YouTube Hijacking: A RIPE NCC RIS case study

17 Mar 2008 • news RIS internet governance

Introduction

On Sunday, 24 February 2008, Pakistan Telecom (AS17557) started an unauthorised 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 the events were seen by RIPE NCC's Routing Information Service (RIS) and how, in general, one can use the RIS tools to obtain hard data on network events.

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

- **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 ASs were still announced by AS17557 through AS3491.

Event Analysis

The prefixes involved in the hijack and YouTube's counter measures were already known from reports on various mailing lists. However, even if this information had not been reported, it is easy to find in the RIPE NCC's Routing Information Service (RIS).

Pakistan aimed to block the YouTube website. youtube.com has three IP numbers in the DNS: 208.65.153.238, 208.65.153.251 and 208.65.153.253.

The RISwhois tool (accessible via whois protocol on riswhois.ripe.net or through the web interface at http://www.ris.ripe.net/cgi-bin/riswhois.cgi) provides a quick look at the most recent set of Routing Information Base (RIB) dumps from the various RIS Remote Route Collectors (RRCs). By entering the IP address 208.65.153.238, we see YouTube (still) originating 208.65.152.0/22, 208.65.153.0/24 and 208.65.153.128/25. The /22 is the one that is most widely seen (by 112 RIS peers). The /24 is seen by 105 peers. The /25 announcement, however, only makes it to 21 of the peers.

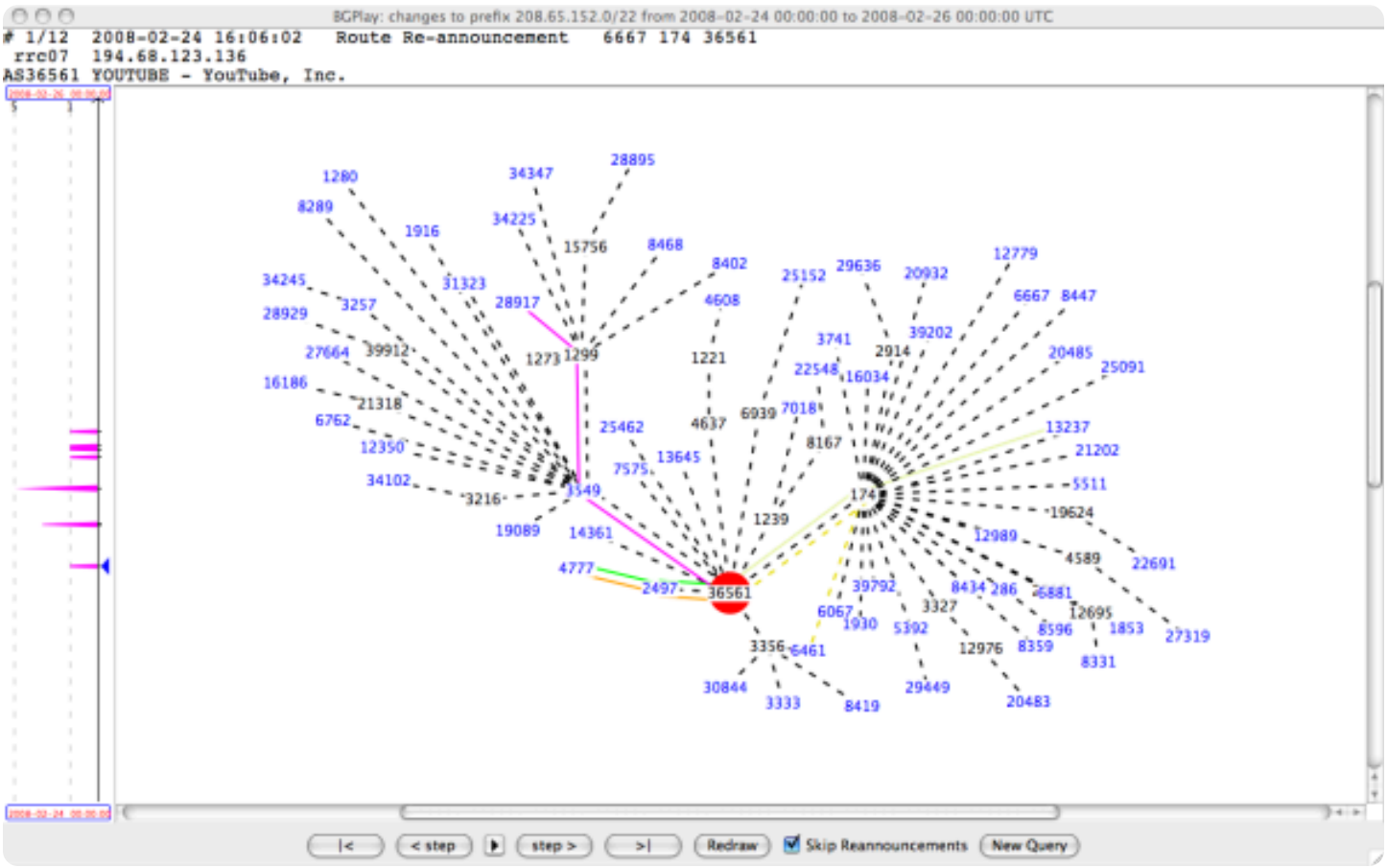
When a routing event is still fresh, it's likely that the associated prefix announcement hasn't yet been included in an RIS RIB dump. In that case, the main RIS search page, http://www.ris.ripe.net/perl-risapp/risearch.html , can be useful. Looking up a youtube.com IP address using the "Less specific" option for the period Sunday, 24 February 2008, 18:00 (UTC) to Monday, 25 February 2008, 01:00 (UTC), shows both AS17557 (Pakistan Telecom) and AS36561 (YouTube) as origin. Folding out the tabs, we see the prefixes involved, as well as an overview of the update/withdrawal events. This shows the last unauthorised announcement from Pakistan was received on Sunday, 24 February 2008, 21:01:22 (UTC).

To understand the dynamics of the route announcements, withdrawals and the "competition" in BGP between the Pakistani /24 and YouTube announcement, we can use the visualisation tool BGPlay . This tool was designed and written by the Computer Networks Research Group at Roma Tre University and has been integrated into the RIS service portfolio. BGPlay snapshots illustrating the state of the network at some key points in time are subject of the next section.

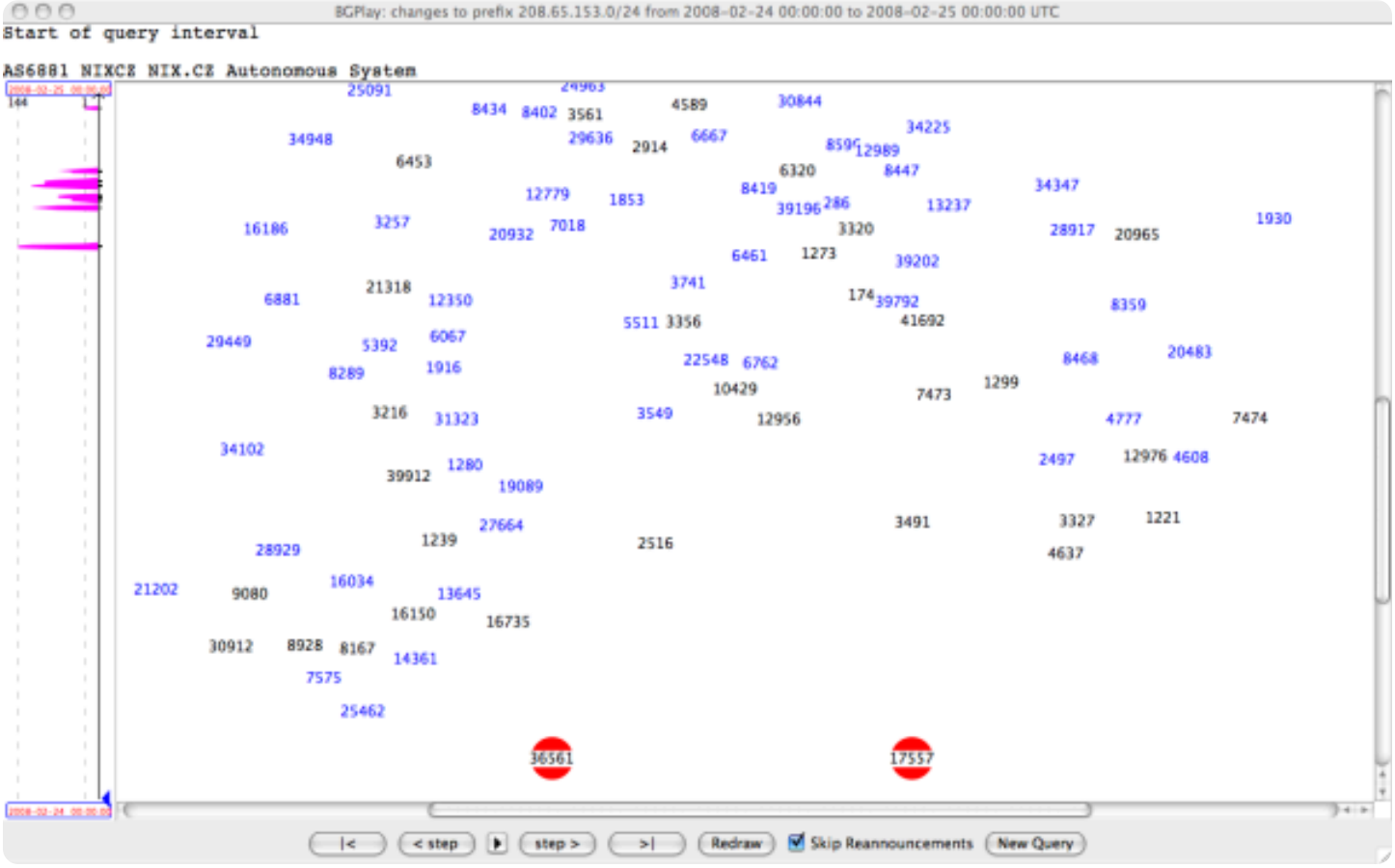
It is important to note that the RIS can only show the collected BGP information and not routing, as such, for the whole Internet. Based on this information, it is not possible to make statements about how many sites had their traffic to YouTube hijacked. The data in RISwhois

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.

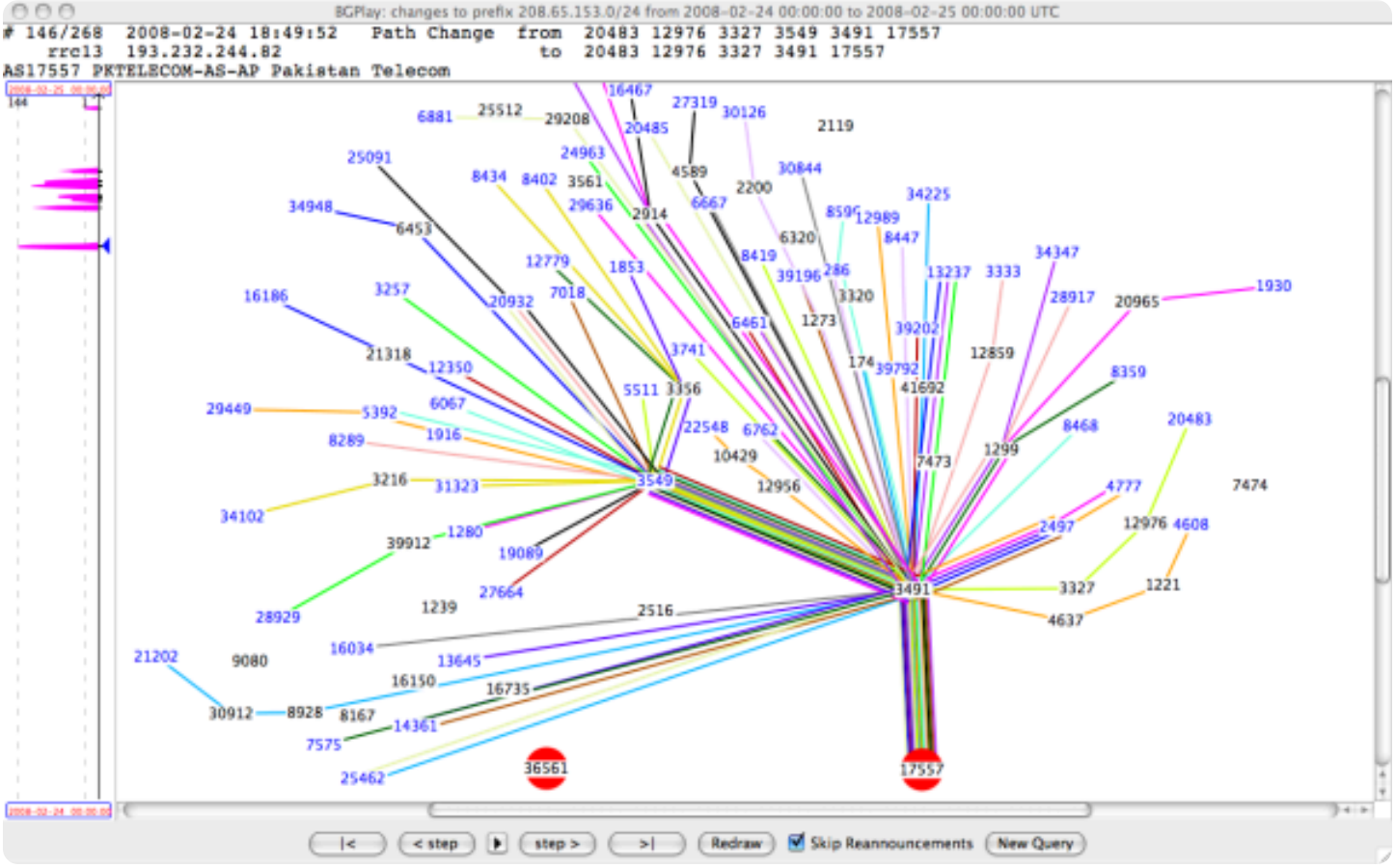


The prefix 208.65.153.0/24 is not announced on the Internet before the event:



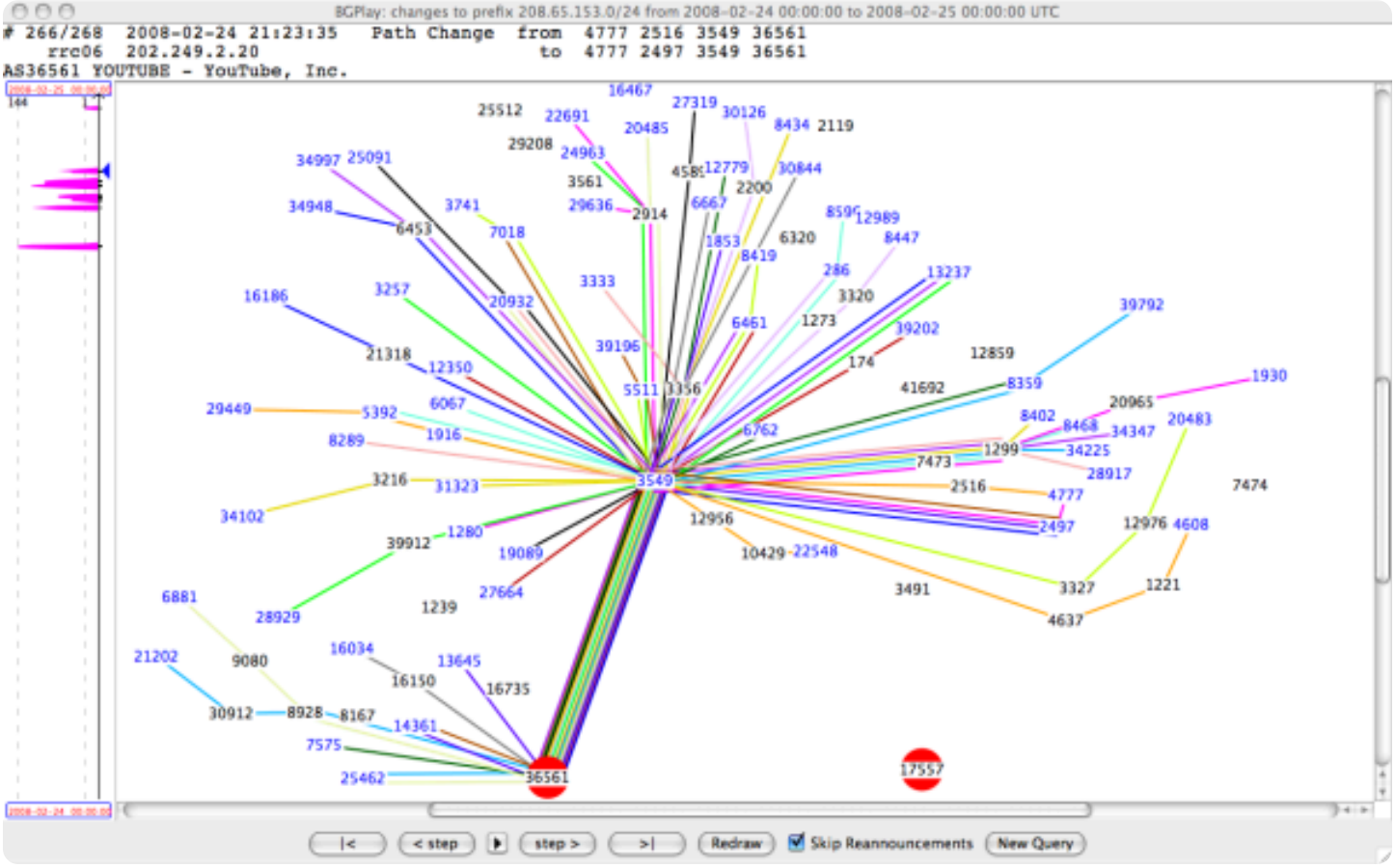
Sunday, 24 February 2008, 18:49 (UTC)

AS17557 (Pakistan Telecom) has been announcing 208.65.153.0/24 for the past two minutes. RIS peers around the world have received the route update, and YouTube traffic is being redirected to Pakistan.



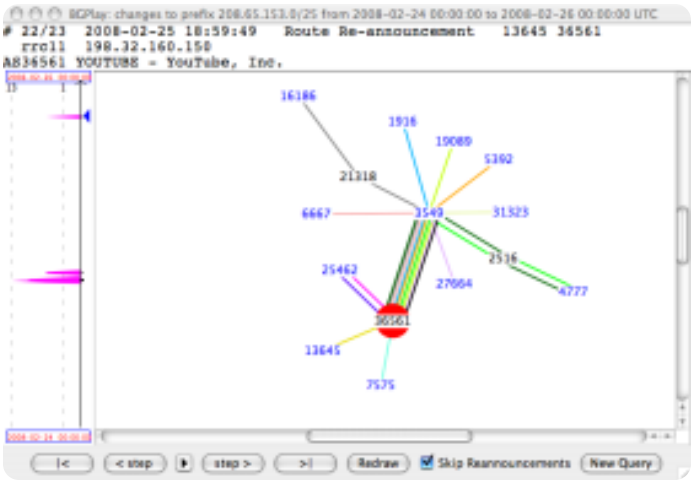
Sunday, 24 February 2008, 21:23 (UTC)

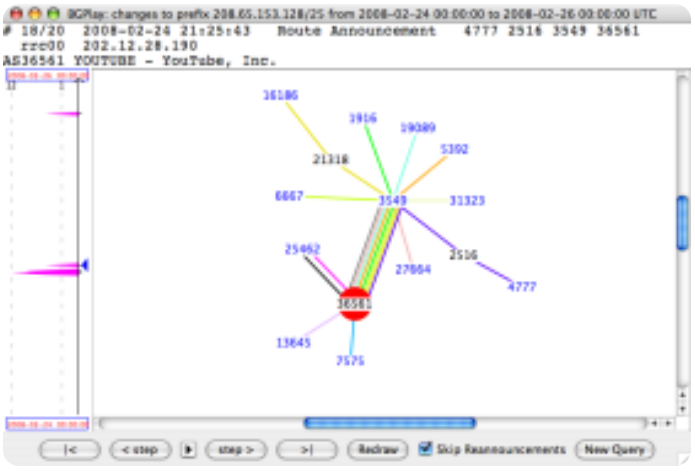
AS36561 (YouTube) has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to YouTube's AS36561



Since Sunday, 24 February 2008, 20:18 (UTC)

AS36561 (YouTube) is 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.

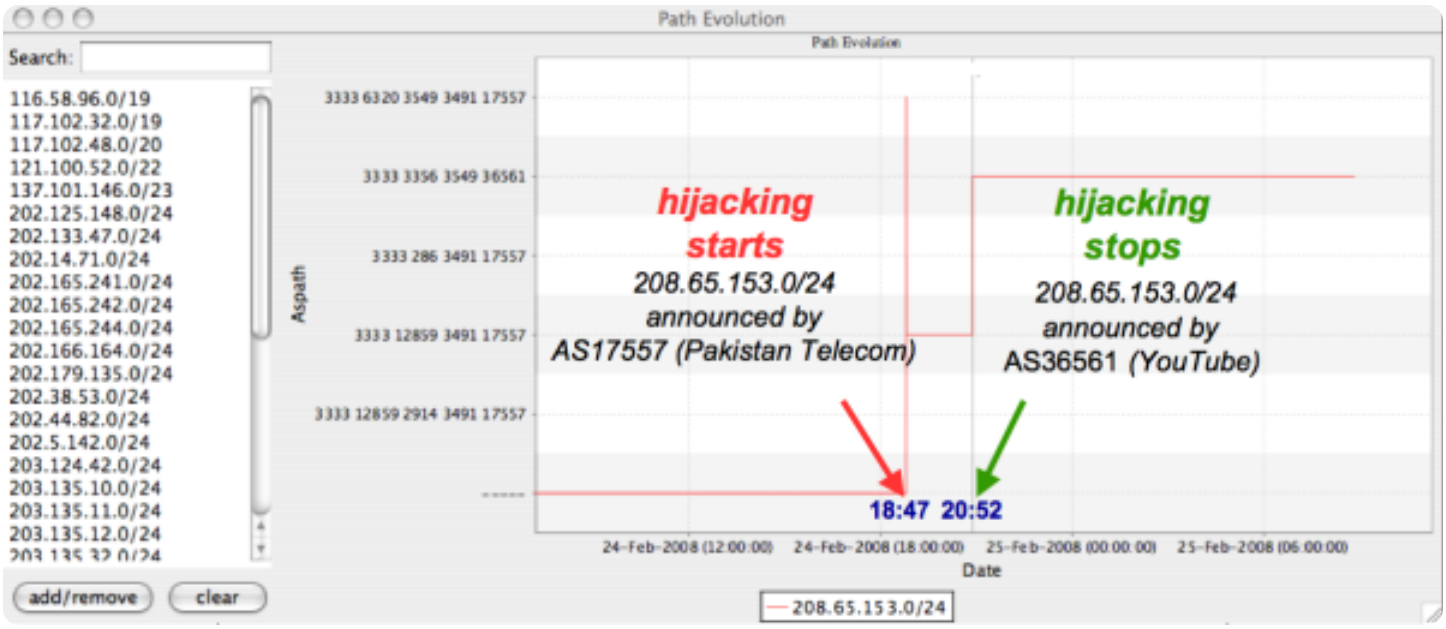




tool from Roma Tre University. The following picture shows the evolution of the path chosen by a specific peer (in this case AS3333, RIPE NCC) to reach the hijacked prefix.

This picture 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



Summary

As the above timeline shows, this event happened in a relatively short time interval: YouTube reacted about 80 minutes after the Pakistan Telecom announcements, and all the major events finished after about two hours. While this report showed that the tools provided by RIPE NCC (such as RISwhois and BGPlay) can help in following and analysing events even on such a short timeline, we also note that unauthorised announcements like this can be prevented from spreading throughout the Internet by appropriate routing configuration by operators of Autonomous Systems. The RIPE NCC provides the RIPE Routing Registry in order to facilitate

RIPE

- Working Groups
- Task Forces
- RIPE Governance
- Initiatives
- RIPE 93
- How to Participate

RIPE NCC

IPs & ASNs

- IPv4
- IPv6
- AS Numbers
- RIPE Database
- LIR Portal
- DNS
- Resource Transfers and Mergers
- Legacy Internet Resources
- Documentation for Resource Management

Analyse

- Statistics
- Internet Measurements
- DNS
- Raw Datasets
- Archived Projects
- Sponsorship

Community

- Working Groups
- Task Forces
- Policy Development
- Internet Governance
- RIPE Labs
- NRO NC
- Initiatives
- RIPE Governance
- RIPE Document Store
- Participate

Membership

- RIPE NCC Membership
- General Meetings
- Billing, Payment and Fees
- RIPE NCC Organisational Documents
- Join a Discussion
- RIPE NCC Forum

Events

RIPE Meetings
Regional Meetings
Roundtable Meetings
General Meetings
Open House
Internet Measurement Days
Hackathons
Events Calendar
Event Sponsorship

About

What We Do
Staff
Executive Board
Financial Information
Press Centre
Legal
News
Support
RIPE NCC Trust Portal
RIPE NCC Middle East

Training

In-Person Training Courses
Webinars
RIPE NCC Academy
Certified Professionals
Videos
Summer School 2026

Languages

English
Türkçe
Español
Italiano
Русский
عربي
فارسی
Українська
Français

Docs

RIPE Document Store
Documentation
IPv6 Information Centre

Your IP Address is: **76.159.199.214**