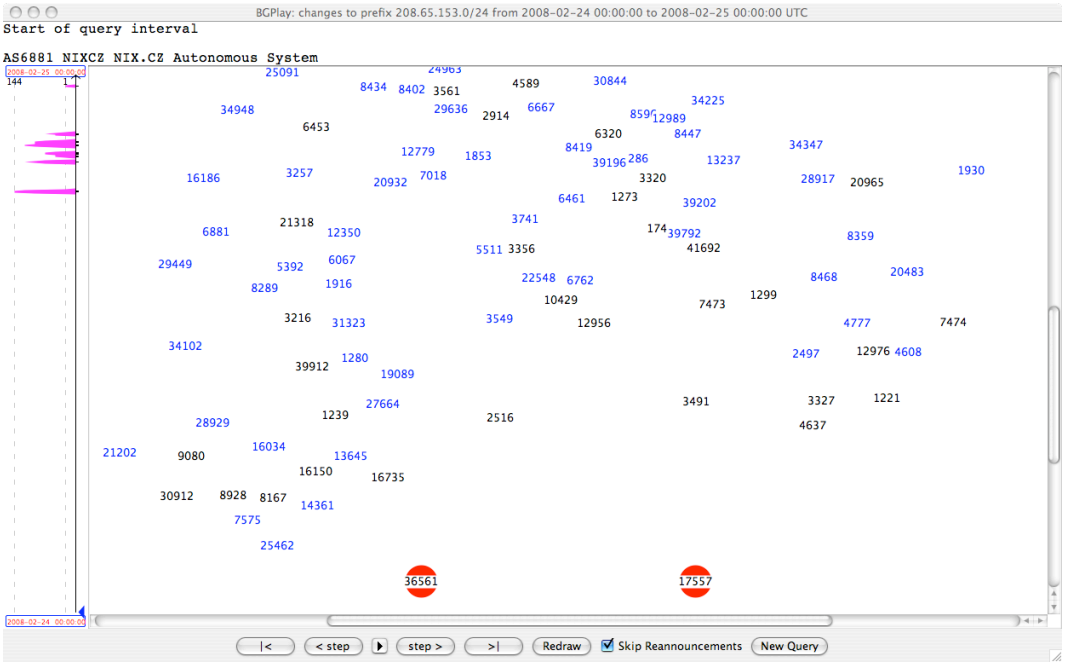
It is important to note that all these tools can only show the BGP data collected by RIS's collector peers and not routing, as such, for the whole Internet. Based on this information, it is not possible to make statements about how many sites had their traffic to YouTube hijacked.

3 Routing States - BGPlay Snapshots

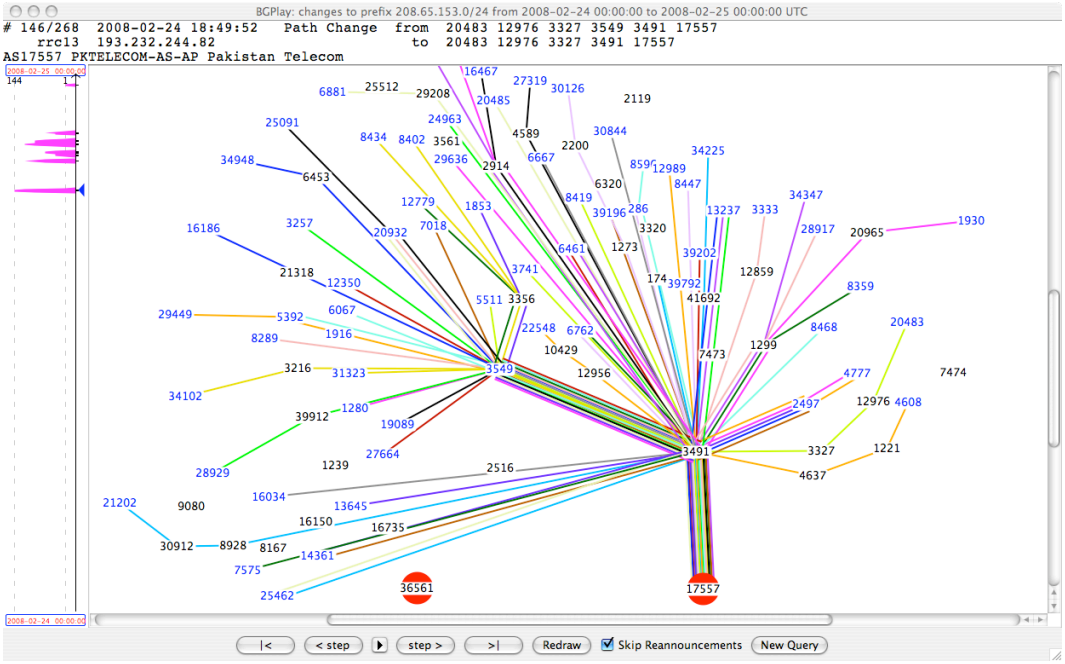
Before, during and after Sunday, 24 February 2008 AS36561 (YouTube) announces 208.65.152.0/22. Note that its connectivity almost doesn't change during the period of the hijacking.



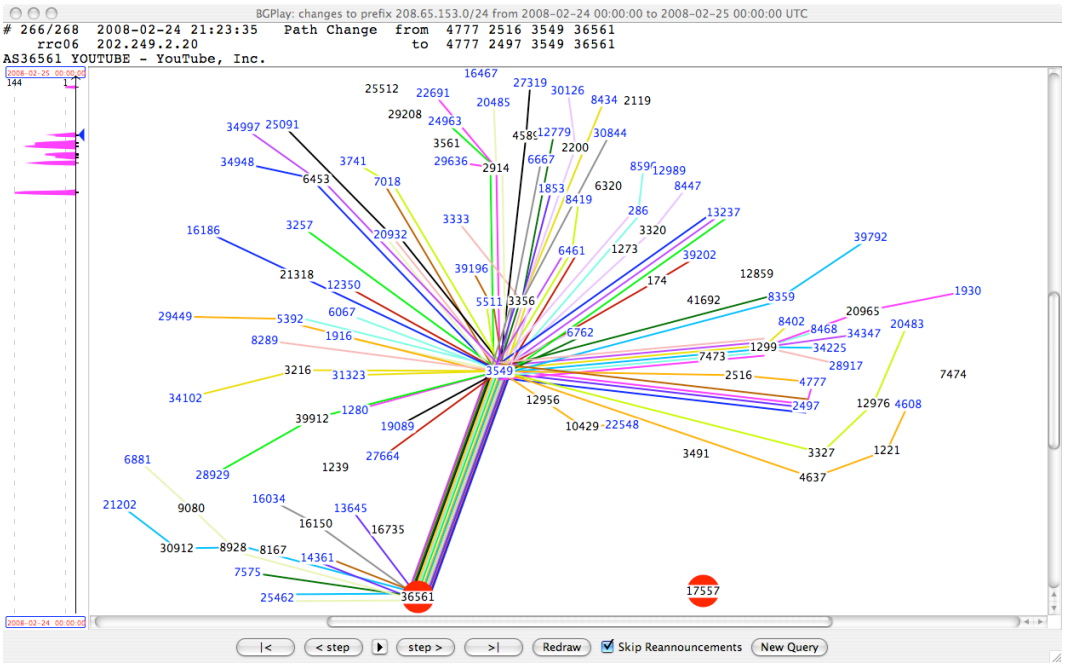
The prefix 208.65.153.0/24 is not announced on the Internet before the event.



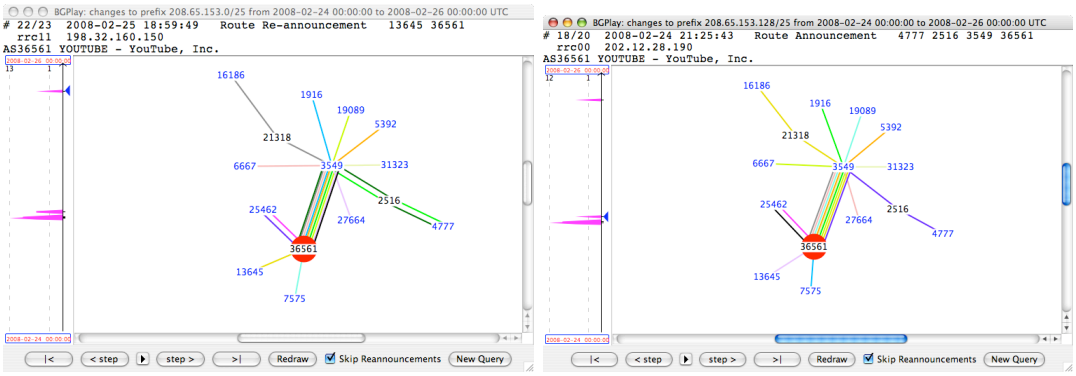
Sunday, 24 February 2008, 18:49 (UTC) AS17557 (Pakistan Telecom) has been announcing 208.65.153.0/24 for the past 2 minutes. The RIS's collector peers around the world have received the route update. The YouTube traffic is being redirected to Pakistan.



Sunday, 24 February 2008, 21:23 (UTC) AS36561 (YouTube) has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to YouTube's AS36561.



Since Sunday, 24 February 2008, 20:18 (UTC) AS36561 (YouTube) are announcing 208.65.153.0/25 and 208.65.153.128/25. Note that both of these prefixes are much less visible on the Internet than the /24 prefix.



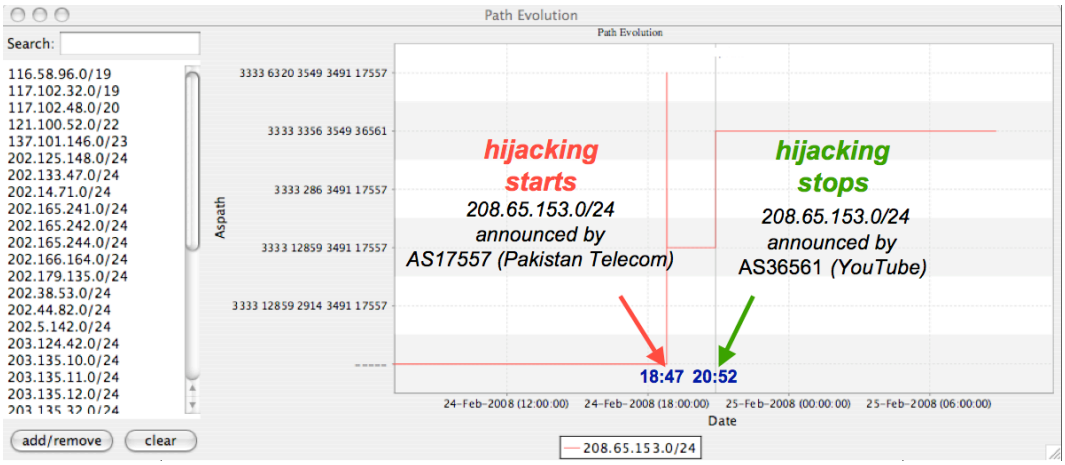
4 Path evolution of the hijacked prefix as observed by a RIS peer - BGPath screenshots

In order to have a complete view of the routing changes that the hijacked prefix (208.65.153.0/24) underwent over the course of the hijacking, we looked at the path evolution over time of the hijacked prefix. Figure 4 shows the evolution of the path chosen by a specific peer (in this case AS3333, RIPE NCC) to reach the hijacked prefix. Namely, Figure 4 shows that:

Until Sunday, 24 February 2008, 18:47 (UTC) AS3333 (RIPE NCC) had no path toward 208.65.153.0/24.

On Sunday, 24 February 2008, from 18:47 to 20:52 (UTC) AS3333 (RIPE NCC) observed 208.65.153.0/24 being announced by AS17557 (Pakistan Telecom) through two distinct paths (3333 6320 3549 3491 17557 and 3333 12859 3491 17557).

Since Sunday, 24 February 2008, 20:52 (UTC) AS3333 (RIPE NCC) has observed 208.65.153.0/24 being announced by AS36561 (YouTube) through the path 3333 3356 3549 36561.



References

[1] BGPath. http://nero.dia.uniroma3.it/rca/.

[2] BGPlay. http://www.ris.ripe.net/bgplay/.

[3] ROMA TRE Compunet Research Group. http://www.dia.uniroma3.it/~compunet/.

[4] RIPE NCC. http://www.ripe.net.

[5] Routing Information Service. http://www.ripe.net/ris/.

[6] YouTube Hijacking: A RIPE NCC RIS case study. http://www.ripe.net/news/study-youtube-hijacking.html.

[7] RIS search page. http://www.ris.ripe.net/perl-risapp/risearch.html.

[8] RIS whois Web Interface. http://www.ris.ripe.net/cgi-bin/riswhois.cgi.

[9] RIS whois. http://riswhois.ripe.net.