



Border Gateway Protocol: The Good, Bad, and Ugly of Internet Routing

Jim Cowie, Chief Scientist

@jimcowie / @DynResearch

Stanford EE Computer Systems Colloquium

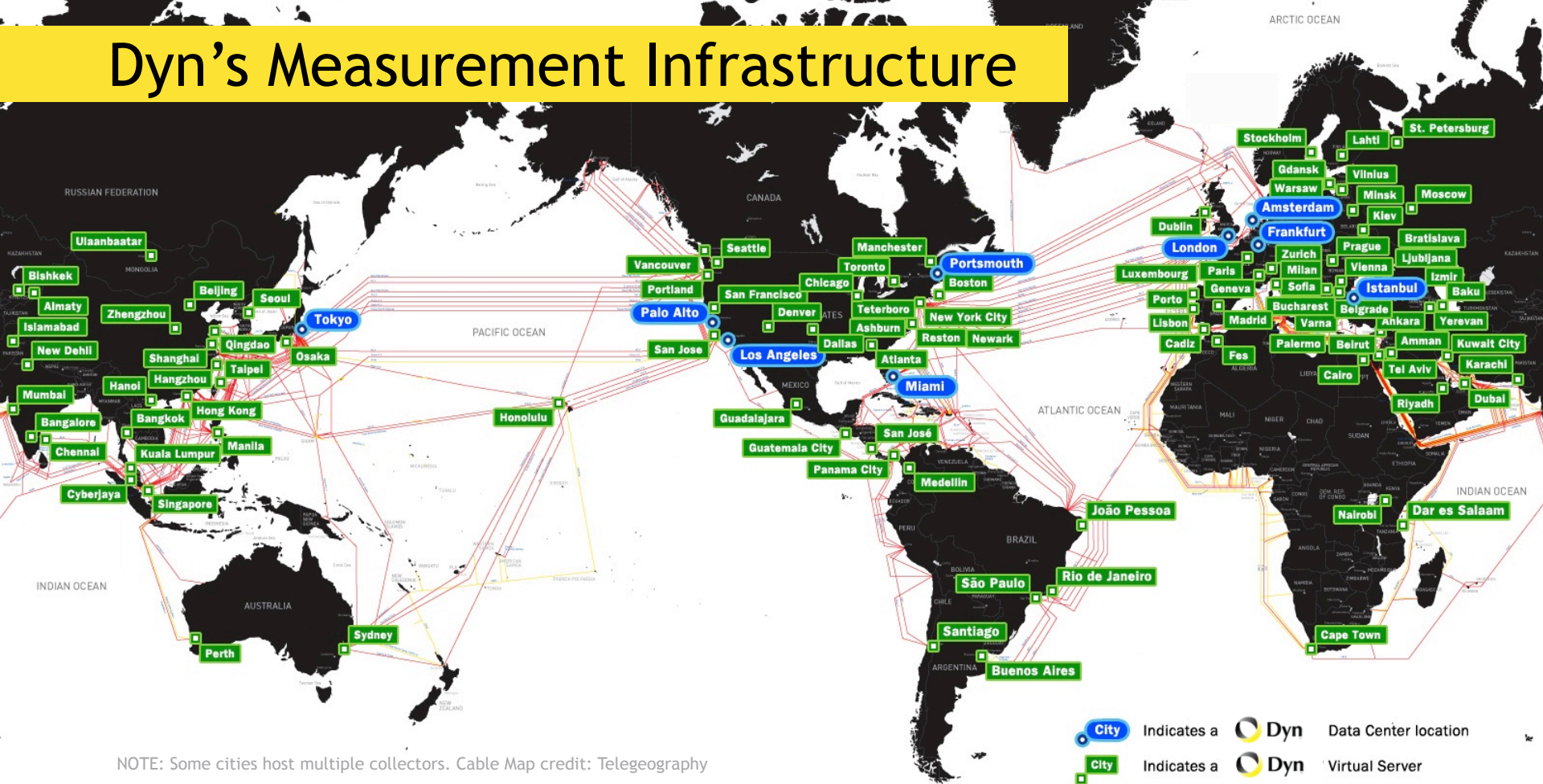
11 February 2015

On the menu today

- The Core Problem: Attribution and Belief on the Internet
- Border Gateway Protocol by example
- Things that Go Wrong
- We play a game: Spot the Evil
- Recent developments: Man in the Middle
- Attribution: No Silver Bullets
- Research Directions
- How You Can Help



Dyn's Measurement Infrastructure





Jim Cowie

Chief Scientist, Dyn Research

- High Performance Computing (1990s)
- Large integer factorization (RSA Challenges)
- High Performance Network Simulation
- Internet Simulation and Visualization
- Internet Measurement and Analytics
- Economics, Regulation, Governance
- Emerging Markets



A Problem of Attribution and Belief

We are presented with an IP address.

- Which organization is actually operating the machine with that address? Where are they?
- When the Internet's underlying routing protocols are manipulated, IP addressing (“ground truth”) becomes **entirely unreliable**

BGP: Border Gateway Protocol (RFC1771, RFC4271)

- This single protocol governs traffic exchange among the roughly 49,000 **Autonomous Systems** that make up the Internet
- Each AS advertises their own IP networks, or **prefixes**, to their peers and transit providers
- Each AS independently picks the best (most specific, then shortest) **ASPath** to every prefix on earth.
- That local decision sends traffic on its way.

BGP's Paradox: Fragility and Resilience

The BGP **protocol** is simple and globally consistent.
But BGP **policy** is complex and locally determined.

- “My network, my rules” - every decision about what gets accepted, rejected, trusted, propagated is a **local decision**.

BGP's Paradox: Fragility and Resilience

The BGP protocol is simple and globally consistent.
But BGP policy is complex and locally determined.

- “My network, my rules” - every decision about what gets accepted, rejected, trusted, propagated is a local decision.
 - **This is good:** Great flexibility to support business objectives
 - **This is bad:** Vulnerability to bogus route propagation.

Let's Work An Example

Infrastructure Vocabulary

Autonomous System Numbers: ~~46~~ 32-bit ints

- Distributed by the Regional Internet Registries in each part of the world (RIPE, ARIN, APNIC,...)
- Small numbers = olde timers
 - MIT (3), Harvard (11), Yale (29), **Stanford (32)**
 - Level3 (3356), China Telecom (4134)
 - Microsoft (8075), Google (15169)
 - Bank of Taiwan (131148), Nomura (197039)

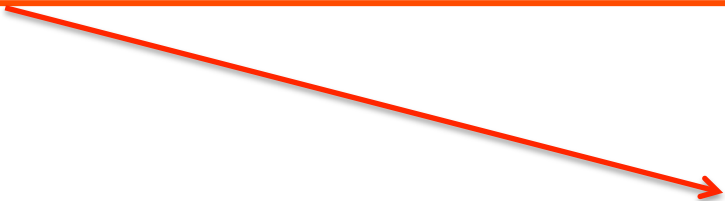
Let's Construct a Scenario

- Here's a complete scenario for how a BGP route hijacking might take place.
- The names and ASNs are real, but the scenario is **entirely fictitious**.
- We'll look at some real examples next.

Nomura Group, PLC (Tokyo, Japan)

Autonomous System #197039

- Assigned in the UK on 27 April 2010
- Authority: RIPE RIR



Nomura
197039



Nomura advertises eleven IPv4 address blocks

IPv4 Originated Networks (Global)	
★ Nomura International Plc AS 3.431	
1. Nomura International Plc (194.36.241.0/24)	Camden, Greater London, United Kingdom
2. Nomura Network 1 (85.119.25.0/24)	Westminster, Greater London, United Kingdom
3. Nomura Network 1 (85.119.26.0/24)	Wandsworth, Greater London, United Kingdom
4. NOMURA HOLDING AMERICA INC (147.62.65.0/24)	United Kingdom
5. Nomura Network 2 (85.119.27.0/24)	West Wickham, Greater London, United Kingdom
6. Nomura International Plc (194.36.240.0/24)	Brent, Greater London, United Kingdom
7. NOMURA HOLDING AMERICA INC (147.62.177.0/24)	New York, NY, United States
8. NOMURA HOLDING AMERICA INC (147.62.2.0/24)	New York, NY, United States
9. Nomura Network 2 (85.119.28.0/24)	Tower Hamlets, Greater London, United Kingdom
10. NOMURA HOLDING AMERICA INC (147.62.75.0/24)	New York, NY, United States
11. NOMURA HOLDING AMERICA INC (147.62.187.0/24)	New York, NY, United States

Nomura
194.36.241.0/24
London, UK

Nomura
197039



Nomura advertises eleven IPv4 address blocks

IPv4 Originated Networks (Global)	
★ Nomura International Plc AS 3.431	
1.	Nomura International Plc (194.36.241.0/24) Camden, Greater London, United Kingdom
2.	Nomura Network 1 (85.119.25.0/24) Westminster, Greater London, United Kingdom
3.	Nomura Network 1 (85.119.26.0/24) Wandsworth, Greater London, United Kingdom
4.	NOMURA HOLDING AMERICA INC (147.62.65.0/24) United Kingdom
5.	Nomura Network 2 (85.119.27.0/24) West Wickham, Greater London, United Kingdom
6.	Nomura International Plc (194.36.240.0/24) Brent, Greater London, United Kingdom
7.	NOMURA HOLDING AMERICA INC (147.62.177.0/24) New York, NY, United States
8.	NOMURA HOLDING AMERICA INC (147.62.2.0/24) New York, NY, United States
9.	Nomura Network 2 (85.119.28.0/24) Tower Hamlets, Greater London, United Kingdom
10.	NOMURA HOLDING AMERICA INC (147.62.75.0/24) New York, NY, United States
11.	NOMURA HOLDING AMERICA INC (147.62.187.0/24) New York, NY, United States

This one has 256 IPv4 addresses ($32-24=8$ bits)

Nomura
194.36.241.0/24
London, UK

Nomura
197039



Nomura advertises eleven IPv4 address blocks...

...and BGP Propagation
will ensure global
reachability of these
blocks.

How?

Nomura
194.36.241.0/24
London, UK

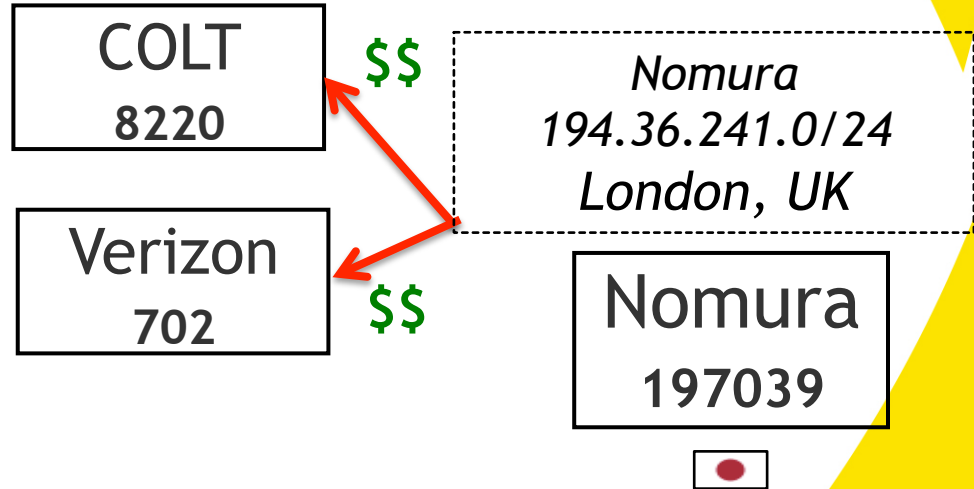
Nomura
197039



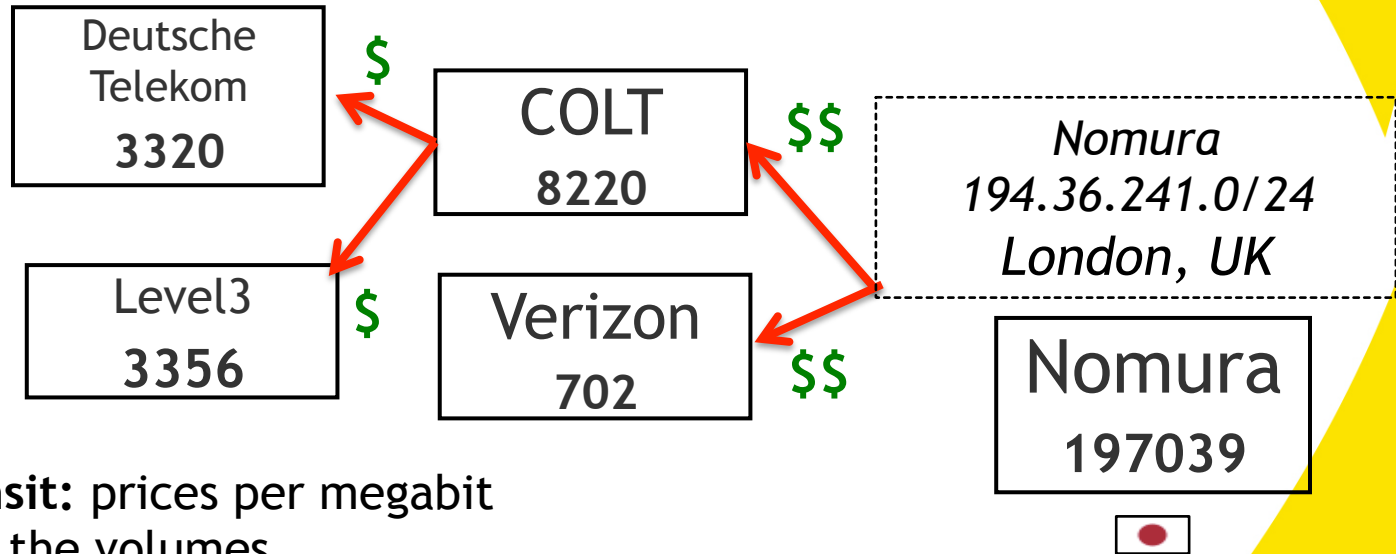
Nomura has two paid transit providers

Transit: I guarantee delivery to the entire world. (\$\$)

Peering: I only guarantee delivery to my customers

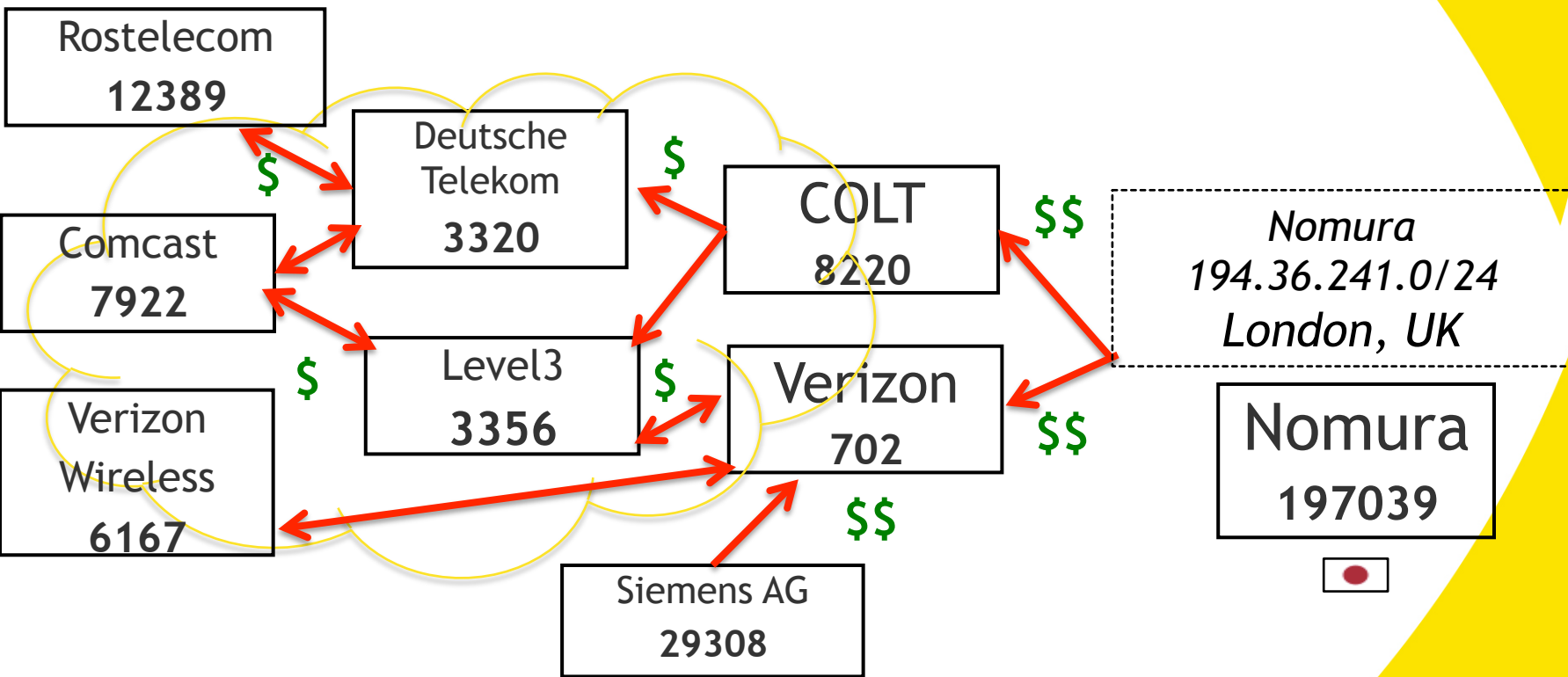


COLT in turn pays two transit providers



Wholesale Transit: prices per megabit tend to drop as the volumes exchanged increase (aggregation)

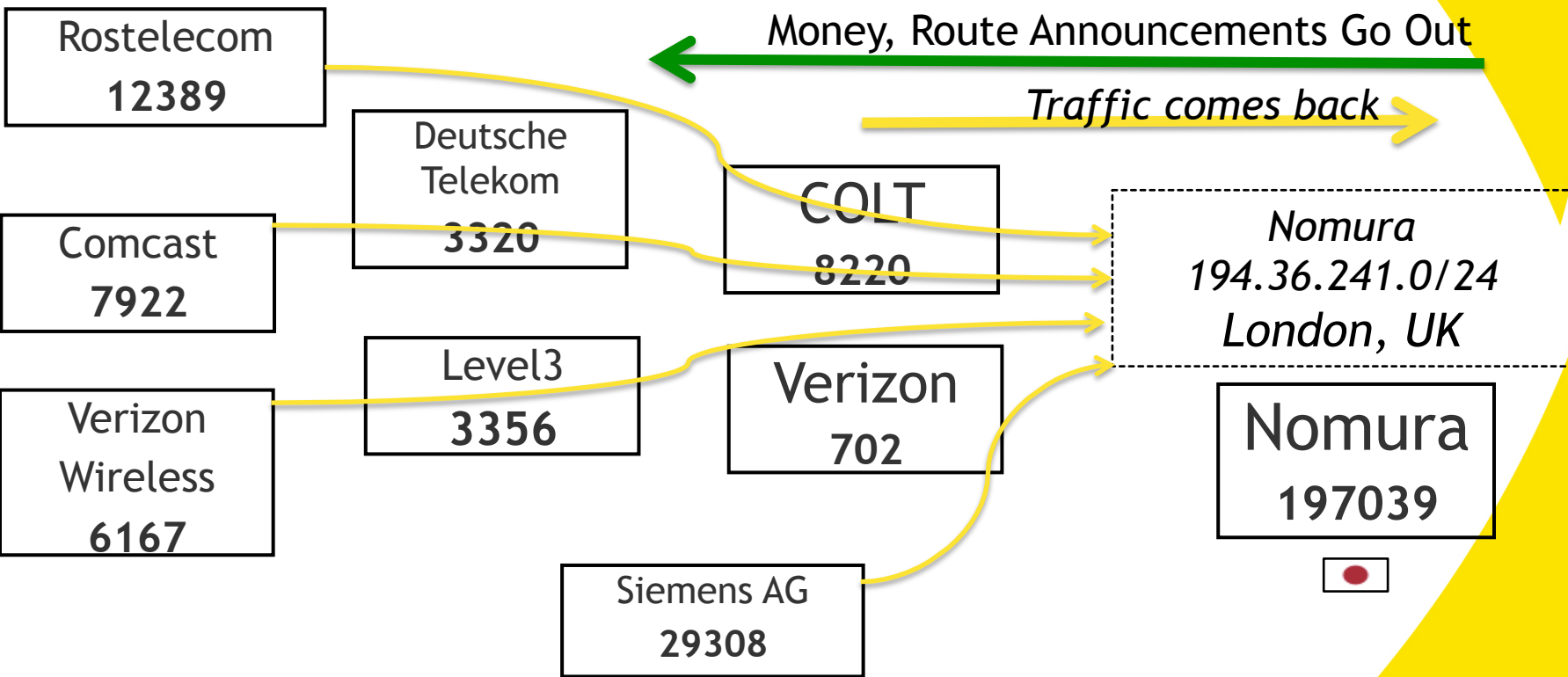
...And so on, until Nomura is globally reachable



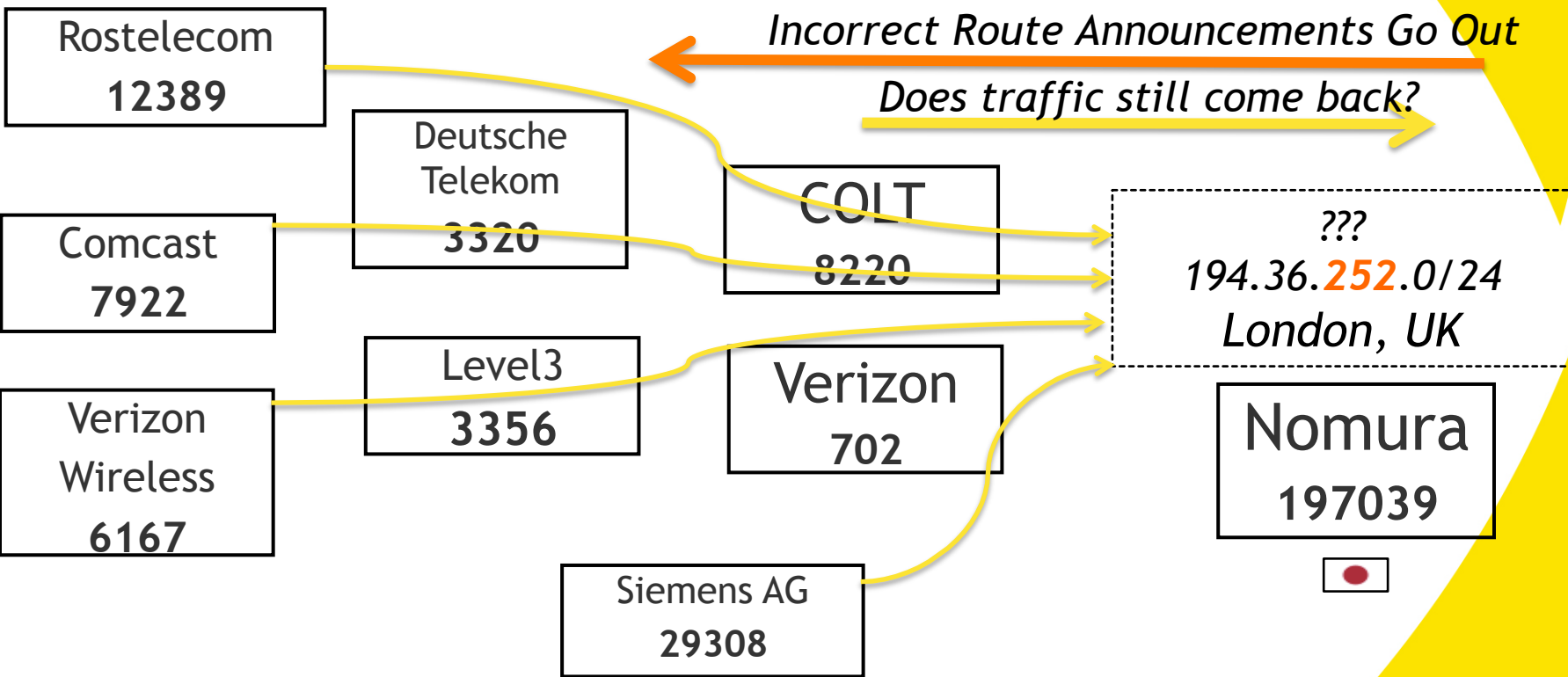
This model scales up nicely!

- 49,500 ASNs speaking BGP to each other
- 520,000 IPv4 networks announced broadly
- Another ~20,000 IPv6 networks
- ~40% of ASNs have one transit ASN, ~40% have two, and ~20% have 3+ (resilience!)
- Convergence time generally within 30s worldwide
- ASPATH lengths (edge to edge) average 5.3 hops

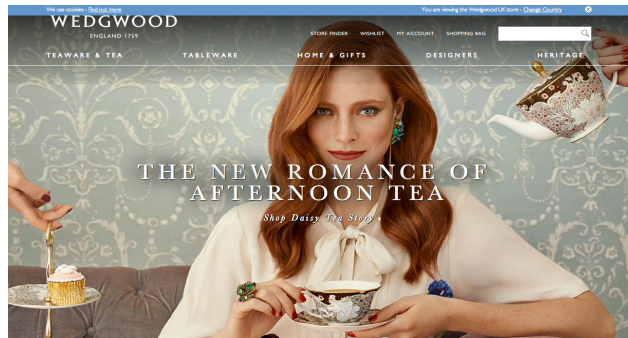
Routing is just a global “Whisper Game”



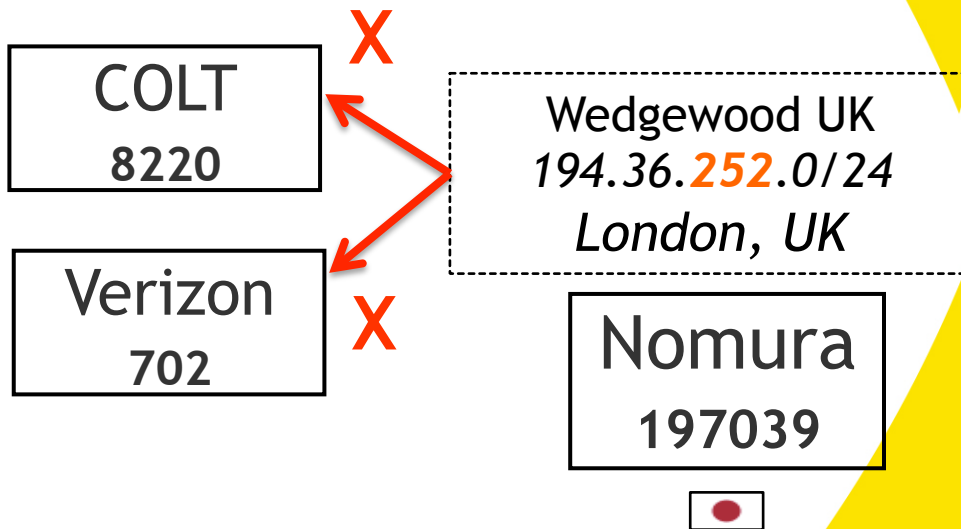
What if ... Nomura made an honest mistake?



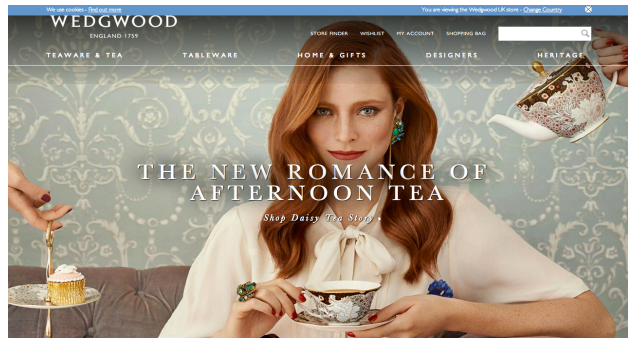
COLT and Verizon should recognize this blunder!



Their customer, Nomura, has no business advertising the (unused, unrouted) address space of Wedgwood China!

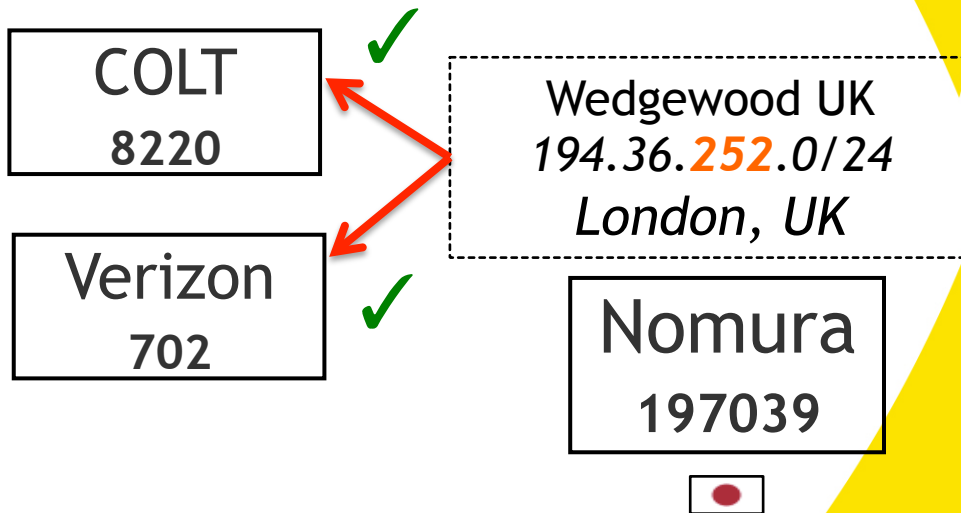


Many service providers filter; many don't.



If they fail to filter this mistake, and propagate the route to their providers and peers, it will probably be accepted everywhere on Earth within a few seconds.

No customer filtering = global propagation



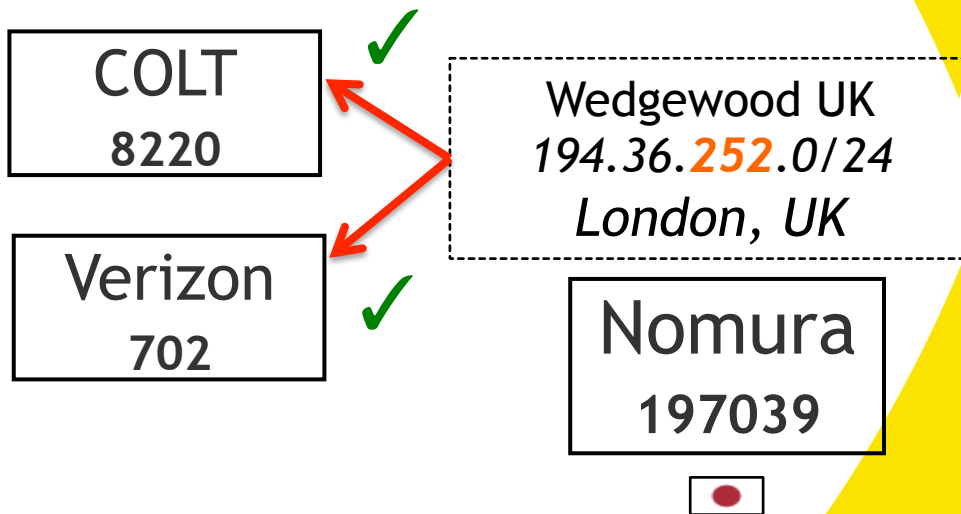
Why doesn't everyone filter customer routes?

Customer filtering is somewhat laborious and error-prone.

Hacks include:

- Setting MAXPREF
- Static lists of allowed prefix originations
- Building filters from entries in various routing registries
- Fragile, not agile

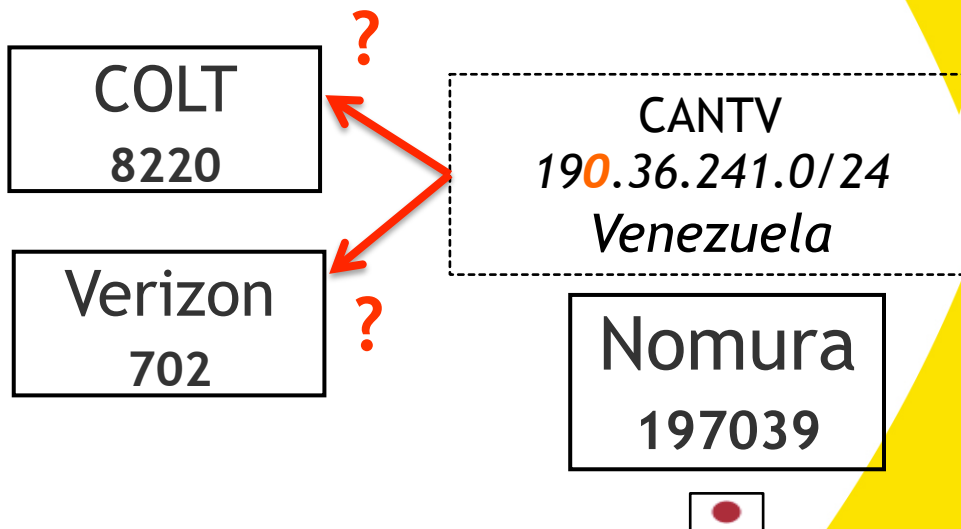
No customer filtering = global propagation



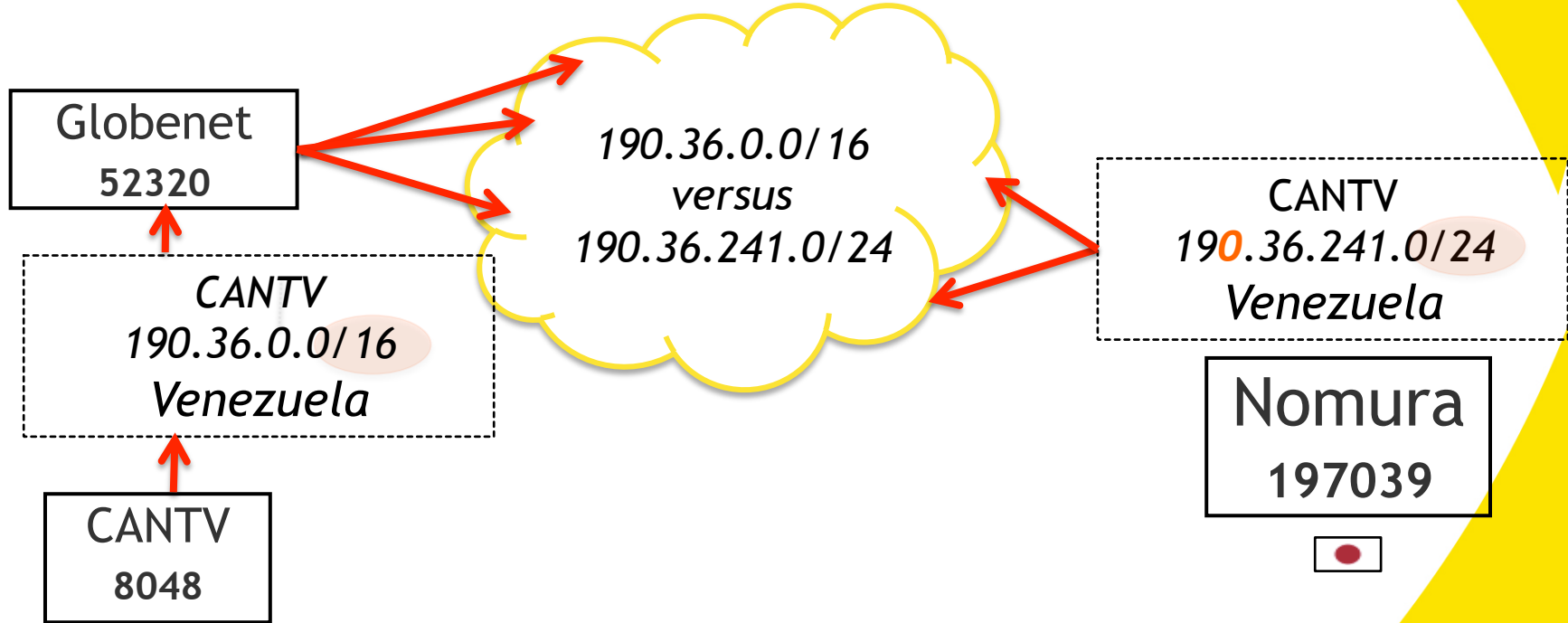
It could be much worse.



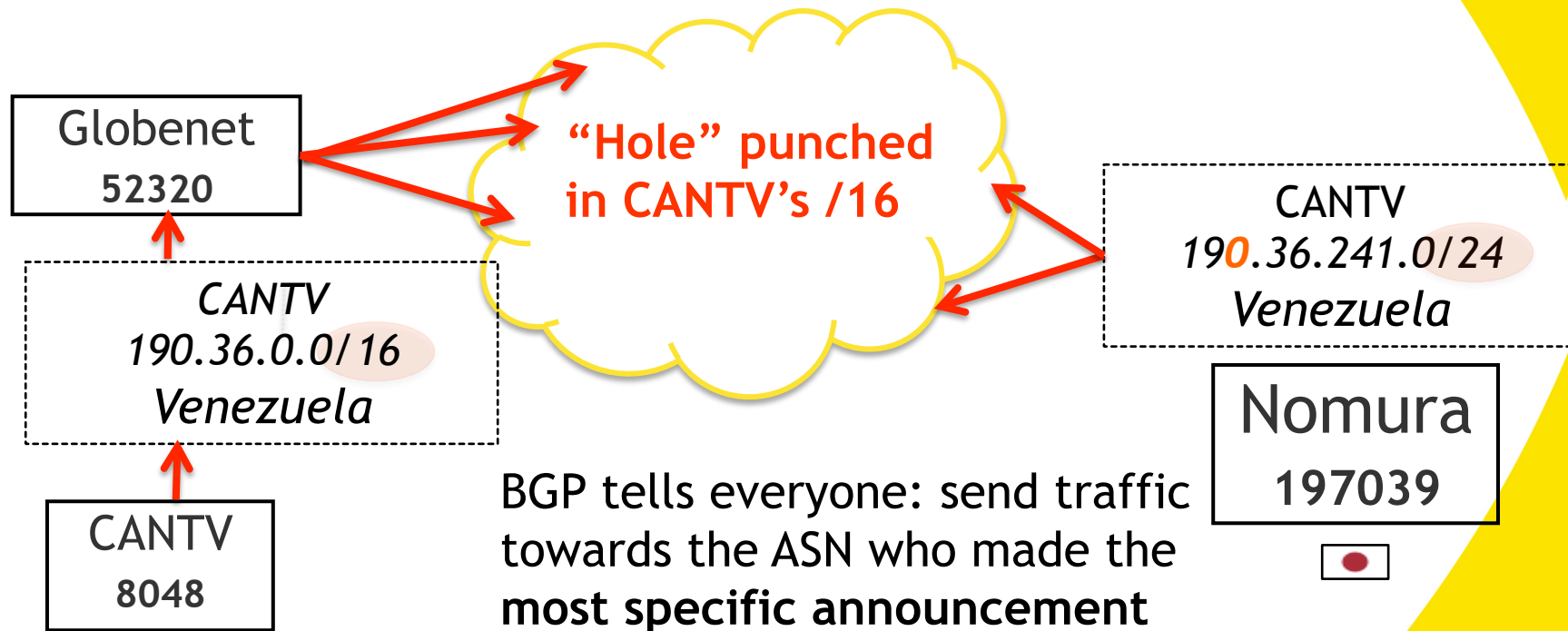
*What if the space is already
routed and in active use?*



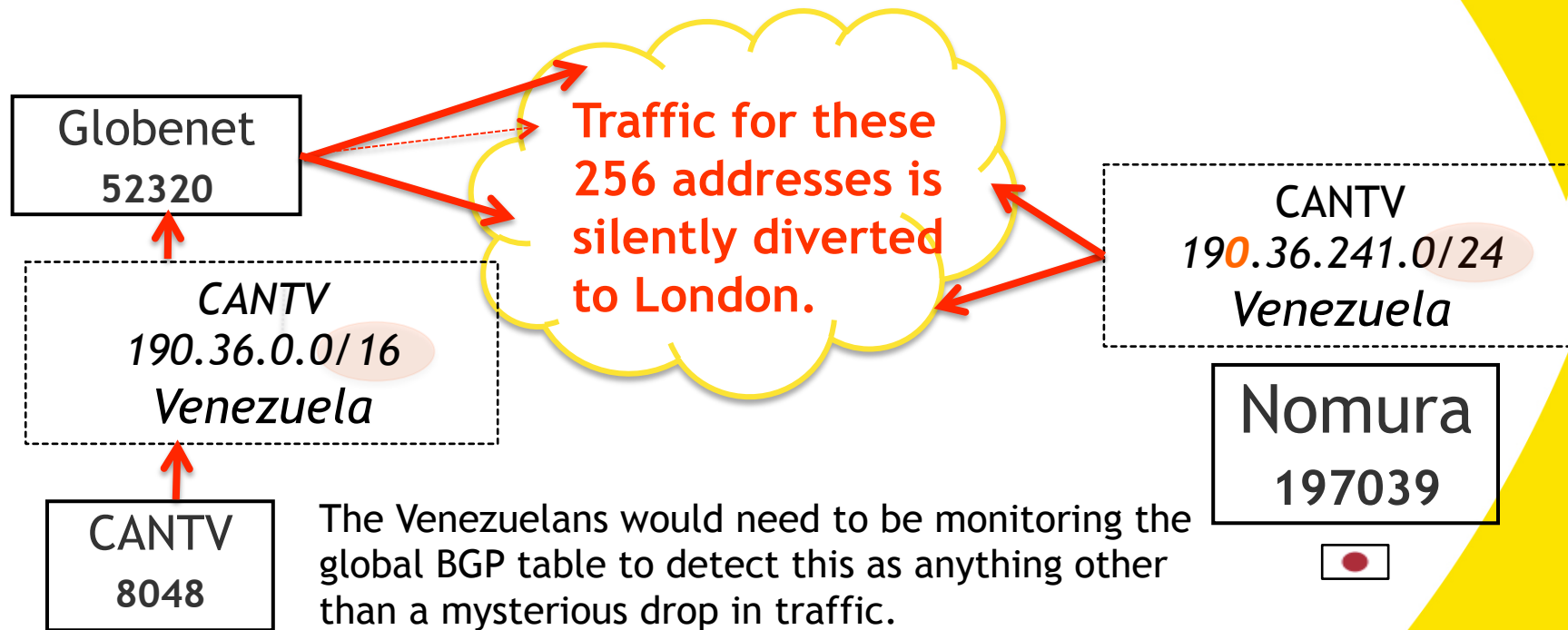
Now we have a fight for the space.



Now we have a fight for the space.



Now we have a fight for the space.



The Key Problem, Obviously, is Trust

Anyone can inject any advertisement they like!

- It's up to your providers and peers to detect and filter.
- There is **no central or even hierarchical authority** one can consult to say whether or not provider X is entitled to originate or transit address space Y

The Key Problem, Obviously, is Trust

Anyone can inject any advertisement they like!

- It's up to your providers and peers to detect and filter.
- There is **no central or even hierarchical authority** one can consult to say whether or not provider X is entitled to originate or transit address space Y
- **This is by design** - if there were such a central point of control, it would be a massive SPOF, subject to inappropriate influence

Enough Theory

Let's See Some Anomalies Already

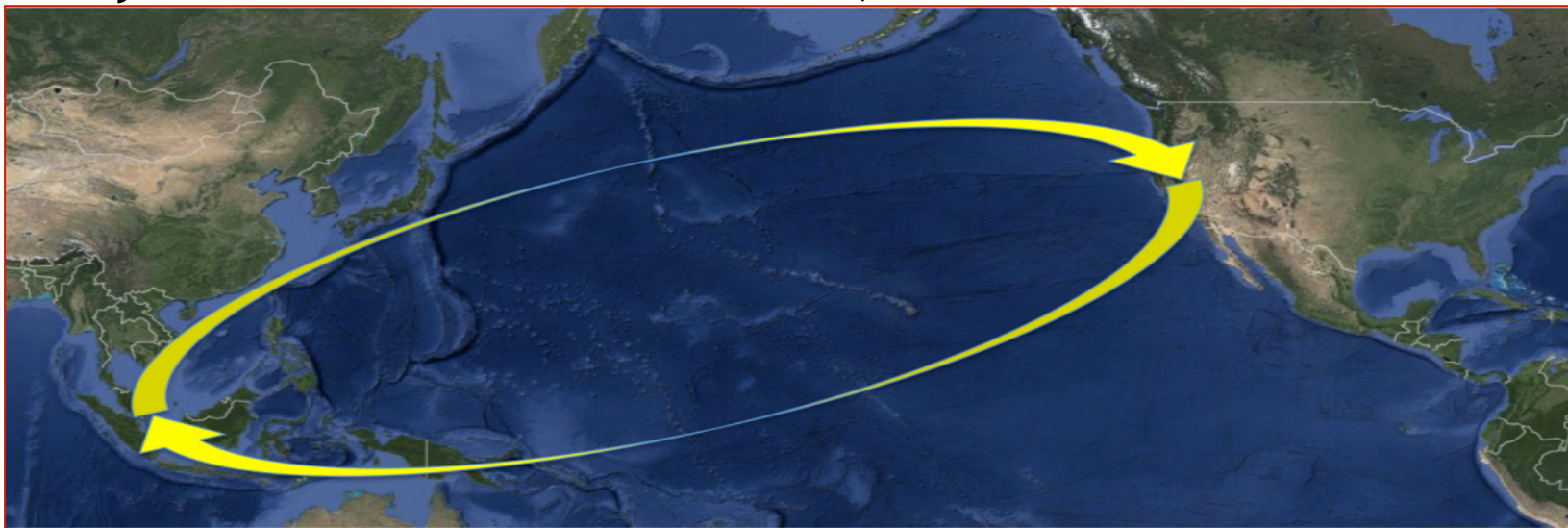
Let's Play a Game!

BGP's flexibility makes it hard to tell good from evil

- I'll show you a real world Internet routing scenario
- You guess whether it's **good** or **evil**
- Reasonable people can disagree on this classification, don't feel bad if you miss it

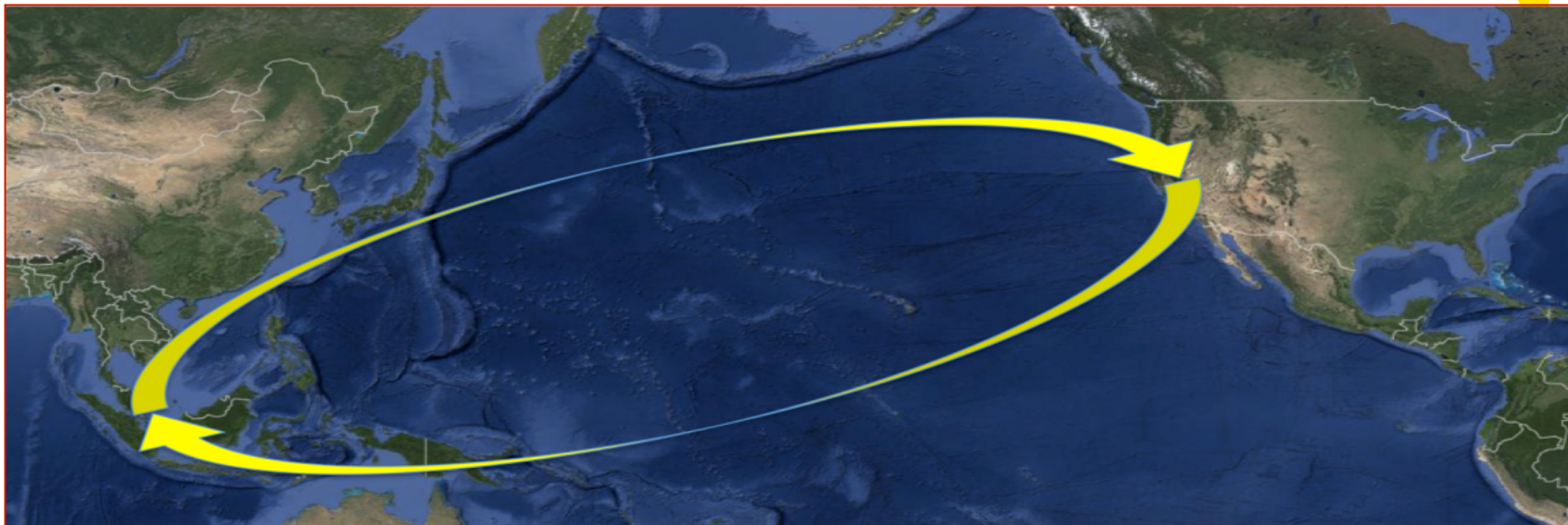
Scenario 1

Traffic between two floors of the **same office building** in Singapore takes over **350ms** round trip, taking a long detour via a mysterious datacenter in San Jose, California



Innocent!

Provider1 won't peer with Provider2 in Singapore; Provider2 must drag traffic to San Jose to hand it off to Provider1, who drags it home again to Singapore.



Scenario 2

Traffic from Western Europe to the US takes around 70ms round trip, traveling via Iceland's incumbent provider



Very Unusual

Iceland's Siminn advertised other people's routes in London, attracted the traffic, and reinjected it in Canada. Transatlantic Internet traffic should probably never come ashore in Iceland (cost, latency, geography).

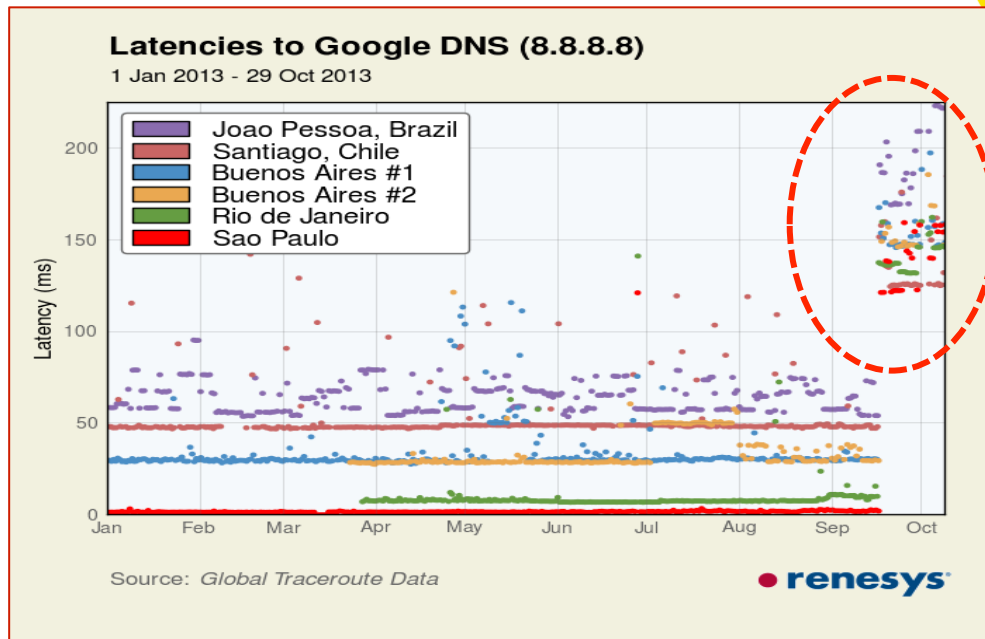


Scenario 3

Latencies to Google's public DNS servers increase dramatically from South America in October 2013.

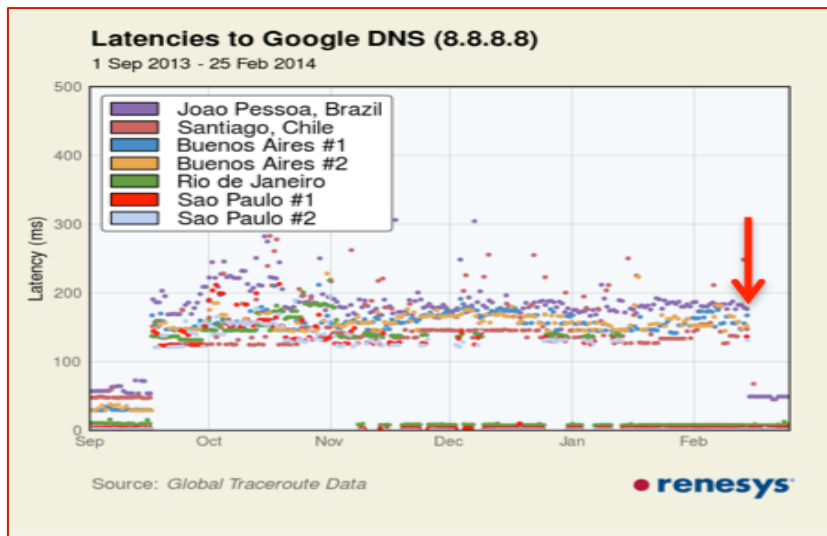
0-50ms RTTs to the
anycasted 8.8.8.8
recursive resolver

ICMP traceroutes from
Brazil, Chile, Argentina
suddenly take **120-220ms**



Not Evil.

Google anycast instances in Brazil stopped responding to South American consumer queries. DNS queries were being answered from California instead.



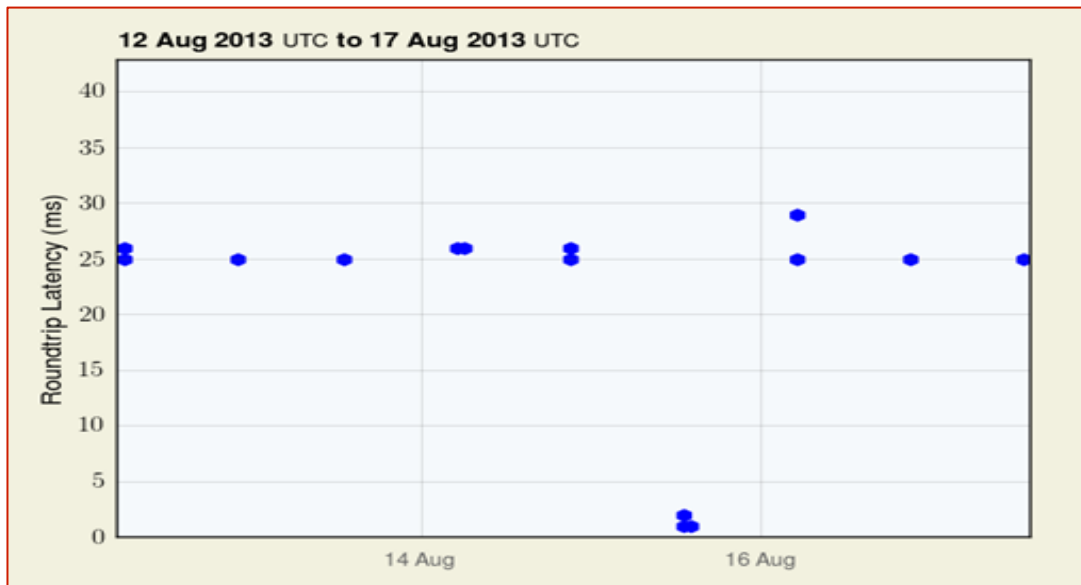
“Anycast” injects the same route in many places, and the BGP-closest instance serves.

Google anycast instances returned to Brazil in February 2014, and it's faster than ever.

Scenario 4

One day, latencies to a particular content provider network (hosting important domains for software download) decrease by 90% from Eastern Europe

ICMP round-trip measurements improve transiently from 25ms to less than 5ms



Really, Really Unusual.

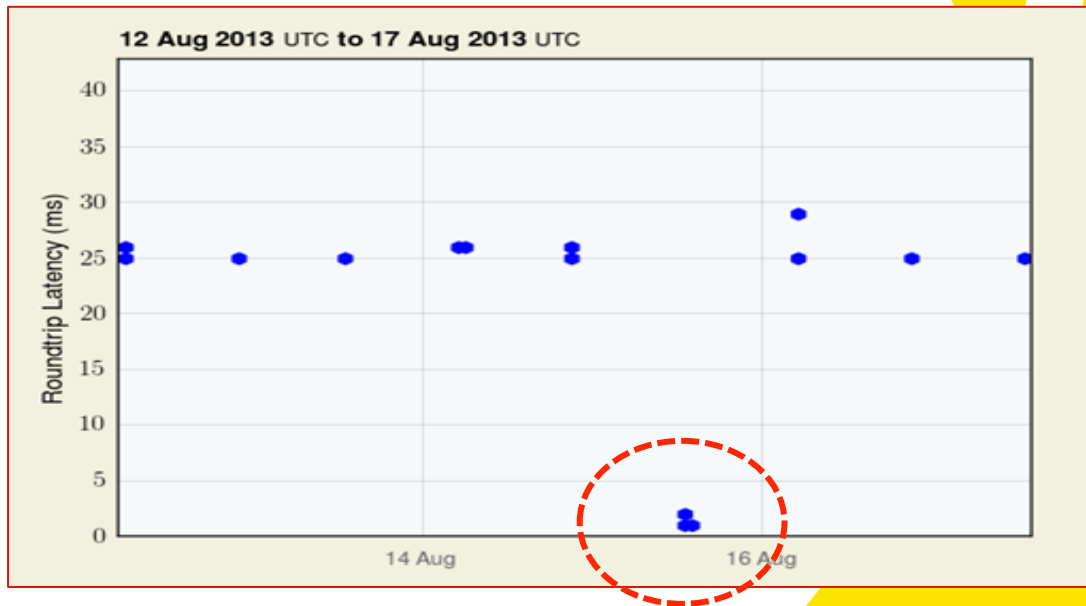
Content network (more specific of routed prefix) is hijacked, misdirection limited to immediate vicinity.

Speed of light violation sends clear signal that the site is now “somewhere else” ..

Traffic is landing on an alternative responder.

Need to assess:

- What's the footprint?
- What was the motive?



Scenario 5

Russian provider Vimpelcom advertises 7,000 customer prefixes to its peer, China Telecom, who in turn announces them to its peers.

China Telecom then announces more than 300,000 global routes to Vimpelcom in return.

Traffic increases **significantly** between the two peers.



A very bad idea.



VimpelCom



中国电信
CHINA TELECOM

trace from **Moscow** to **Manchester, NH** at 12:09 Aug 05, 2014

```
1 *
2 194.154.89.125 (Vimpelcom, Moscow, RU) 0.743ms
3 79.104.235.66 mx01.Frankfurt.gldn.net 40.574ms
4 118.85.204.53 beeline-gw3.china-telecom.net 43.198ms
5 202.97.58.57 (China Telecom, Shanghai, CN) 302.433ms
6 202.97.58.238 (China Telecom, Los Angeles, US) 479.642ms
7 202.97.49.14 (China Telecom, Los Angeles, US) 487.225ms
8 38.104.139.77 te0-7-0-24.ccr21.sjc03.atlas.cogentco.com 380.087ms
9 154.54.6.105 be2000.ccr21.sjc01.atlas.cogentco.com 375.079ms
10 154.54.28.33 be2164.ccr21.sfo01.atlas.cogentco.com 371.727ms
11 154.54.30.54 be2132.ccr21.mci01.atlas.cogentco.com 372.585ms
12 154.54.6.86 be2156.ccr41.ord01.atlas.cogentco.com 370.596ms
13 154.54.44.86 be2351.ccr21.cle04.atlas.cogentco.com 367.498ms
14 154.54.25.89 be2009.ccr21.alb02.atlas.cogentco.com 371.972ms
15 38.104.52.78 (Cogent, Albany, US) 367.334ms
16 70.109.168.139 burl-lnk.ngn.east.myfairpoint.net 321.980ms
17 64.222.166.166 (Fairpoint Communications, Concord, US) 315.036ms
18 64.223.189.66 static.man.east.myfairpoint.net 321.682ms
```

*Trace from Moscow to the US East Coast ...through
Shanghai and California*

Remember, peers are only supposed to provide mutual visibility into each others' customers.

When peers announce peer routes to other peers, it quickly turns into traffic misdirection .. Not a hijacking, but a policy breakdown.



BGP Hijacks, 2013-2015

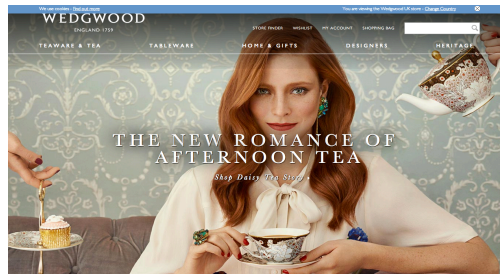
BGP Hijacks, 2013-2015

**Emergence of Man in the Middle (MITM)
Traffic Diversion**

Review: the “pecking order” of route hijacking

- Hijack space nobody is using in public (merely rude)

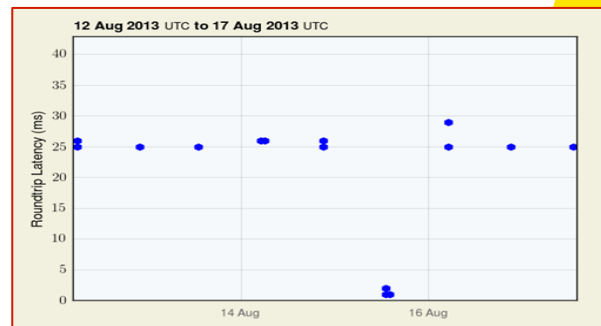
This will become more common as IPv4 address space nears exhaustion!



Review: the “pecking order” of route hijacking

- Hijack space nobody is using in public (merely rude)
- “Exact match” hijacking: attract some portion of the victim’s traffic and deny it to them
- Victim: **x.y.z.w/24** Hijacker: **x.y.z.w/24**

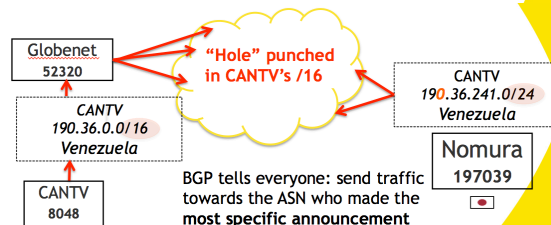
Basic denial of service. You only get the portion of global traffic that's “closer” to you (shorter ASPath). Your victim may not even notice!



Review: the “pecking order” of route hijacking

- Hijack space nobody is using in public (merely rude)
- “Exact match” hijacking: attract some portion of the victim’s traffic and deny it to them
- “More specific” hijacking: take **all** of the traffic to a subset of the victim’s address space

Victim sees 100% denial of service on the specific address range you’re hijacking --- even people very close to the victim may be fooled. (Youtube/Pakistan)



Review: the “pecking order” of route hijacking

- Hijack space nobody is using in public (merely rude)
- “Exact match” hijacking: attract some portion of the victim’s traffic and deny it to them
- “More specific” hijacking: take **all** of the traffic to a subset of the victim’s address space
- “Covering more specific” hijacking: deaggregate into more specifics, take **all** the traffic to **all** of the victim’s address space

Example: split the victim’s /22 into two /23s or four /24s. Very evil!

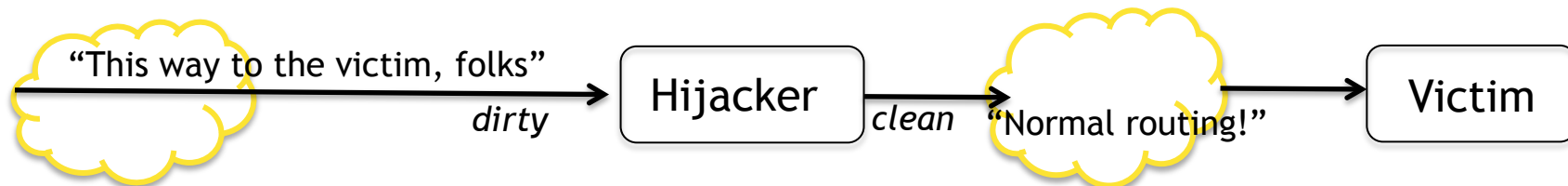
Review: the “pecking order” of route hijacking

- Hijack space nobody is using in public (merely rude)
- “Exact match” hijacking: attract some portion of the victim’s traffic and deny it to them
- “More specific” hijacking: take **all** of the traffic to a subset of the victim’s address space
- “Covering more specific” hijacking: deaggregate into more specifics, take **all** the traffic to **all** of the victim’s address space
- “Man in the middle:” attract the victim’s traffic, inspect it and/or modify it, and then quietly **deliver it to the victim** ✓✓✓

BGP MITM

Man in the Middle Hijacking requires two paths:

- One “dirty path” inbound, that believes your false routes
- One “clean path” outbound, that is unaware of them



Traffic comes in the dirty path, leaves by the clean path

What you do with it in the meantime is up to your imagination.

BGP MITM

Classic MITM was demonstrated live by Pilosov & Kapela on the show network at Defcon 16 (2008):

- Announce more-specifics, attract traffic
- AS path poisoning to maintain one clean path from attacker to victim
- **Never observed “in the wild”.**
- See the Renesys Black Hat DC 2009 talk.



BGP MITM

ASPath poisoning cleverly injects the victim's **own ASN** into the path

Loop detection algorithm blinds the victim to the manipulation

Everyone else, of course, can see what's going on.

Subsequent refinements will all focus on careful control of visibility of path manipulation.

BGP MITM

At least two possible approaches beyond Pilosov/Kapela simple path poisoning, *both of which* we first saw in 2013:

- **BGP Communities**
 - Used to limit propagation by upstream providers
 - Tricky to get right, especially since the upstreams might be interconnected
 - We've seen use of communities evolve over time
- **Announcements only to peers**, not transit providers
 - Peering relationships are between competitors
 - Peers will not propagate routes (otherwise they provide free transit!)

Requires provider with many peers in order to get appreciable amounts of traffic

MITM Hijacks in 2013

Beltelecom (AS 6697)

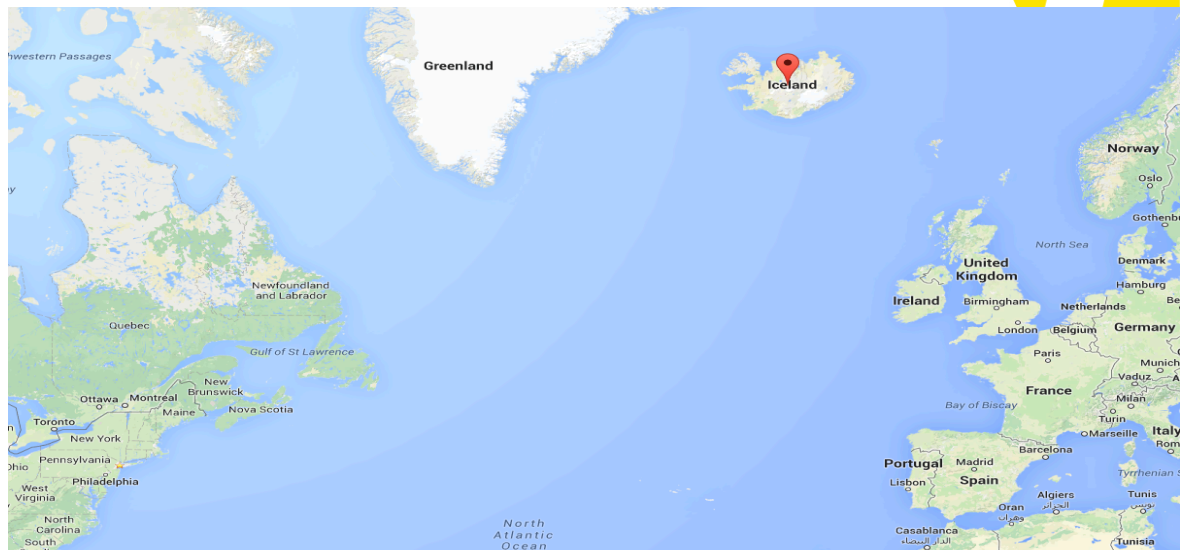
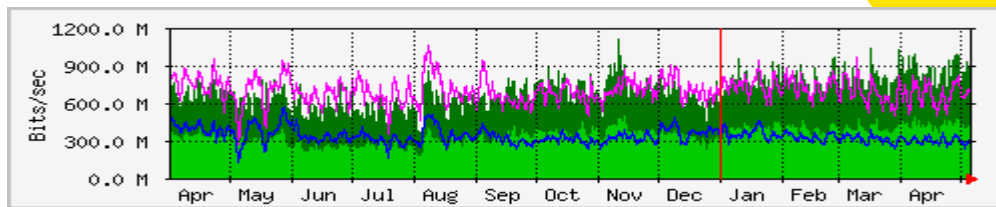
- Belarus incumbent
- Several downstream AS “origins” for hijacked prefixes
- Traces pass only through Beltelecom, not the claimed origin



MITM Hijacks in 2013

Siminn (AS 6677)

- Iceland incumbent
- Several downstream AS “origins”
- Traces pass only through Siminn, not the claimed origin
- Siminn conceded redirection of traffic, but claimed router bug



NYC to Los Angeles

Traceroute Path from New York, NY to Los Angeles, CA via *Belarus*



Germany to California

Traceroute from Frankfurt, Germany to Fremont, CA via *Iceland*



Denver to... Denver!

Traceroute Path from Denver, CO to Denver, CO via *Iceland*



Exploiting BGP Communities

Hijacker announces prefix p to regional provider P with BGP community P:71990

Whois tells us:

remarks	To deny prefix propagation,
remarks	use P:7DNNA, where
remarks	D - Deny announcements:
remarks	1 - International peers
remarks	2 - In-country peers
...	
remarks	NN - Upstream:
remarks	01 - Provider 1
remarks	02 - Provider 2
...	
remarks	99 - All Upstreams
...	
remarks	A - Action:
remarks	0 - Do not announce prefix

- The hijacker tells P not to announce p to any of its international peers, implying that it should announce p only to its domestic peers and customers.
- In this way, the hijack of p is constrained to a geographic region.
- Regional traffic for p is misdirected to the attacker, who can then forward it onward to its rightful owner via a clean path through another provider.

2013 Statistics

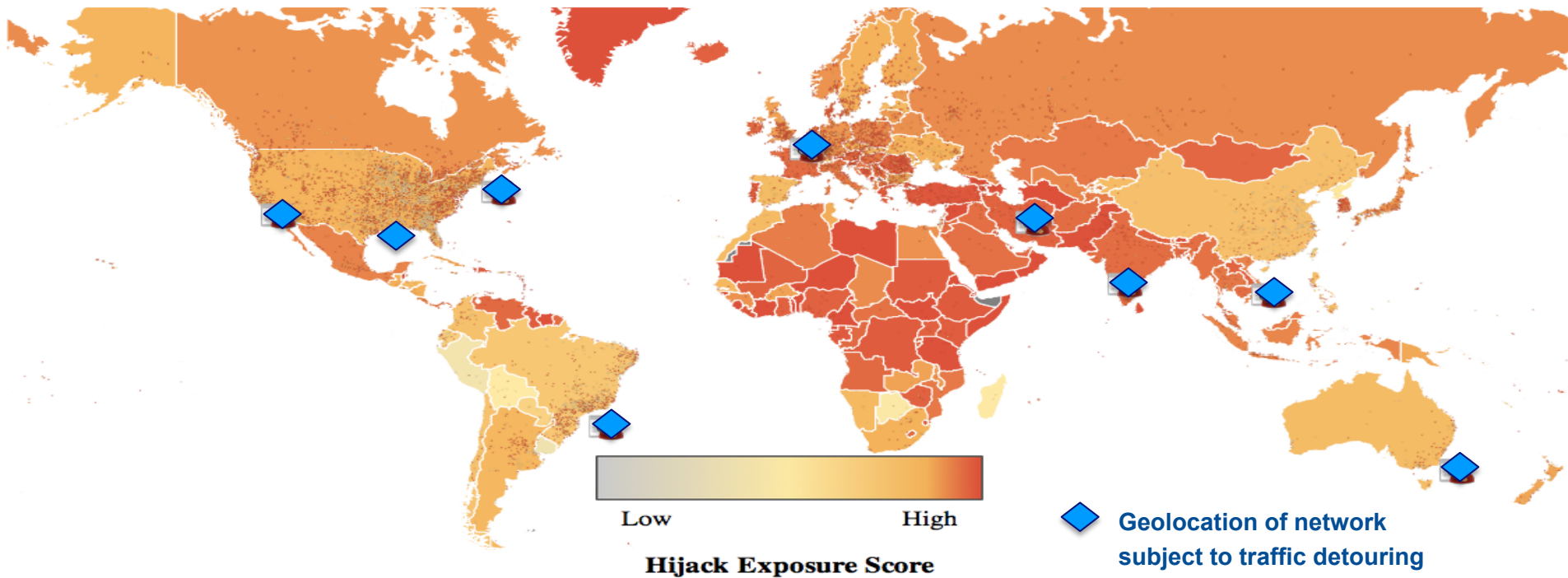
- Major hijacks occurred on **102 days** in 2013 (29% of the days), and most were suddenly MITM
- Almost 1,500 networks (prefixes) were targeted, geolocating to over 150 cities worldwide. Targets included financial services, various governments, NSPs, content providers.
- Hijacked networks contain over 500,000 domains (FQDNs)
- Traffic detouring was persistent! *One hijack persisted for 3 months.*
- Techniques were refined over time.
- Global impact varied depending on providers accepting the bogus routes and techniques employed

2013 Hijacks by City



27 Feb 2013

Hijack Score -- Wed Feb 27 00:00:00 2013



What Happened Next

The Washington Post

PostTV

Politics



The Switch

Where technology and policy connect

(The Cat Leaves the Bag)

ars technica



MAIN MENU

MY STORIES: 25

WIRED

GEAR

SCIENCE

ENTERTAINMENT

BUSINESS

SECURITY

DESIGN

OPINION

MAGAZINE

THREAT LEVEL

cybersecurity

Hacks and Cracks

Security

surveillance

Someone's Been Siphoning Data Through a Huge Security Hole in the Internet

BY KIM ZETTER 12.05.13 | 6:30 AM | PERMALINK



3



1



558



RISK ASSESSMENT / SECURITY & HACKTIVISM

Repeated attacks hijack huge chunks of Internet traffic, researchers warn

Man-in-the-middle attacks divert data on scale never before seen in the wild.

by Dan Goodin - Nov 20 2013, 1:00pm CET

HACKING NETWORKING

86

dyn.com

@dyn

Result: a Brief Slowdown in BGP Mischief

We continued to see ‘traditional’ hijackings:

- Accidental route leaks
- Fat finger typos
- Active verification showed *less MITM* after our publication

Impacts were significant for those whose networks are involved, but this seemed like “benign” hijacking compared to 2013’s MITM series.





The screenshot shows the Dyn Research website header with the logo and tagline 'THE NEW HOME OF renesys'. Below the header is a navigation bar with 'HOME', 'TOPICS', 'PRESENTATIONS', and 'ABOUT'. A secondary bar displays metadata: 'JANUARY 29, 2015', 'COMMENTS (9)', 'VIEWS: 5751', 'SECURITY', and 'DOUG MADORY'. The article title is 'The Vast World of Fraudulent Routing', followed by social media icons. The text discusses network security challenges, mentioning 'entirely on trust' and 'autonomous system numbers (ASNs)'. It describes how criminals hijack IP address space by misdirecting traffic through victim ASNs.

Dyn Research
THE NEW HOME OF renesys

HOME TOPICS PRESENTATIONS ABOUT

○ JANUARY 29, 2015 💬 COMMENTS (9) 📊 VIEWS: 5751 📁 SECURITY 👤 DOUG MADORY

The Vast World of Fraudulent Routing

🐦 📘 🍏 🔗 📺

As network security engineers have attempted to categorize blocks of IP addresses associated with spam or malware for subsequent filtering at their firewalls, the bad guys have had to evolve to continue to target their victims. Since routing on the global Internet is based *entirely on trust*, it's relatively easy to commandeer IP address space that belongs to someone else. In other words, if the bad guys' IP space is blocked, well then they can just steal someone else's and continue on as before.

In an attempt to cover their tracks, these criminals will sometimes originate routes using *autonomous system numbers (ASNs)* that they don't own either. In one of the cases described below, perpetrators hijacked the victim's ASN to originate IP address space that could have plausibly been originated by the victim. However, in this case, the traffic was misdirected to the bad guy and an unsophisticated routing analysis would have probably shown nothing amiss.

Reprieve: 6 months.

All that changed in the second half of 2014, and in 2015, hijackers are back in force.

We think it's being driven by

- Address space scarcity
- Sending spam
- Malware hosting
- Need to cover one's tracks

Defense?

Defense?

Let's start with Discovery.

Achieving Global Coverage

Each of the 49,000+ ASes on the Internet could ...

- Use their favorite route monitoring service.
- Publish their routing policies in an IRR and keep them updated, allowing others (who?) to do the monitoring.
- Cryptographically sign their originations and establish chain of authority for every change
- “Origin authentication” necessary but not sufficient
- “Route update validation” requires broad deployment of routers that validate, and a lot of compute cycles per BGP update

Validating a BGPsec Update Message

“When a BGPsec update message is received by a BGP speaker, the BGP speaker can validate the message as follows. For each signature, the BGP speaker first needs to determine if there is a valid RPKI Router certificate matching the SKI and containing the appropriate AS number. The BGP speaker then verifies the signature using the public key from this BGPsec router certificate. If all the signatures can be verified in this fashion, the BGP speaker is assured that the update message it received actually came via the AS path specified in the update message. In the above example, upon receiving the BGPsec update message, a BGP speaker for AS 4 would do the following. First, it would look at the SKI for the first signature and see if this corresponds to a valid BGPsec Router certificate for AS 1. Next, it would verify the first signature using the key found in this valid certificate. Finally, it would repeat this process for the second and third signatures, checking to see that there are valid BGPsec router certificates for AS 2 and AS 3 (respectively) and that the signatures can be verified with the keys found in these certificates. Note that the BGPsec speaker for AS 4 should additionally perform origin validation as per RFC 6483 [RFC6483]. However, such origin validation is independent of BGPsec....” [https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-overview-06]

Until that day comes

We can use global historical routing data to identify anomalies as they emerge, and chase them down algorithmically.

- Find suspicious origins, AS paths
- Use global traceroute data to look for MITM or hosts in the attacker's network that answer (e.g., Turkey answering for Google's DNS servers).
- Difficulty: The Internet is a very dynamic place.
- It's really easy to generate an overwhelming number of false positives.

False positives

A new more-specific prefix announced from a seemingly unrelated origin will always generate an alert.

AS393327 (THE GEORGE W. BUSH FOUNDATION, US)

announced 1 pfx(s) that are potentially
hijacks of currently routed address space:

12.203.53.0/24 (GEORGE W. BUSH PRESIDENTIAL
CENT, US), seen by 394 peers for an average
of 0.57 hours. This is a more specific of
12.128.0.0/9 (AT&T Bell Laboratories, US)
Origin=7018 (AT&T, US)

*** 8 MAY 2014

False positives

A new more-specific prefix announced from a seemingly unrelated origin will always generate an alert.

AS393327 (THE GEORGE W. BUSH FOUNDATION, US)
announced 1 pfx(s) that are potentially
hijacks of currently routed address space:

12.203.53.0/24 (GEORGE W. BUSH PRESIDENTIAL
CENT, US), seen by 394 peers for an average
of 0.57 hours. This is a more specific of
12.128.0.0/9 (AT&T Bell Laboratories, US)
Origin=7018 (AT&T, US)

*** 8 MAY 2014 - **ROUTING ACCOMPLISHED**



Eliminating False Positives Requires Domain Knowledge

Suppress alerts for *new* originations that meet certain conditions:

- Origination has been **seen in the past** (e.g., traffic engineering)
- Origination seen by **very few peers** or a very short duration
- Prefix is one known to be **multiply originated** (e.g., root server, anycast infrastructure)
- New origin is part of the **same organization** as typical origin
 - (e.g., AT&T has over 100 ASNs)
- New origin is a **DDoS mitigation** service (e.g., Prolexic)
- **Obvious typos** (e.g., edit distance 1 from legitimate announcement)
- ... many more rules to filter innocent errors / typical usage

Look for Novelty in the Rest

Score new origination patterns by *unusualness*

- Hijacking AS now operating in a **new, distant geography**?
- Hijacked prefix hosting **important domains**?
- Traces pass *through* hijacking AS onto legitimate AS (**MITM**)?
- Traces *terminate* at hijacking AS (**impersonation**)?
- ... many more rules to score novelty and call out the most suspicious originations for review

Automated Reporting

Dyn Research generates a handful of internal reports per day.

Many are false positives and easily dismissed.

Occasionally, we get a “live one”.

Here is one automated report entry from April 2014:

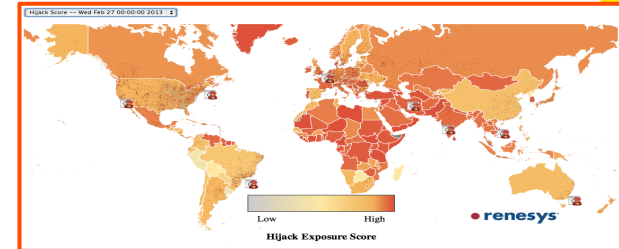
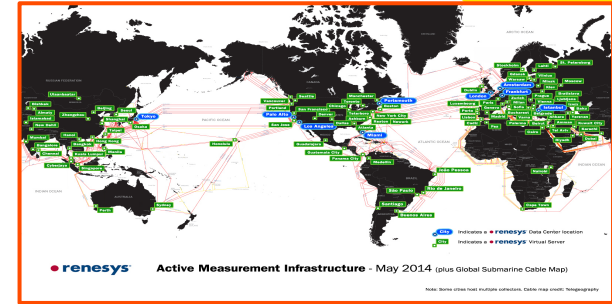
```
AS6697 (Beltelecom, BY) announced 1 pfx(s) that are potentially hijacks of  
currently routed address space:
```

```
XXX.YYY.151.0/24 (ZZZZ, GB), seen by 310 peers for an average of 1.16  
hours. This is a more specific of prefix: XXX.YYY.128.0/19 (ZZZZZ),  
Origin=NNNN (ZZZZZ, GB)
```

Fundamental Detection Issues

Fundamental Detection Issues

- Internet infrastructure incidents impacting a specific enterprise typically occur beyond the enterprise's perimeter and *may be invisible from the enterprise's vantage points*
- Widely distributed global sensor network is necessary to *minimize false negatives* (otherwise, regional or provider specific events can be missed)
- Multiple data sources and sophisticated analytics are necessary to detect deviations from “normal” and *minimize false positives*



Fundamental Detection Issues

How do we distinguish malicious/suboptimal from legitimate?

Best case: An enterprise knows “Ground Truth” for what it cares about.
Monitoring system then alerts on any deviations.

Actual case: “Ground Truth” is rarely fully and correctly specified,
and never will be for most organizations.

Monitor long enough to determine the “approximately correct”★ state,
alert on deviations, automate response processing

★ with thanks to Leslie Valiant, author of *Probably Approximately Correct*.

Route Hijacking Is Here to Stay

- It's no longer acceptable for route hijacking to go unobserved.
- BGP route hijacking is an attack on the foundations of the Internet, and there are no simple solutions within reach of global deployment
- The incidence of malicious route hijacking can be driven to zero, *if everyone commits to watching carefully.*

Research Data and Other Resources

- CAIDA: <http://www.caida.org>
- Measurement Lab: <http://www.measurementlab.net>
- Oregon Routeviews: <http://www.routeviews.org>
- RIPE RIS: <https://www.ripe.net/data-tools/stats/ris/ris-raw-data>

Each of these repositories of datasets has associated caveats, but finding them is part of the challenge, and you can't beat the price.

A final plea

If you aspire to study Internet measurement:

- Seek fellowship with people who make their living pushing packets
- Attend conferences where network operators gather
- Buy them refreshments
- Sanity-check your great ideas against their experience



Thank you!

<http://research.dyn.com>



Border Gateway Protocol: The Good, Bad, and Ugly of Internet Routing

Jim Cowie, Chief Scientist

@jimcowie / @DynResearch

Stanford EE Computer Systems Colloquium

11 February 2015