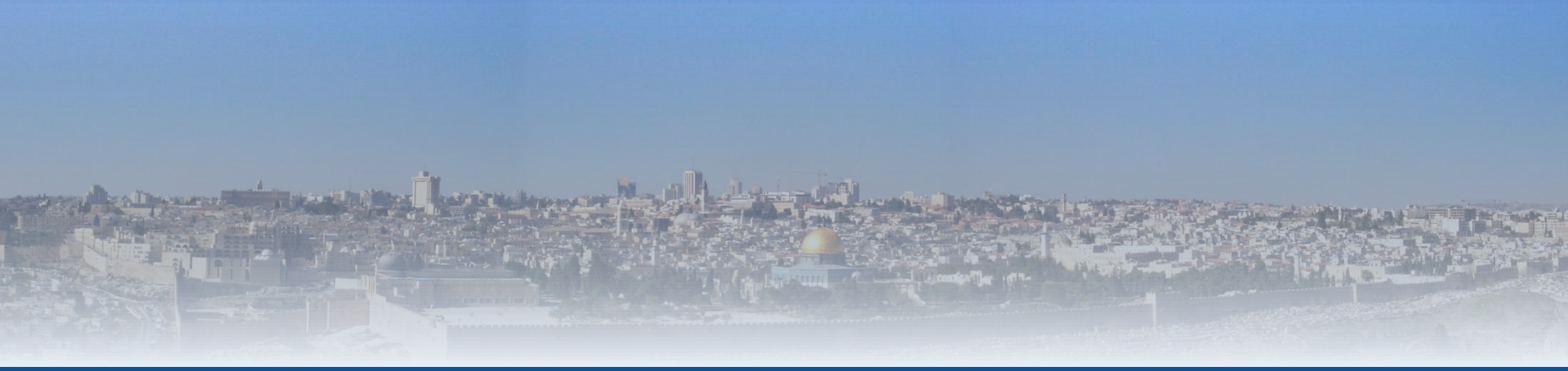


# Who/How to Blame for Attacks on the Internet Infrastructure?


Michael Schapira

School of Computer Science and Engineering

האוניברסיטה העברית בירושלים

THE HEBREW UNIVERSITY OF JERUSALEM

Hebrew University

# 3 stories, 1 theme

- The Internet infrastructure is alarmingly **insecure**
- The Internet's infrastructure was designed in the 80's without security in mind
- **Security not even on the horizon**

# 3 stories, 1 theme

- **Naming/addressing** with the Domain Name System (DNS)
  - DNS = the Internet's phone book
  - google.com = ?


- **Routing** with the Border Gateway Protocol (BGP)
  - BGP = the Internet's google maps / Waze

- The Network **Time** Protocol (NTP)
  - NTP = the Internet's global clock

# An Anecdote


Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via Belarus
START 1. Guadalajara, Mexico
2. Monterrey, Mexico
3. Laredo, TX
4. Ashburn, VA
5. Washington, D.C.
6. London, UK
7. Moscow, Russia
8. Minsk, Belarus
9. Frankfurt, Germany
10. New York, NY
11. Washington, D.C. END
Repeated attacks against major financial institutions and governments in Europe and the US
renesys
Source: Renesys Path Measurements

# Rare Incident? Not Really!

renesys

Products Solutio

Con-Ed Steals the

22 JAN, 2006 | 11:06 PM | BY

IT档案馆

¥111.43

¥258.00

¥145.00

The Telegraph

nt Culture Travel Li

fence Health Scotland

The Register®

ence Bootnotes C

TV: CNNUS CNNI

Home TV & Vide

Report: C

From

Noven

Traceroute

rene

ts

VIDEO

load No

nds according to

s their route.

MT) on April 2, with

about their routes

Pin it

eland

N D S S '15

S Y M P O S I U M

## Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks


Pierre-Antoine Vervier
Symantec Research Labs/Eurecom
Pierre-Antoine_Vervier@symantec.com

Olivier Thonnard
Symantec Research Labs
Olivier_Thonnard@symantec.com

Marc Dacier
Qatar Computing Research Institute
mdacier@qf.org.qa



***Abstract*—Some recent research presented evidence of blocks of IP addresses being stolen by BGP hijackers to launch spam campaigns [35]. This was the first time BGP hijacks were seen in the wild. Since then, only a very few anecdotal cases have been reported as if hackers were not interested in running these attacks. However, it is a common belief among network operators and ISPs that these attacks could be taking place but, so far, no one has produced evidence to back up that claim. In this paper, we analyse 18 months of data collected by an infrastructure specifically built to answer that question: are intentional stealthy BGP hijacks routinely taking place in the Internet? The identification of what we believe to be more than 2,000 malicious hijacks leads to a positive answer. The lack of ground truth is, of course, a problem but we managed to get confirmation of some of our findings thanks to an ISP unwittingly involved in hijack cases we have spotted. This paper aims at being an eye opener for the community by shedding some light on this undocumented threat. We also hope that it will spur new research to understand why these hijacks are taking place and how they can be mitigated. Depending on how BGP attacks are carried out, they can be very disruptive for the whole Internet and should be looked at very closely. As of today, as much as 20% of the whole IPv4 address space is currently allocated but not publicly announced, which makes it potentially vulnerable to such malicious BGP hijacks.**


[23], [29], [40], [50] which is still acceptable to these users since they are only interested in alerts related to the networks they own. Other proposals aim at preventing BGP hijacks [24], [25], [30] but their large-scale adoption and deployment are hindered by the implementation cost.

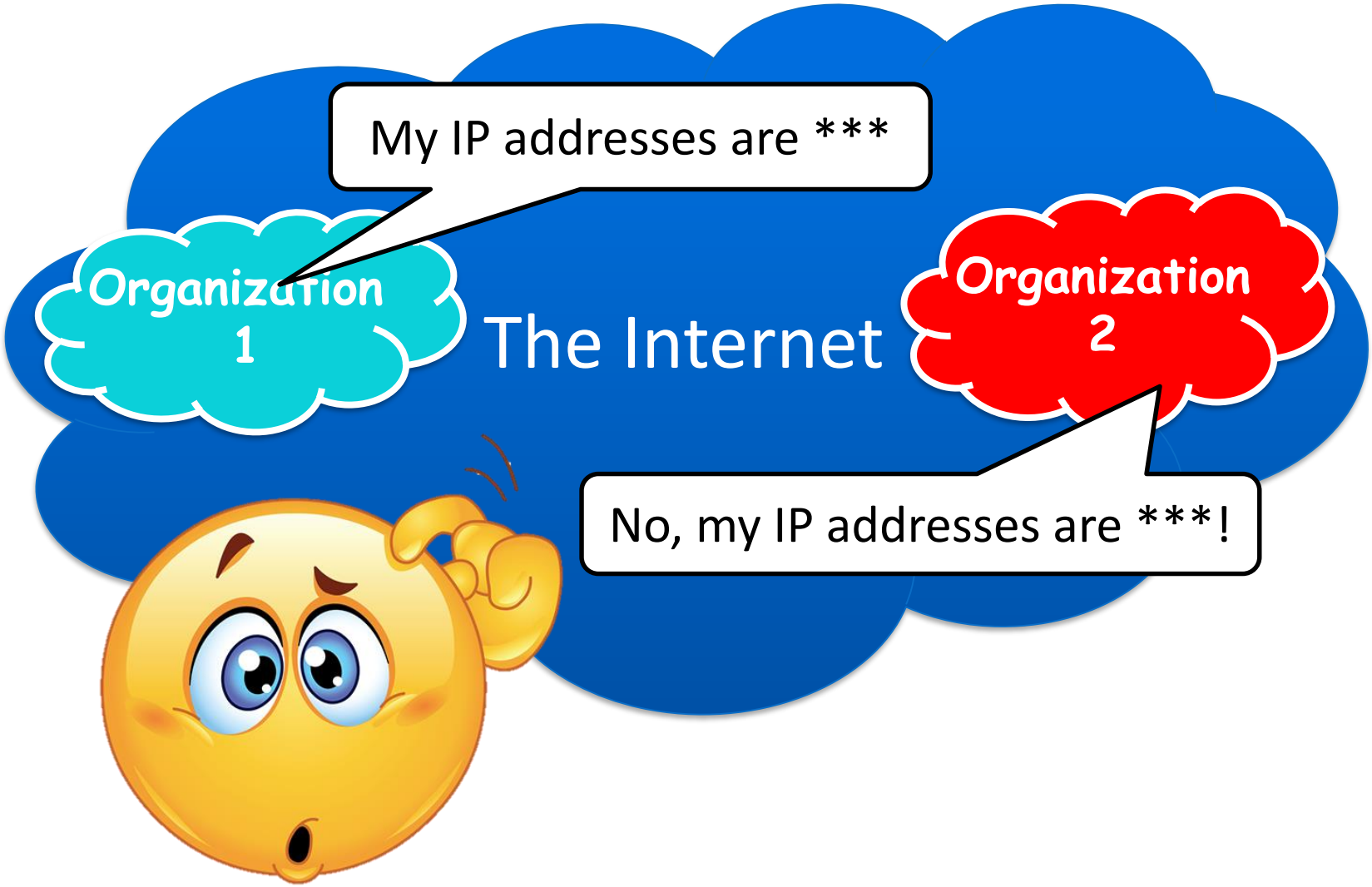
In 2006, Ramachandran et al. [35] introduced a new phenomenon called "BGP spectrum agility", which consists of spammers advertising for a short period of time (*i.e.*, less than one day) BGP routes to large (*i.e.*, /8) previously unannounced blocks of IP addresses and, subsequently, using the available IP addresses for spamming. Later, some other authors also identified the emission of spam emails coming from hijacked prefixes [20], [23]. Furthermore, complementing the work done in [39], we have described in [47] a special case of hijack in which a couple of IP address blocks were stolen and used to send spam. Most recently, we have also shown in [46], thanks to another real-world case, that correlating routing anomalies with malicious traffic, such as spam, is not sufficient to decisively prove the existence of a malicious BGP hijack.

Besides these sparse cases and despite the apparent desire of some owners to detect whether their own IP address block could ever be stolen, to the best of our knowledge we have no documented evidence that BGP attacks are a threat worth

# Why Do this?

- To **disconnect** victim from the Internet (large corporation, nation state, …)
- To be a **man-in-the-middle** (snoop on traffic, tamper with traffic, …)
- To **impersonate** the victim
- To **hide under someone else's identity**
- To **attack protocols/mechanisms that utilize Internet routing** (BitCoin, DNS, …)
- …

# Attack: Hijacking IP Addresses



# What's So Special About These Attacks?

- Devastating
  - Can bring down an organization/state
- Easy to launch
  - All you need is a BGP router
- Hard to detect in real time
  - often only detected (if at all) after the fact
- Plausible deniability
  - configuration errors are common!
  - market for compromised routers

# Did Russia Manipulate the US Presidential Elections?

President Vladimir V. Putin of Russia suggested on Thursday that **"patriotically minded" private Russian hackers could have been involved in cyberattacks … Hackers, he said, "are like artists"** who choose their targets depending how they feel "when they wake up in the morning."

(NY Times, June 2017)

# Some Questions

- Is attribution the real challenge?
- What is the nation state accountable for?
- What do nation states want?
  - Deliberate ambiguity? Nuclear capabilities as a useful analogue?
- How is Internet security achievable
  - Regulation? Incentives?

# Thank you