Global Routing Incidents

And the Need for Good MANRS

Jim Cowie, Chief Scientist
Doug Madory, Director of Internet Analysis

13 October 2015
Odessa, Ukraine

INTERNET
PERFORMANCE.
DELIVERED.

dyn.com @dyn

The Problem with Global Routing

- IPv4: 52,000+ active ASNs
  - 550,000+ routes
  - 385,000+ *ASN relationships*
- IPv6: 10,000+ active ASNs
  - 16,000+ IPv6 routes
  - 100,000+ *ASN relationships*

No global agreement (and very little regional or local agreement) about "who should be routing what"

TODAY: FOUR OPERATIONAL

risks

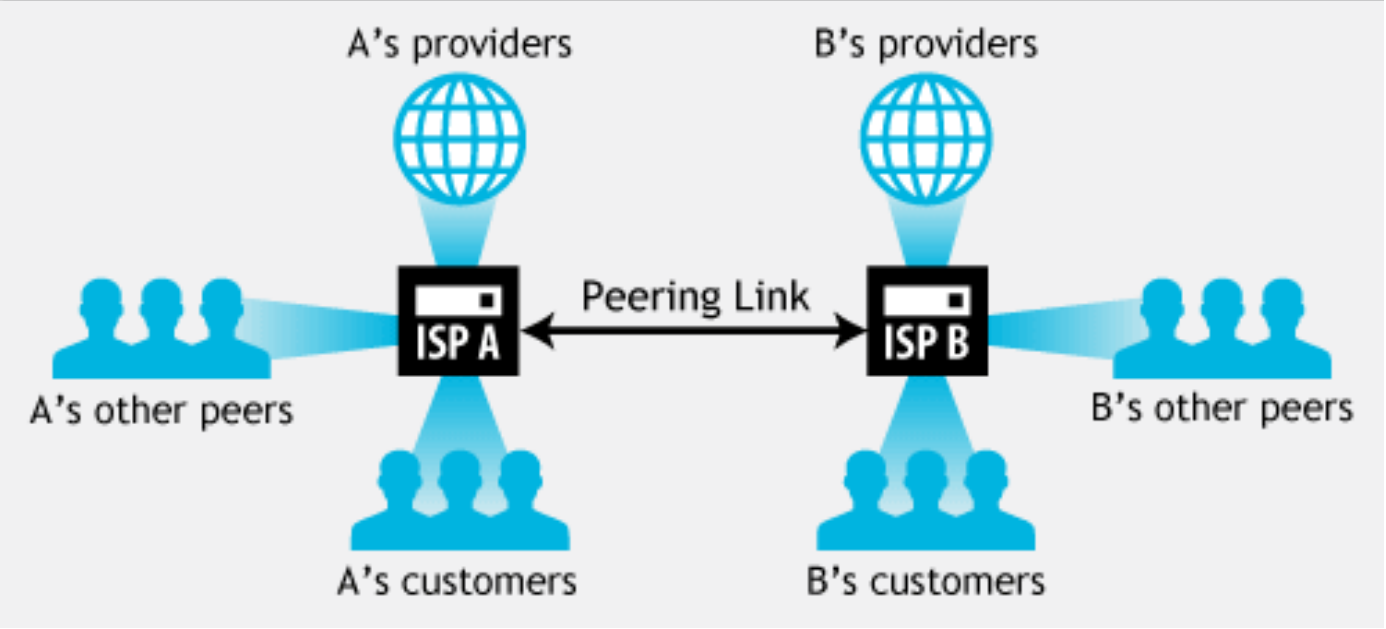
AND NO PERFECT SOLUTION

RISK #1

oversharing

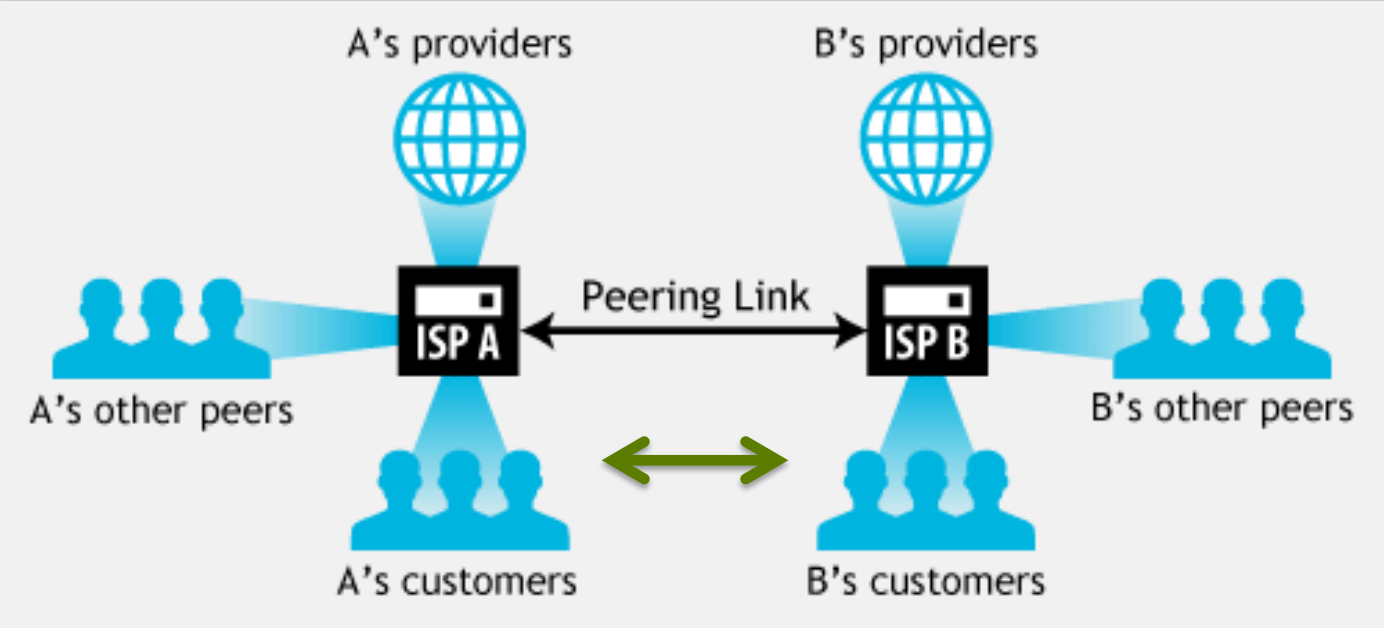
SENDING ROUTES TO THE WRONG PEOPLE

Peering - Normal Behavior



Peering: the most common kind of interconnection on the Internet!

Peering - Normal Behavior

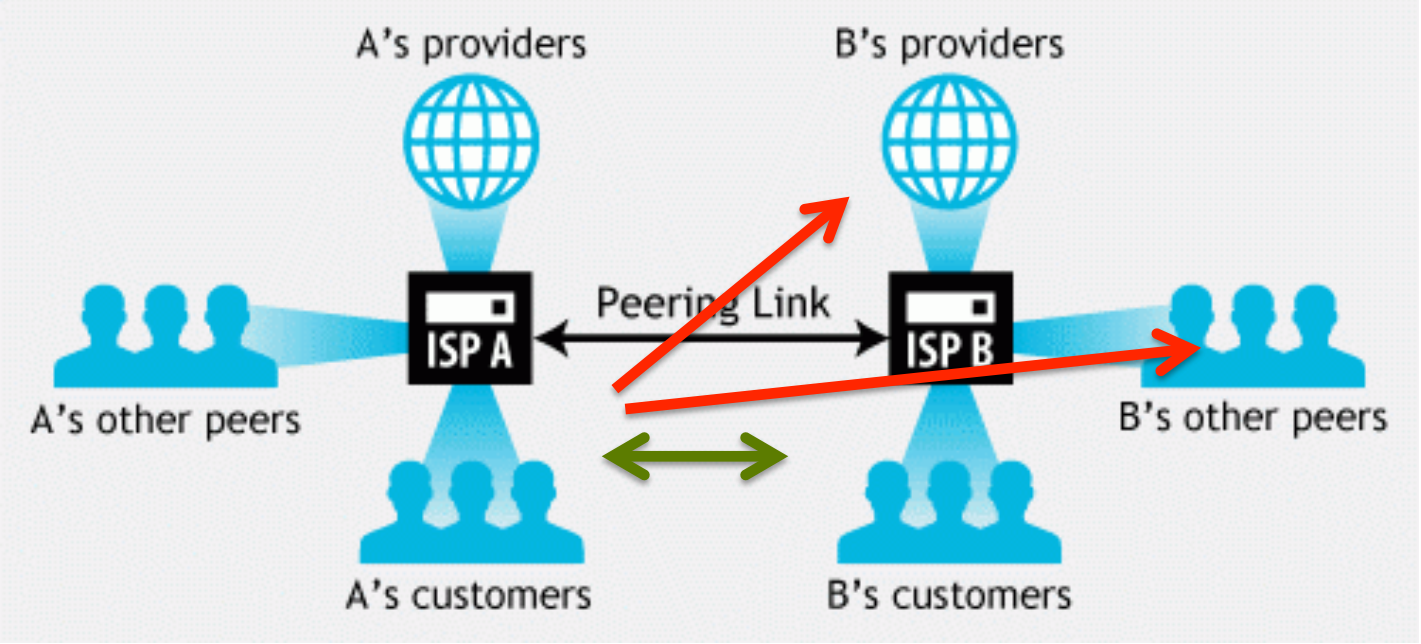


We need just two rules to make peering for mutual benefit leak-free.

A announces **only its customers** to B

B **only sends** these announcements to its **own customers**

Peering - Routing Leak (Scenario 1)

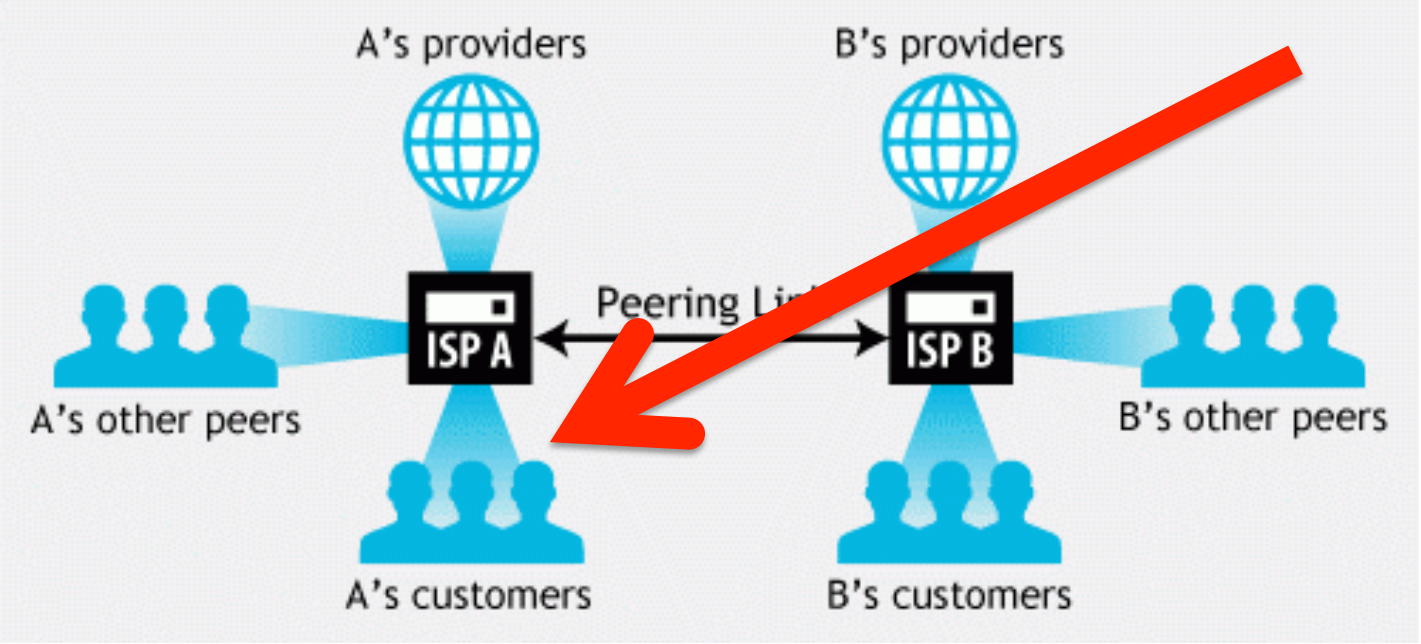


One way to leak: send peering routes to the wrong people

A announces **only its customers** to B

B **also sends** these announcements to its peers .. or providers

Peering - Routing Leak (Scenario 1)

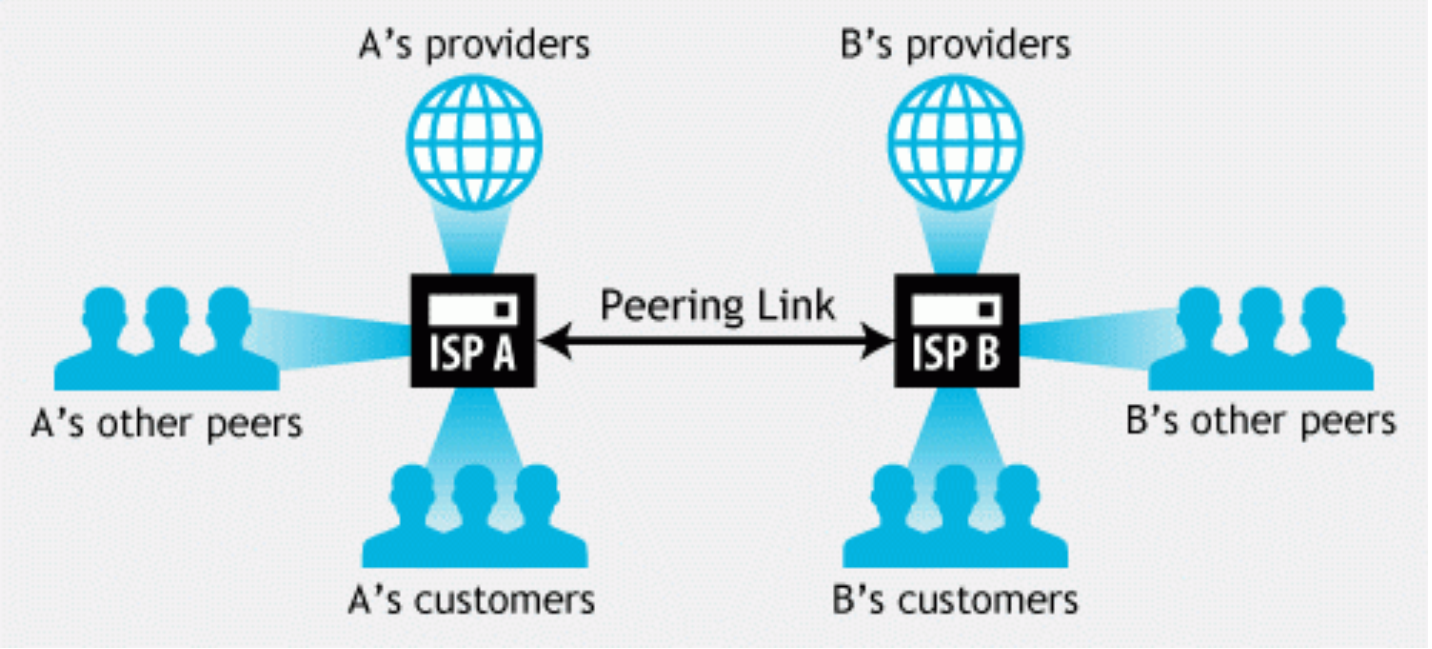


B is inserted into the inbound traffic going to A's customers

A announces **only its customers** to B

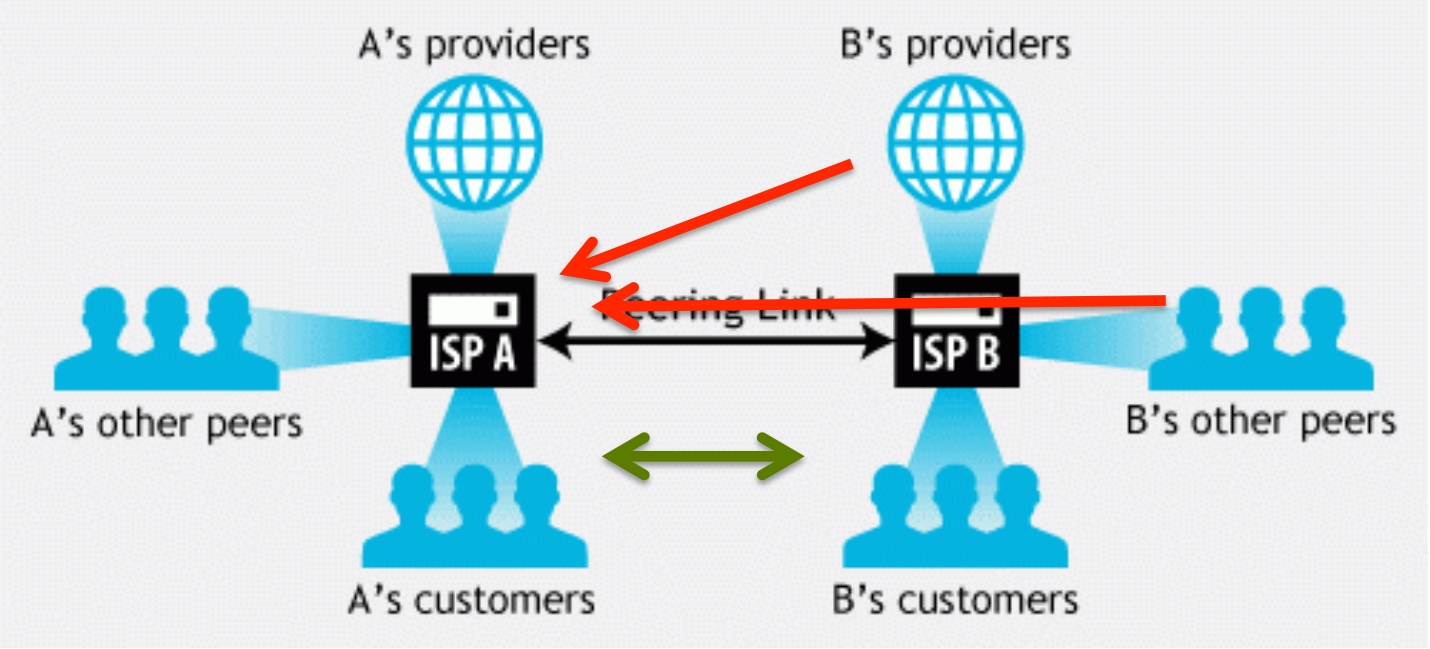
B **also sends** these announcements to its peers .. or providers

Peering - Routing Leak (Scenario 2)



Alternatively, if A accepts B's noncustomer routes, B becomes an "accidental transit provider"

Peering - Routing Leak (Scenario 2)



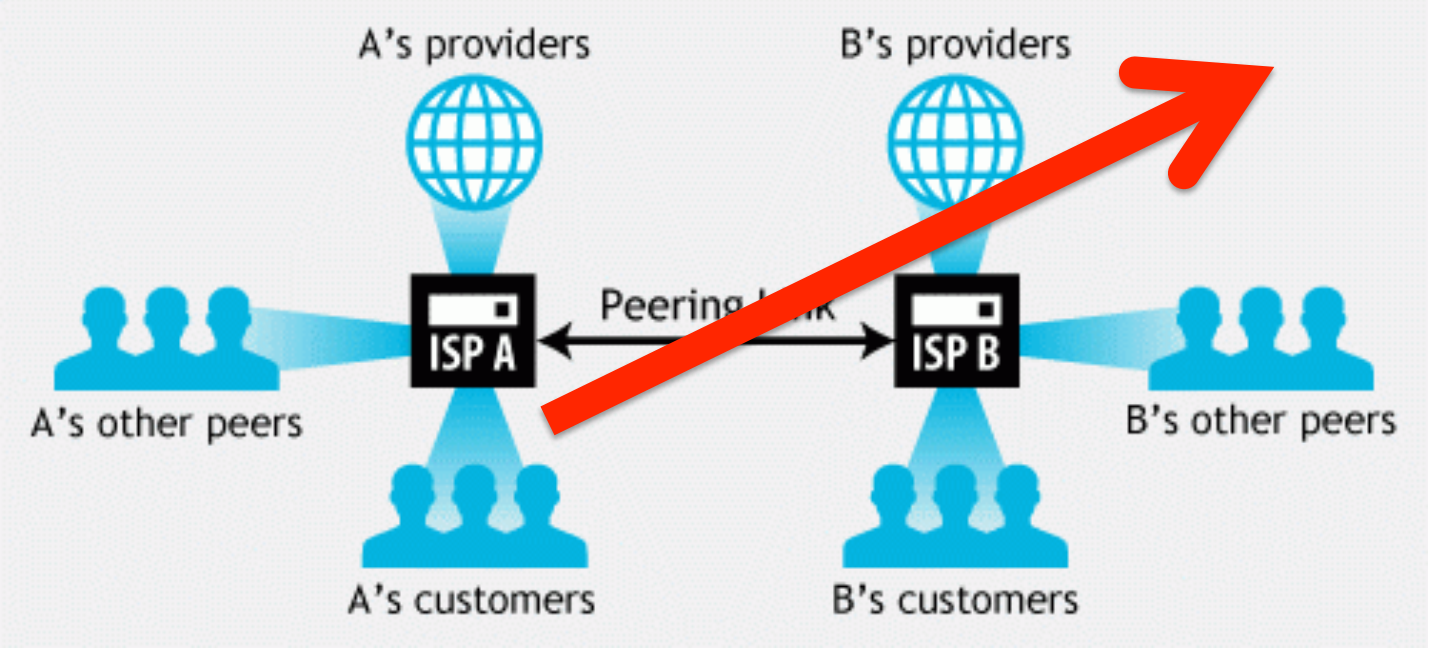
Alternatively, if A accepts B's noncustomer routes, B becomes an "accidental transit provider"

A announces **only its customers** to B

B also sends peer and provider announcements to A

http://research.dyn.com/2014/11/use-protection-if-peering-promiscuously/

Peering - Routing Leak (Scenario 2)



Now B is inserted into the outbound traffic from A to the world

A announces **only its customers** to B

B also sends peer and provider announcements to A

http://research.dyn.com/2014/11/use-protection-if-peering-promiscuously/

Examples: ISPs leaking ISP routes

Vimpelcom (AS3216)- China Telecom (AS4134)

At 10:23 UTC on 5 August 2014:

… {1299, 3257, 1273, …} 4134 3216 … 7k prefixes *(scenario 1)*

… 3216 4134 {2914, 7018, 1239, …} 326k prefixes *(scenario 2)*

http://research.dyn.com/2014/11/chinese-routing-errors-redirect-russian-traffic/

Moscow to New Hampshire.. Via China

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

VimpelCom

中国电信 CHINA TELECOM

Moscow to New Hampshire.. Via China

```
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
```

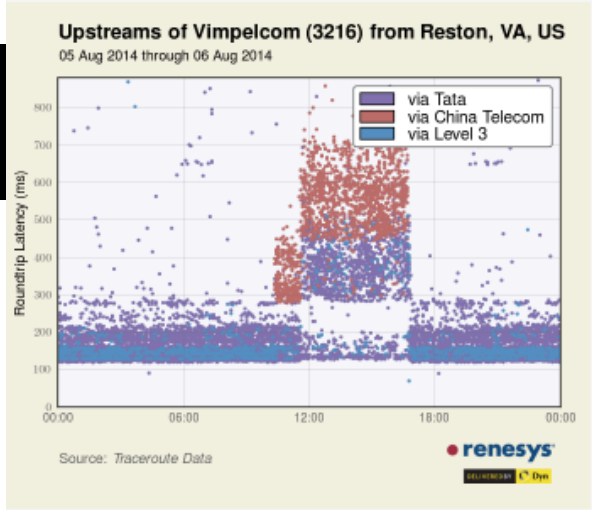
VimpelCom

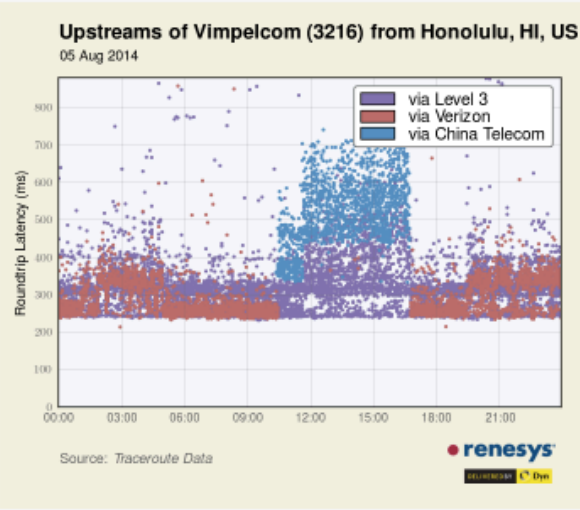
中国电信 CHINA TELECOM

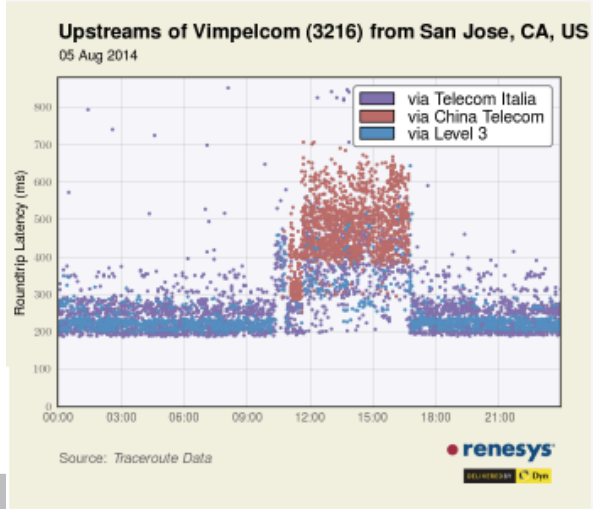
When peers announce peers to peers .. It's a policy breakdown.

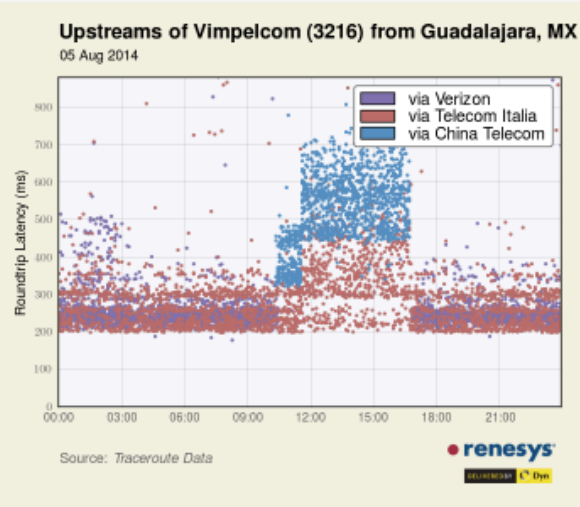
Impacts on Latency

Traffic redirection can significantly affect end user experience … carefully engineered paths are replaced by unexpected detours!









“Peering” not just for ISPs

Leaking content/CDN routes to peers that were meant only for customers?

At 18:15 UTC on 6-Nov-14, Vocus (AS4826, Australia) begins leaking Microsoft (AS12076) routes to large (non-customer) ASNs:

Cogent, HE, PCCW, …

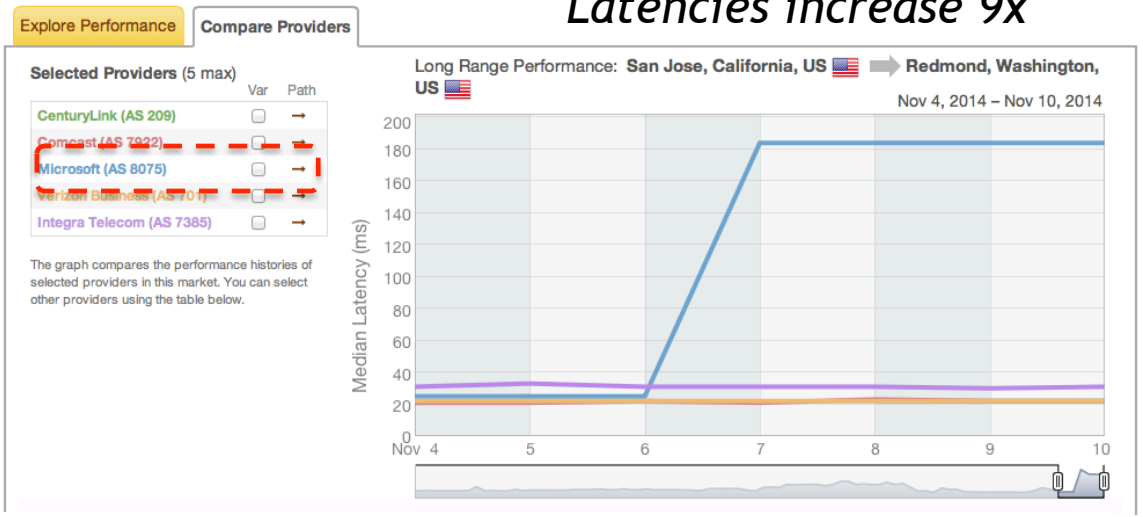
… {174, 6939, 3491,… } 4826 12076 65.52.0.0/14 (& 30 more)

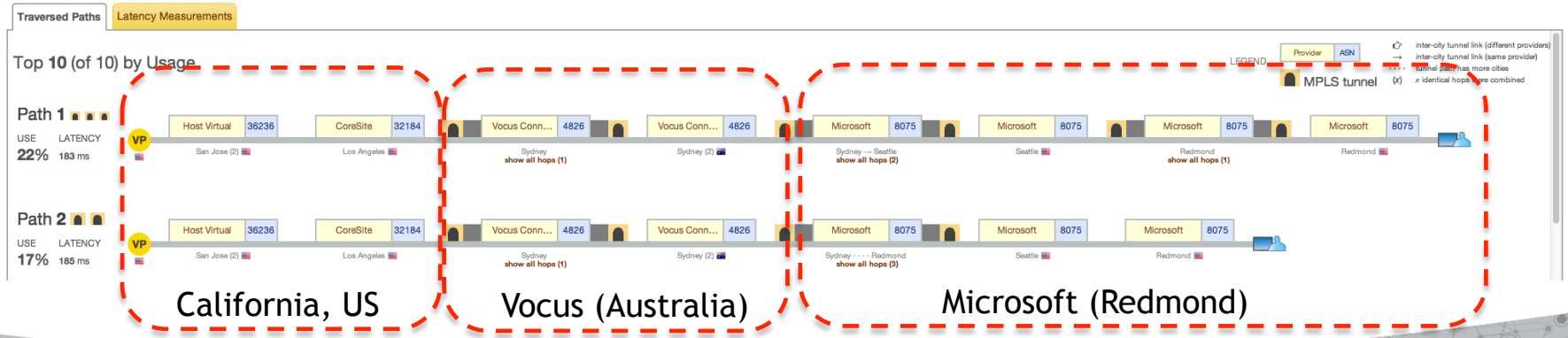
Can you figure out the likely impact?

Long Detours

West Coast USA: traffic paths to content drag to Australia and back for up to 6 days. Who paid?

Latencies increase 9x





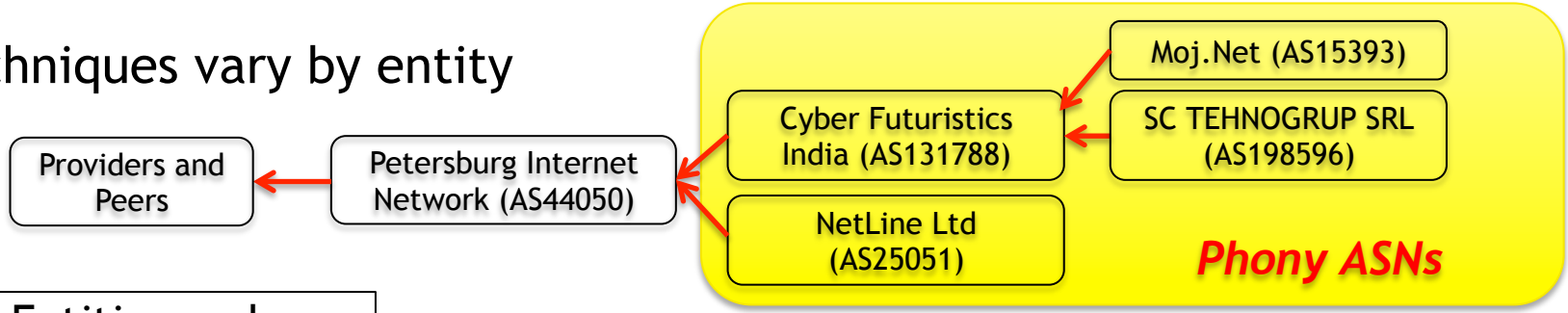
RISK #2

squatting

ON PREVIOUSLY UNROUTED SPACE

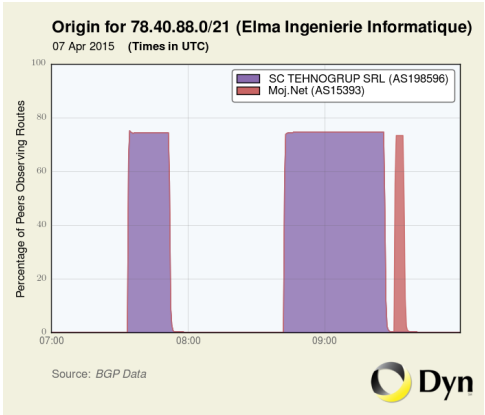
Fradulent Routing of Unused Space

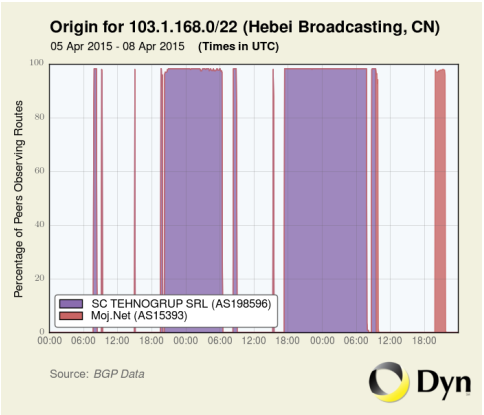
Techniques vary by entity



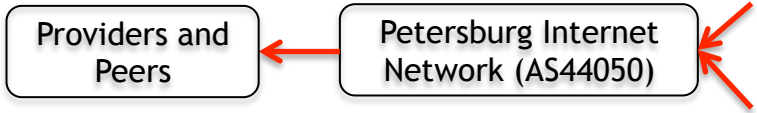
Entities under Petersburg Internet Network (AS44050) rapidly rotate IP address ranges

ASPATHs are synthetic, built from unrelated origin ASNs



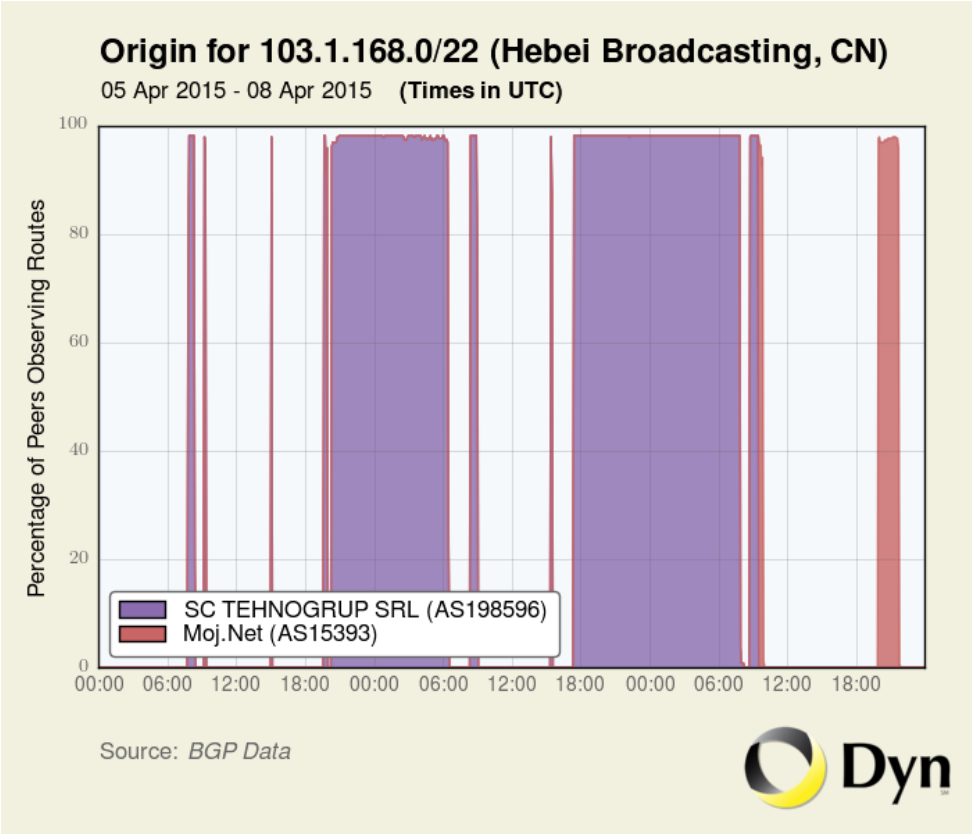


Fradulent Routing



Rapid “flicker” of ASN origination lasting minutes or hours

Origin-based path analysis fails; attacker is 2 ASNs further “upstream”



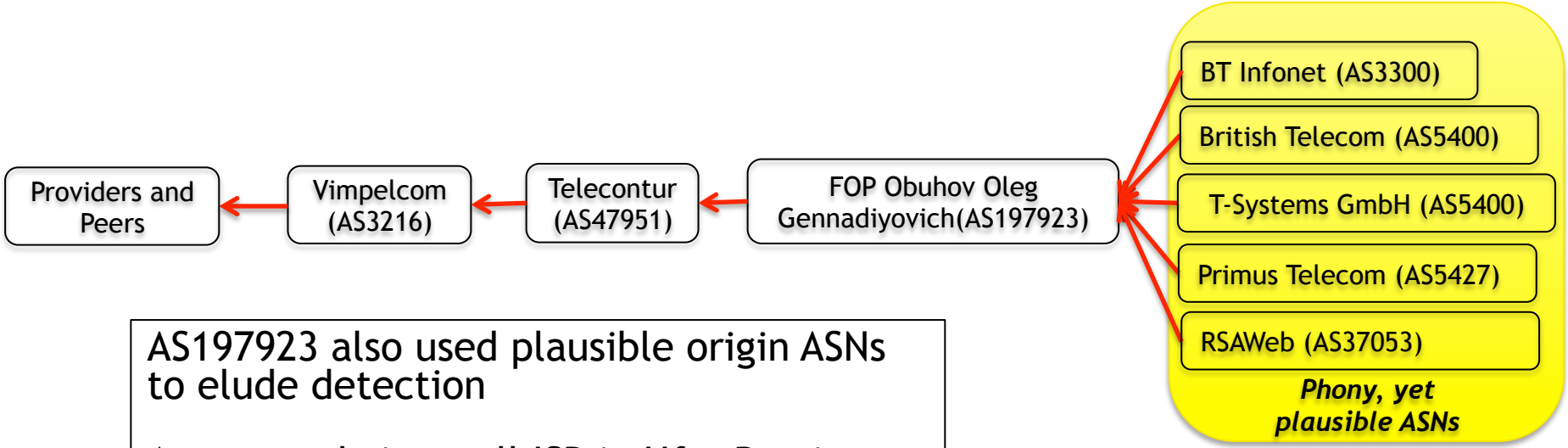
July 2015

Space utilized transiently by Peterburg Internet Network in *one month* of observation

205.142.128.0/22			206.130.224.0/24	Fastman	CA
94.127.72.0/21	Akamai International B.V.		206.130.234.0/24	Marsulex Inc.	CA
91.209.38.0/24	Interglobe LLC	AM	206.130.235.0/24	Marsulex Inc.	CA
185.37.200.0/24	Red Bull Media House GmbH	AT	209.221.119.0/24	York Region District School Board	CA
103.9.162.0/24	DC West Pty Ltd	AU	209.221.126.0/24	York Region District School Board	CA
116.213.3.0/24	Bluecentral Pty Ltd	AU	209.221.66.0/24	York Region District School Board	CA
125.63.131.0/24	Optus Macquarie Park (OCS)	AU	209.221.68.0/24	York Region District School Board	CA
125.63.133.0/24	Optus Macquarie Park (OCS)	AU	209.221.96.0/24	York Region District School Board	CA
125.63.159.0/24	Optus Macquarie Park (OCS)	AU	67.23.142.0/24	Netfirms Inc	CA
125.63.167.0/24	Optus Macquarie Park (OCS)	AU	74.127.198.0/24	Xplornet Communications Inc.	CA
125.63.182.0/24	Optus Macquarie Park (OCS)	AU	74.127.222.0/24	Xplornet Communications Inc.	CA
125.63.183.0/24	Optus Macquarie Park (OCS)	AU	74.127.230.0/23	Xplornet Communications Inc.	CA
125.63.185.0/24	Optus Macquarie Park (OCS)	AU	74.127.252.0/24	Xplornet Communications Inc.	CA
192.232.131.0/24	imported inetnum object for BHCT	AU	185.79.252.0/22	LITECOM AG	CH
202.0.113.0/24	Olex Cables Limited	AU	200.12.132.0/24	Centro de Estudios Cientificos de Santiago.	CL
202.10.249.0/24	FOXTEL Management Pty Ltd	AU	103.1.168.0/22	Hebei Broadcasting•_TV Information Network Corp.•_Ltd	CN
202.61.153.0/24	M2 Telecommunications Group Ltd	AU	103.1.168.0/22	Hebei Broadcasting•_TV Information Network Corp.•_Ltd	CN
203.17.50.0/23	Asia Pacific Network Information Centre	AU	103.22.40.0/22	CHINANET Guangdong province network	CN
203.21.141.0/24	M2 Telecommunications Group Ltd	AU	103.239.184.0/22	Jinhua mili network technology service co.,ltd.	CN
203.214.20.0/24	iiNet Limited	AU	103.245.60.0/22	Beijing Wangliansutong Networks Technology Co. ,Ltd	CN
203.23.51.0/24	Australian Micro Labs	AU	103.32.240.0/22	CE Dongli Technology Co., Ltd., WuXi Branch	CN
203.23.51.0/24	Australian Micro Labs	AU	103.34.36.0/22	Huaihudong (Beijing) Technology Co.,Ltd.	CN
203.25.76.0/24	Newcastle Grammar School Pty Ltd	AU	103.39.204.0/22	China Radio International	CN
203.26.110.0/24	Queensland Teachers Credit Union Ltd	AU	103.48.220.0/22	Beijing Huacheng Tongmao Network Technology Co., Ltd.	CN
203.26.54.0/24	Rhythm Media Pty Ltd	AU	103.50.228.0/22	Hangzhou Yunzan Technology Co.,Ltd.	CN
203.27.112.0/23	TK Net Server	AU	114.28.134.0/24	263 Shanghai Communications Ltd.	CN
203.28.139.0/24	Open Integration Pty Ltd	AU	114.28.187.0/24	Shanghai Information Network Co.,Ltd.	CN
203.28.80.0/24	Alphawest Services Pty Ltd	AU	114.28.202.0/24	263 Shanghai Communications Ltd.	CN
203.6.195.0/24	Reed Elsevier Australia Pty Ltd	AU	114.28.220.0/24	263 Shanghai Communications Ltd.	CN
203.98.79.0/24	Crucial Paradigm Pty Ltd	AU	118.194.30.0/24	Guangxi SeeHu Technology Co., Ltd.	CN
185.26.184.0/22	Eurosel LLC	AZ	202.137.231.0/24	CHINANET FUJIAN PROVINCE NETWORK	CN
200.50.132.0/24	ARIN - American Registry for Internet Numbers	BB	203.148.86.0/23	CHINANET FUJIAN PROVINCE NETWORK	CN
200.50.135.0/24	ARIN - American Registry for Internet Numbers	BB	203.23.47.0/24	CHINANET FUJIAN PROVINCE NETWORK	CN
142.194.119.0/24	Allstream Corp.	CA	203.27.16.0/24	CHINANET FUJIAN PROVINCE NETWORK	CN
142.194.121.0/24	Allstream Corp.	CA	43.227.180.0/22	Hangzhou Aiming Xianfa Network Technology Co.,Ltd.	CN
142.194.126.0/24	Allstream Corp.	CA	43.229.192.0/22	Beijing Linkdata Investment Co.,LTD	CN
142.194.196.0/24	Allstream Corp.	CA	45.114.196.0/22	Da Lian Yi Ding net	CN
142.194.199.0/24	Allstream Corp.	CA	45.123.28.0/22	Dr Peng telecom media group co., LTD., nanning branch	CN
142.194.201.0/24	Allstream Corp.	CA	58.65.232.0/21	CHINANET Guangdong province network	CN
142.194.204.0/24	Allstream Corp.	CA	200.12.170.0/24	Colombiano de Baterias Colbateco S.A. Varta	CO
142.194.216.0/24	Allstream Corp.	CA	193.218.120.0/24	AMEuroTel s.r.o.	CZ
142.194.217.0/24	Allstream Corp.	CA	185.98.56.0/22	Intersolute GmbH	DE
142.194.218.0/24	Allstream Corp.	CA	192.166.254.0/24	Schock GmbH	DE
198.169.130.0/24	EnHansen Information Systems Ltd.	CA	194.113.84.0/22	WARNER MUSIC Group Germany Holding GmbH	DE
198.73.94.0/24	Hayes Dana Inc	CA	194.55.190.0/24	Muenchen Ticket GmbH	DE
199.175.120.0/24	Placer Dome Inc.	CA	91.220.115.0/24	Smeet Communications GmbH	DE
199.43.150.0/24	Rand Technologies Inc.	CA	192.66.186.0/24	DELEGATED BLOCK	DK
199.43.151.0/24	Rand Technologies Inc.	CA	192.98.37.0/24	Keski-Pohjanmaan sairaanhoitopiirin kuntayhtyma	FI
199.71.87.0/24	OCRI	CA	185.81.201.0/24	ASS ORDRE NATIONAL DES MEDECINS	FR
205.151.219.0/24	CSP Foods Ltd	CA	192.33.152.0/24	Institut Francais de Recherche Scientifique pour le	FR
205.207.230.0/24	Hartek Limited	CA	192.33.169.0/24	Institut Superieur d'Informatique et D'Automatique de ...	FR
205.207.240.0/24	Pronexus Inc.	CA	193.56.95.0/24	Conseil General de l'Isere	FR
205.210.131.0/24	SHL Systemhouse/Ottawa Outsourcing Centre	CA	192.171.136.0/24	Natural Environment Research Council (NERC)	GB
194.106.199.0/24	Freepoint Commodities Services Ltd	GB			
194.50.165.0/24	Sky UK Limited	GB			
212.59.67.0/24	Clements Shine Investments Limited	GB			
46.161.42.0/24	leased	GB			
196.10.137.0/24	National Health Insurance Authority Ghana	GH			
202.53.132.0/24	Micro 2000 Ltd.	HK			
103.1.6.0/24	Esoft Technologies Ltd.	IN			
202.131.157.0/24	Karuturi Telecom Pvt Ltd	IN			
202.9.172.0/24	Internet Service Provider	IN			
210.210.0.0/24	SIFY INFRASTRUCTURE	IN			
27.124.51.0/24	NOIDA Software Technology Park Ltd	IN			
185.32.148.0/22	Alsalami Company for Software Engineering & Information ...	IQ			
94.142.192.0/21	TELECOM ITALIA SPARKLE S.p.A.	IT			
103.60.188.0/22	N-WAVE Bldg. 602, 2 Chome-7-19 Nanbanaka, Naniwa-ku,	JP			
117.46.182.0/24	SOFTBANK MOBILE Corp.	JP			
117.46.221.0/24	SOFTBANK MOBILE Corp.	JP			
192.135.89.0/24	Yokogawa System Engineering Corporation	JP			
210.57.6.0/24	Telstra Global Internet Services Network Blocks	JP			
103.2.76.0/22	KangNam CableTV	KR			
185.100.224.0/22	LLP ALMA-TV	KZ			
185.100.224.0/24	LLP ALMA-TV	KZ			
185.100.225.0/24	LLP ALMA-TV	KZ			
185.100.226.0/24	LLP ALMA-TV	KZ			
185.100.227.0/24	LLP ALMA-TV	KZ			
91.212.193.0/24	LLP Company of Processing and Personalization	KZ			
31.184.232.0/23	Virty.io	LU			
200.13.32.0/24		MX			
176.126.82.0/24	TerraTransit AG	NL			
202.36.5.0/24	SPARK NEW ZEALAND TRADING LIMITED	NZ			
210.54.145.0/24	SPARK NEW ZEALAND TRADING LIMITED	NZ			
180.232.1.0/24	Eastern Telecom's DSL-Client	PH			
180.232.11.0/24	Eastern Telecom's DSL-Client	PH			
180.232.12.0/24	Eastern Telecom's DSL-Client	PH			
180.232.16.0/24	Eastern Telecom's DSL-Client	PH			
180.232.160.0/24	Eastern Telecom's IDS-Client	PH			
180.232.171.0/24	Eastern Telecom's IDS-Client	PH			
180.232.179.0/24	Eastern Telecom's IDS-Client	PH			
180.232.195.0/24	Eastern Telecom's IDS-Client	PH			
180.232.196.0/24	Eastern Telecom's IDS-Client	PH			
180.232.206.0/24	Eastern Telecom's IDS-Client	PH			
180.232.208.0/24	Eastern Telecom's IDS-Client	PH			
180.232.214.0/24	Eastern Telecom's IDS-Client	PH			
180.232.224.0/24	Eastern Telecom's IDS-Client	PH			
180.232.241.0/24	Eastern Telecom's IDS-Client	PH			
180.232.50.0/24	Eastern Telecom's DSL-Client	PH			
180.232.59.0/24	Eastern Telecom's DSL-Client	PH			
185.99.104.0/22	Centrum Personalizacji Dokumentow Ministerstwa Spraw ...	PL			
193.84.71.0/24	Rodan Systems S.A.	PL			
81.163.192.0/21	Przedsiebiorstwo Zastosowan Elektroniki "ASK" Pawel Szymonek	PL			
197.157.212.0/22	Airtel Rwanda Ltd.	RW			
94.143.224.0/21	ELECTRONIA COMPANY LTD.	SA			
192.150.72.0/24	Logica AB	SE			
192.165.175.0/24	Telia Mobile	SE			
194.88.254.0/24	Volvohandelns Utvecklings Aktiebolag	SE			
91.198.95.0/24	Benzler Data AB	SE			
128.199.6.0/24	Digital Ocean, Inc.	SG			
58.64.27.0/24	Assign for BuddyBB customers	TH			
58.64.31.0/24	Assign for BuddyBB customers	TH			
195.33.194.0/24	ECZACINET	TR			
195.33.195.0/24	ECZACINET	TR			
195.33.197.0/24	ECZACINET	TR			
195.33.255.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.10.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.12.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.13.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.19.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.22.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.237.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.25.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.27.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.29.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.30.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.31.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.38.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.58.0/24	Superonline Iletisim Hizmetleri	TR			
213.14.86.0/24	Superonline Iletisim Hizmetleri	TR			
213.74.1.0/24	TR-SOL-BB-ADSL-Rezerve	TR			
213.74.33.0/24	Tellcom Anatolia Corporate Voice Block	TR			
213.74.37.0/24	TR-SOL-BB-ADSL-Rezerve	TR			
213.74.62.0/24	TR-SOL-BB-FTTX-Rezerve	TR			
78.135.65.0/24	SH-Customer78	TR			
78.135.67.0/24	SH-Customer78	TR			
78.135.71.0/24	SH-Customer78	TR			
192.72.11.0/24	imported inetnum object for III	TW			
153.112.89.0/24	Volvo Information Technology	US			
205.142.128.0/22		US			
74.121.208.0/21	TWO SIGMA INVESTMENTS, LLC	US			
74.121.208.0/21	TWO SIGMA INVESTMENTS, LLC	US			
45.119.76.0/22	CTC Media Technology Apply Joint Stock Company	VN			
196.10.1.0/24	Business Connexion Communications	ZA			
196.10.232.0/22	Katz International Corporation Ltd	ZA			
196.216.21.0/24	Dedicated Client Hosting Firewall and hosting ranges	ZA			
196.216.22.0/24	Static ADSL allocations -RESERVED.	ZA			
197.221.183.0/24	Sainet DSL Dial Pool	ZA			

Source: Dyn Internet Intelligence

Another Example: “Unused Space”

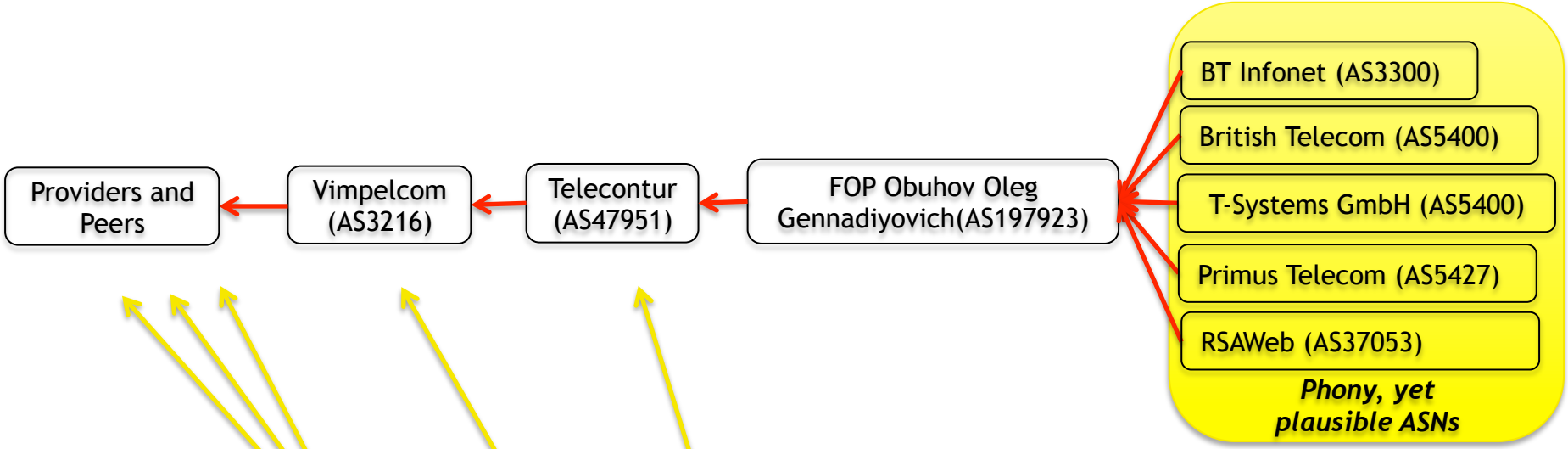


AS197923 also used plausible origin ASNs to elude detection

Announced via small ISP in Ufa, Russia who should have known better

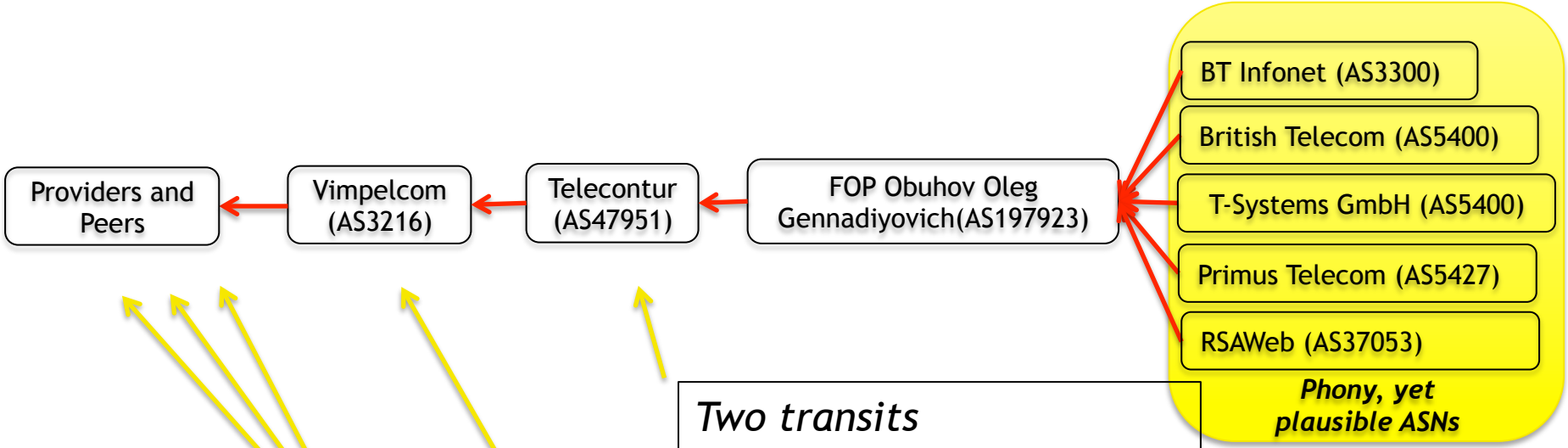
Modified AS path to make AS3300 (BT Infonet) appear to originate unused IP address space registered to BT Infonet

Fradulent Routing of Unused Space

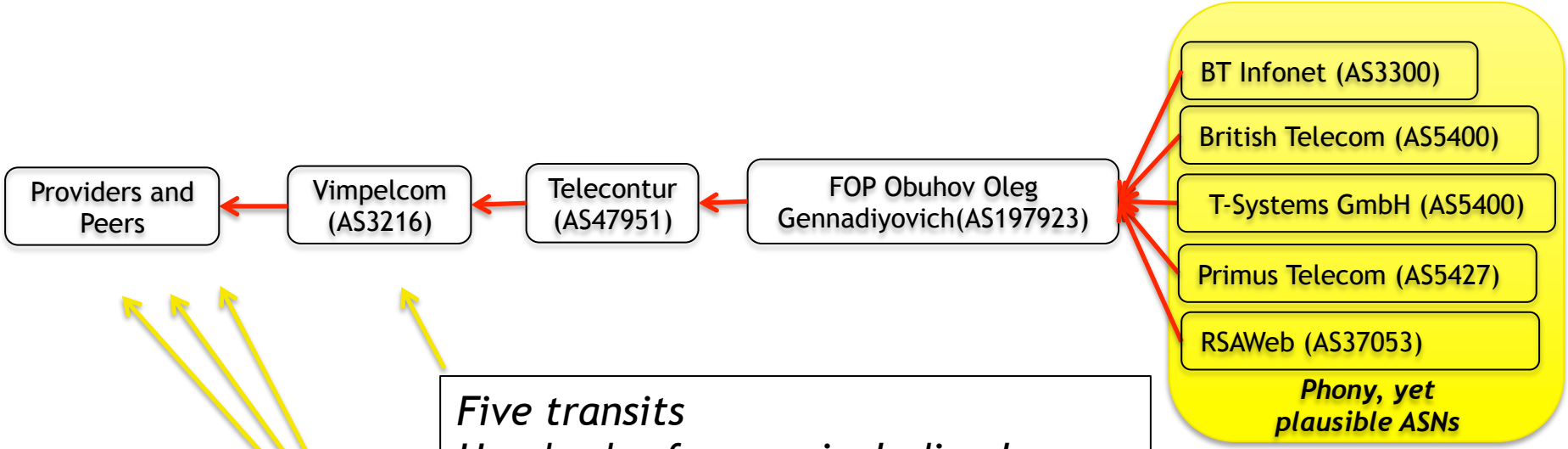


How many chances did we have to block this close to the source?

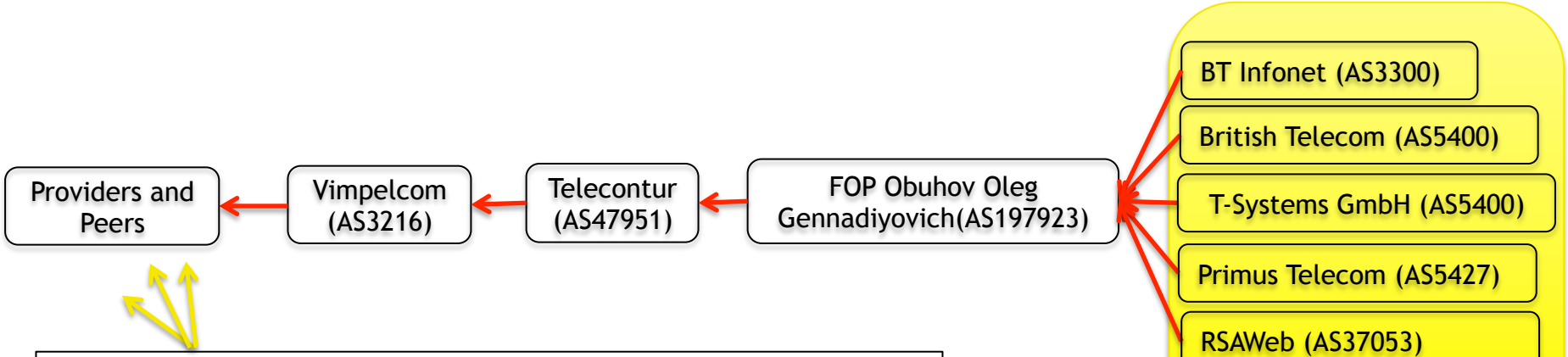
Fradulent Routing of Unused Space



Fradulent Routing of Unused Space



Fradulent Routing of Unused Space



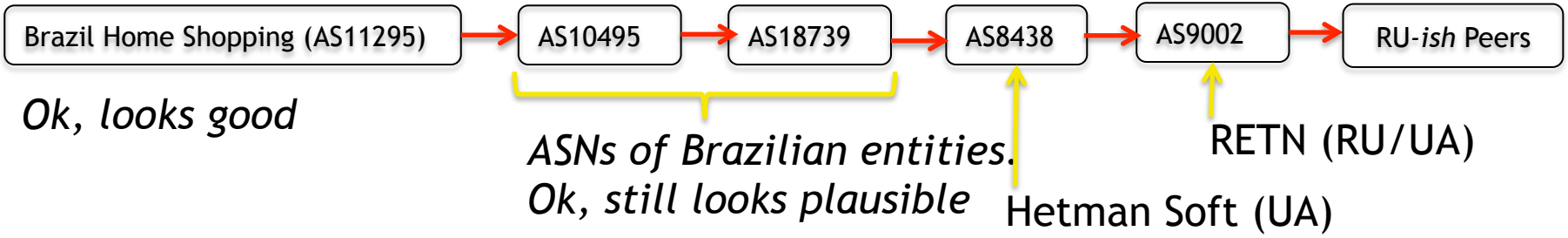
Transitive closure: 50,000+ ASNS

If bad routes escape confinement, they will be widely believed, despite appearing in no route registry anywhere. Worse, plausible but fake ASNs defeat casual inspection of ASPaths

Transregional Effects

- Ufa-based activity disappeared on Nov 5, 2014
- Similar activity began in Ukraine in Dec 2014, currently on-going
- Example: 200.202.64.0/19 (Brazil Home Shopping Ltd)

Currently originated by: ***Exclusively*** transited along following path:



Route circulated only to a limited set of (mostly Russian) carriers

Simulated Routing Reality

- Other examples of routes seen ***exclusively*** along 9002_8438:

Prefix	**Plausible, but Phony Origin**
187.239.0.0/16 (Uninet, MX)	AS8151 (Uninet, MX)
177.90.0.0/16 (Universidade De Sao Paulo, BR)	AS28571 (Univ De Sao Paulo, BR)
200.200.0.0/16 (Embratel, BR)	AS4230 (Embratel, BR)
181.56.0.0/16 (Telmex Colombia, CO)	AS10620 (Telmex Colombia, CO)
161.255.0.0/16 (Movistar (Telcel), VE)	AS6306 (Movistar (Telcel), VE)
177.21.128.0/20 (Netdigit Telecomunicacoes, BR)	AS28245 (Netdigit Telecomunicacoes, BR)
196.3.16.0/20 (Net Uno, C.A., VE)	AS11562 (Net Uno, C.A., VE)
186.189.224.0/20 (FastBee Argentina S.A.)	AS28028 (FastBee Argentina S.A)
186.236.240.0/20 (Prefeitura de Cuiabá, BR)	AS263638 (Prefeitura de Cuiabá, BR)
191.102.224.0/20 (DirecTV Colombia)	AS262928 (DirecTV Colombia)
177.8.80.0/20 (CITE ,BR)	AS52890 (CITE, BR)
... many more	

RISK #3

buying

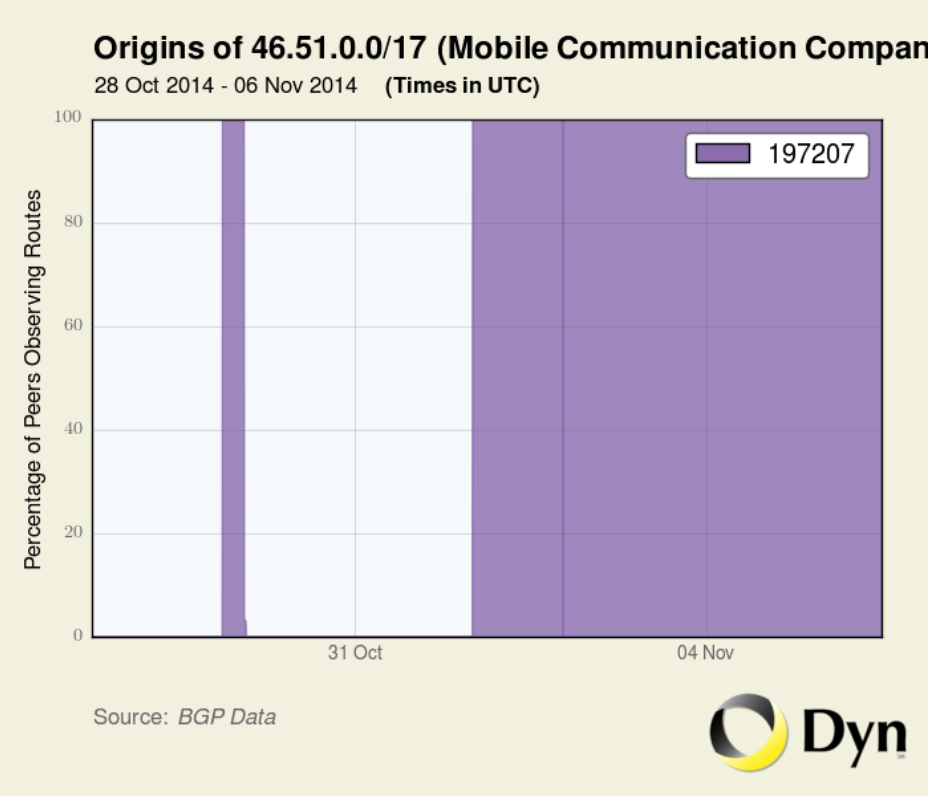
BADLY ROUTED IPv4 SPACE

Address Transfer Markets

Eastern Europe is a major source of new inventory for the IPv4-hungry Middle East

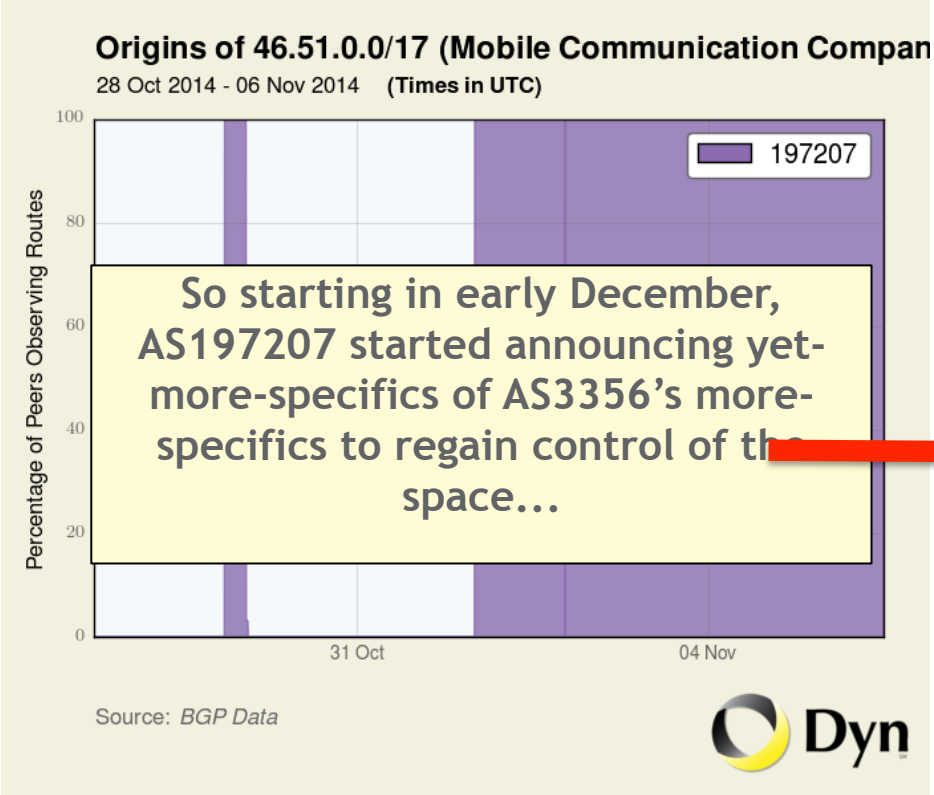
- Official in-region RIPE transfers continue to accelerate
- Interregional transfers coming soon
- Legacy space transfers have been going all along
- $10-$15 per /32 not uncommon

Misroutings affect transfer space

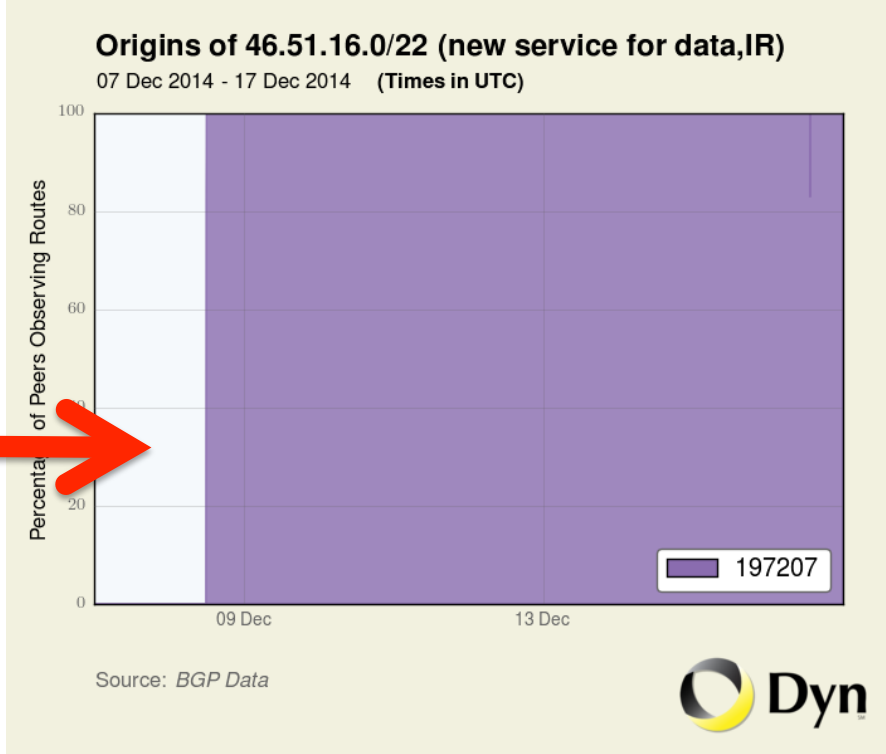


- 27-Oct-2014: 46.51.0.0/17 was transferred from Netserv Consult SRL (RO) to Mobile Communication Company of Iran
- Mobile Communication Company of Iran (AS197207) began announcing the prefix immediately
- **However, Level 3 (AS3356) has announced more-specific prefixes within this range since early 2012**
  - 46.51.16.0/21, 46.51.24.0/21, 46.51.32.0/21, …

Buyers fight to regain control



So starting in early December, AS197207 started announcing yet-more-specifics of AS3356's more-specifics to regain control of the space...

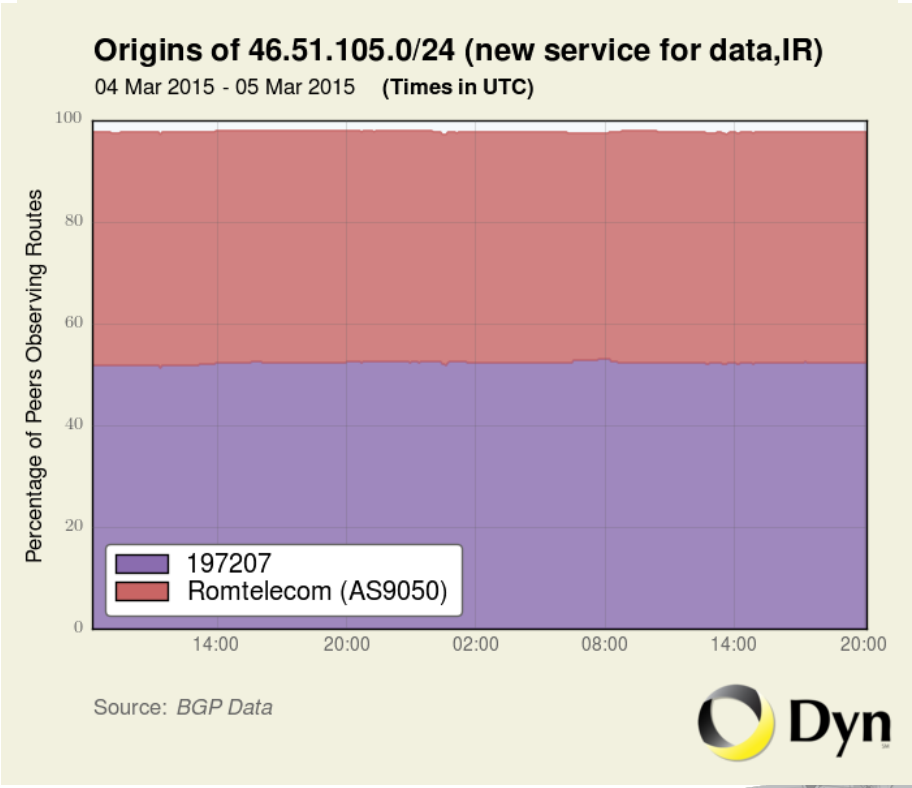


Imperfect “transfer of title”

And then we end up with situations where prefixes are being originated by both the buyer and the seller simultaneously…

Reachability will vary.

Peers and upstreams happily accept and propagate routes from *both*!



Risk #4:

interception

MAN IN THE MIDDLE ATTACKS

Man in the Middle Hijacks

Beltelecom (AS6697)

- Belarus incumbent hijacked multiple entities in February 2013
- Multiple downstream AS origins for hijacked prefixes
- Traceroutes pass only through Beltelecom
- Targeted US financial institutions and Foreign Ministries of numerous governments

http://research.dyn.com/2013/11/mitm-internet-hijacking/

Man in the Middle Hijacks

Dyn

http://research.dyn.com/2013/11/mitm-internet-hijacking/

Man in the Middle Hijacks

```
trace from Helsinki to Ministry of Foreign Affairs of Lithuania
(May 23, 2013)
1   *
2   62.78.114.228   Helsinki, Finland      0.519
3   62.78.111.198   Helsinki, Finland      0.508
4   62.78.107.128   Tampere, Finland       8.669
5   62.78.107.135   Tampere, Finland      14.401
6   62.78.107.51    Tampere, Finland       8.694
7   194.68.123.212  Stockholm, Sweden     21.758
8   217.150.62.234  Moscow, Russia       156.642
9   217.150.62.233  Minsk, Belarus        44.710
10  84.15.6.213     Vilnius, Lithuania    66.443
11  213.226.128.18  Vilnius, Lithuania    66.613
12  195.22.173.222  Ministry of Foreign   68.120
                      Affairs of Lithuania
```

Legitimate route:

… 13194 **24825** 195.22.173.0/24

Ministry of Foreign Affairs of Lithuania

Hijack route:

Beltelecom

… 13194 **6697** 56498 195.22.173.0/24

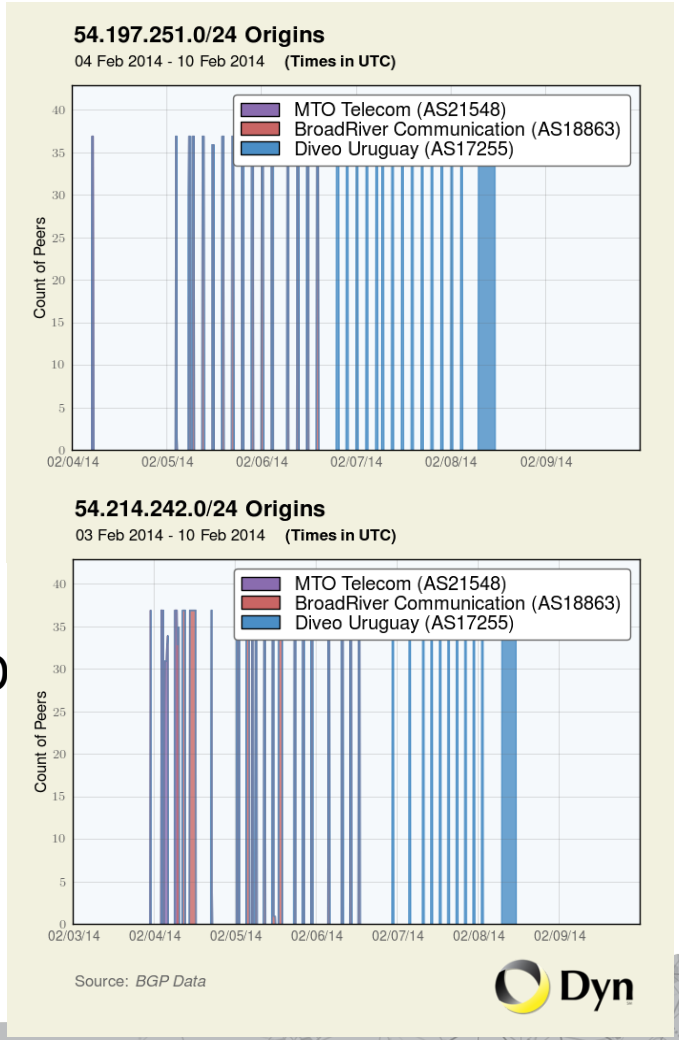
- Hijack route was in circulation for about 1hr
- BGP communities used to deliberately limit propagation to create MITM

http://research.dyn.com/2013/11/mitm-internet-hijacking/

Bitcoin BGP Hijacks

- Prefixes hosting bitcoin mining sites were repeatedly hijacked in Feb 2014
- Amazon, OVH, Digital Ocean targeted
  - 54.197.251.210 useast.middlecoin.com
  - 54.214.242.184 uswest.middlecoin.com
- Hijacked traffic was routed through AS21548 (MTO Telecom) in Montreal
- Attack generated an estimated $80k

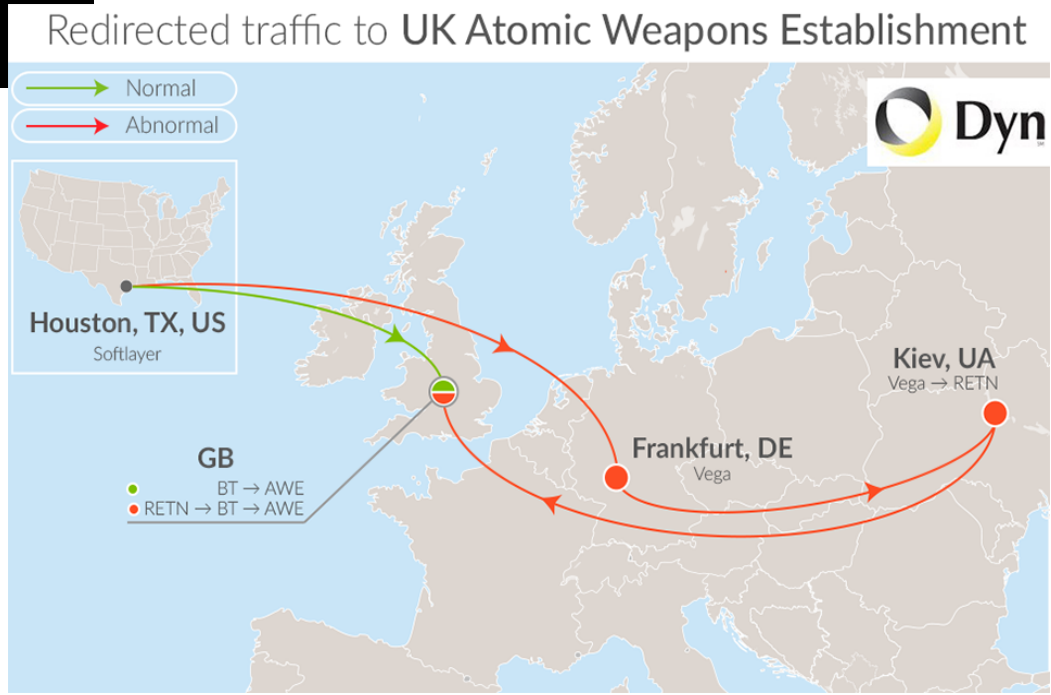
http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/



Innocent Mistake?

Vega Telecom (AS12883)

- Ukrainian reseller of BT services
- Announced 14 BT prefixes for a week, then 167 prefixes for 90 minutes
- Traffic passes through Vega en-route to BT in England



- British organizations affected included the UK Atomic Weapons Establishment (also Walmart and Coca-Cola)

How Does This

happen?

ANSWER: WE LET IT HAPPEN

Improving our MANRS

Expected Actions cover three categories:

1. **Problems related to incorrect routing information;**

2. Problems related to traffic with spoofed source IP addresses; and

3. Problems related to coordination and collaboration between network operators.

https://www.routingmanifesto.org/

Expected Action #1

“Network operator defines a clear routing policy and implements a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.”

Expected Action #2

“Network operator is able to communicate to their adjacent networks which announcements are correct.”

Expected Action #3

“Network operator applies due diligence when checking the correctness of their customer’s announcements, specifically that the customer legitimately holds the ASN and the address space it announces.”

Conclusions

- As IPv4 runs to exhaustion, and address space utilization gets denser and more complex, these “right of routing” issues get more serious.

- Regional and local ISP participation is vitally important, because this gets **exponentially harder** as we try to apply MANRS principles in the Internet core

- The history of leaks and hijacks is, in some sense, a public record. We can tell who did a good job last year.. And who still has some work to do.

QUESTIONS?

Global Routing Incidents

And the Need for Good MANRS

Jim Cowie, Chief Scientist
Doug Madory, Director of Internet Analysis

13 October 2015
Odessa, Ukraine

INTERNET
PERFORMANCE.
DELIVERED.

dyn.com @dyn