Internet Routing Vulnerability

Routing-based Internet Infrastructure Attacks & Manipulations

Doug Madory
Director of Internet Analysis

LACSEC / LACNIC

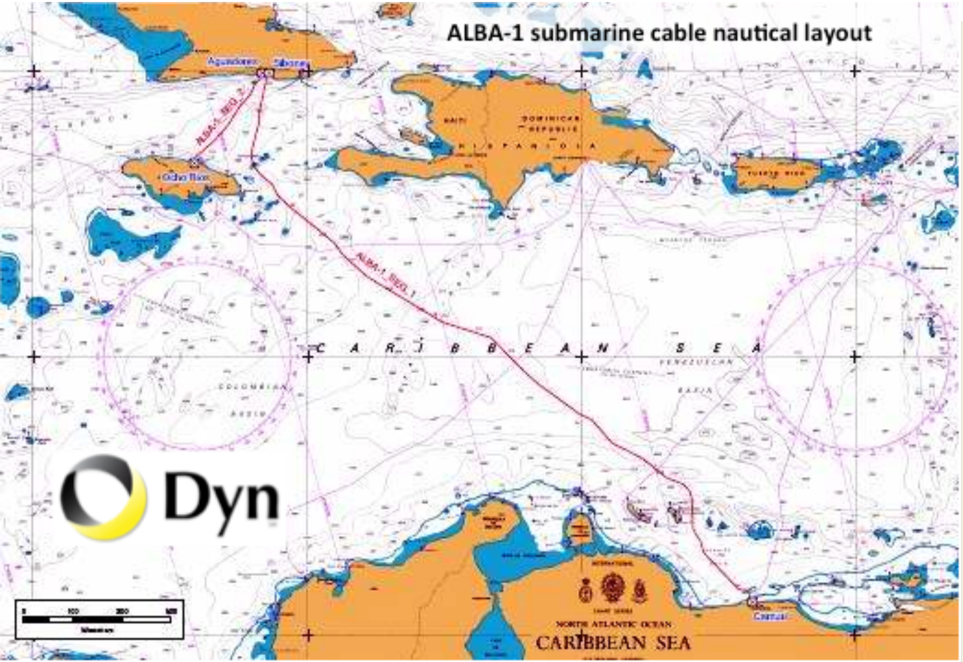
Havana, Cuba *6 May 2016*

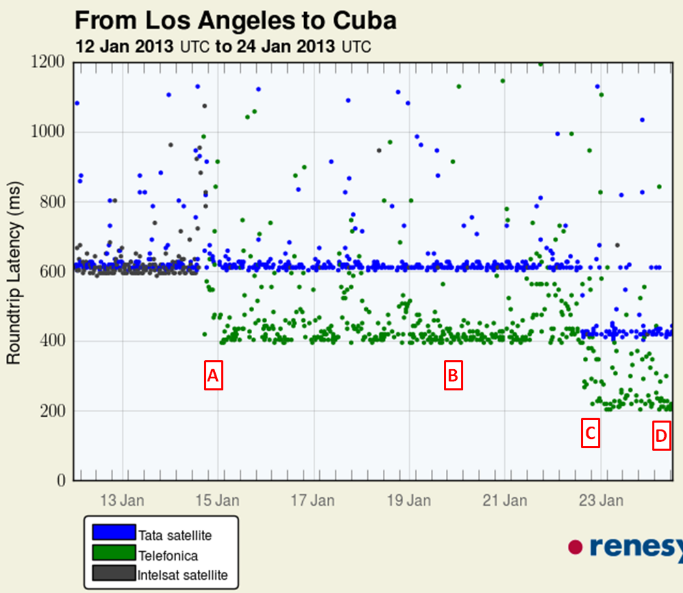
INTERNET
PERFORMANCE.
DELIVERED.

dyn.com @dyn

Discovery of ALBA-1 Activation

- 14 January 2013: ALBA-1 began carrying Internet traffic





A 14 Jan: Renesys first observes use of ALBA-1 in Cuba.

B 20 Jan: Renesys publishes evidence of asymmetric cable use (potential misconfiguration)

C 23 Jan: Renesys publishes data suggesting ETECSA working to resolve misconfiguration.

D 24 Jan: Cuban government confirms Renesys analysis: ALBA is live, but not widely available.

BGP governs movement of Internet traffic

- Single protocol governs traffic exchange among the roughly 50,000+ Autonomous Systems that make up the Internet
- Each AS advertises their own IP networks, or prefixes, to their peers and transit providers

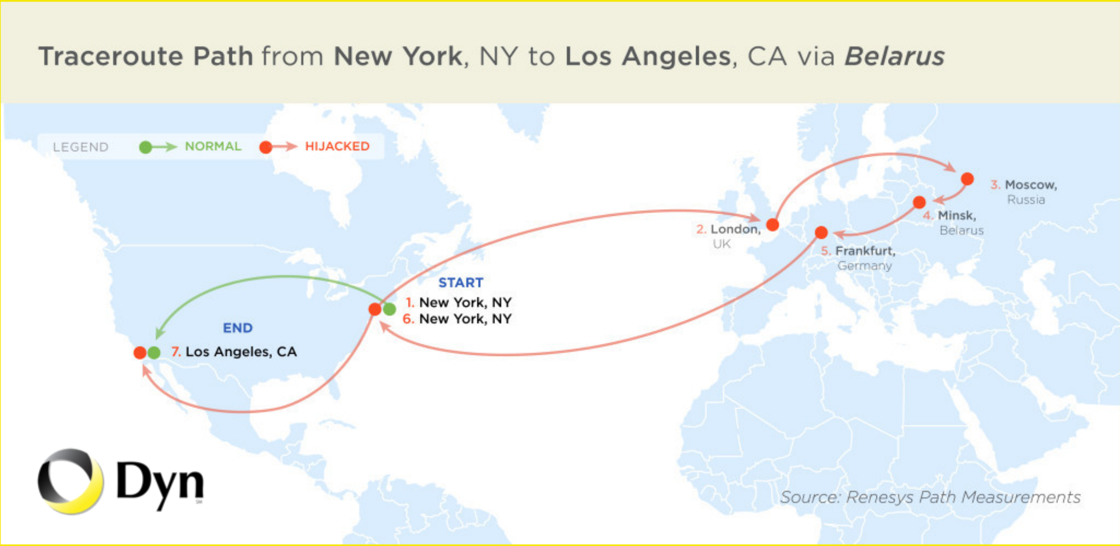
Prefix: 194.123.122.0/24 (256 addresses)
ASNs: AS286 (KPN), AS1103 (SURFnet)

- Each AS independently picks the best route to every prefix on earth *(most specific, then shortest AS path)*
- However, each AS also has the ability to announce any other AS's IP address space!

The system that directs Internet traffic is based on entirely on *trust*

BGP MITM 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



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

Source: Renesys Path Measurements

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

BGP MITM 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

… 20485 **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/

Global routing system can be *(and has been)* manipulated to redirect Internet traffic

Vast World of Fraudulent Routing

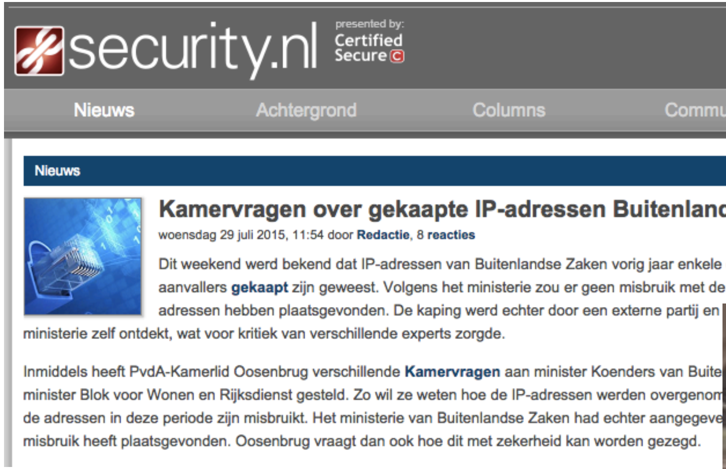
- Numerous entities currently engaged in IP squatting

- Common technique for spam generation, but also used for distribution of malware and botnet CnC

- Obfuscates perpetrator’s true source

- Mostly unused IP space, but sometimes used space

http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/



Kamervragen over gekaapte IP-adressen Buitenlandse Zaken

woensdag 29 juli 2015, 11:54 door Redactie, 8 reacties

Dit weekend werd bekend dat IP-adressen van Buitenlandse Zaken vorig jaar enkele dagen door aanvallers gekaapt zijn geweest. Volgens het ministerie zou er geen misbruik met de gekaapte IP-adressen hebben plaatsgevonden. De kaping werd echter door een externe partij en ministerie zelf ontdekt, wat voor kritiek van verschillende experts zorgde.

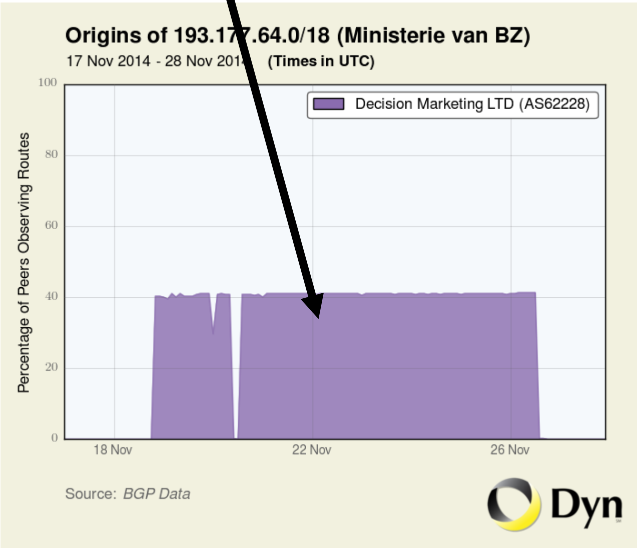
Inmiddels heeft PvdA-Kamerlid Oosenbrug verschillende Kamervragen aan minister Koenders van Buite minister Blok voor Wonen en Rijksdienst gesteld. Zo wil ze weten hoe de IP-adressen werden overgenom de adressen in deze periode zijn misbruikt. Het ministerie van Buitenlandse Zaken had echter aangegeve misbruik heeft plaatsgevonden. Oosenbrug vraagt dan ook hoe dit met zekerheid kan worden gezegd.

Dutch Minister of Foreign Affairs questioned by member of parliament over why their IP space was hijacked.

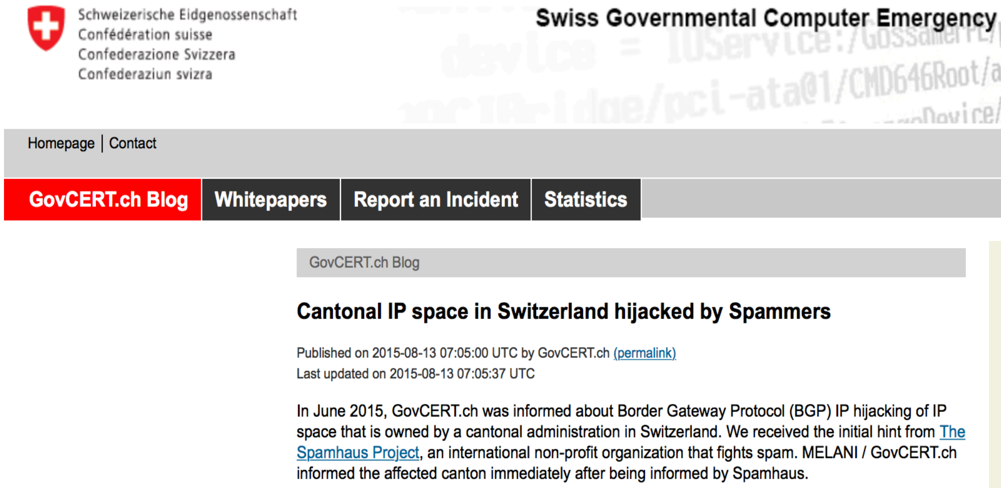
Dutch Minister of Foreign Affairs

Dyn

About 40% of our BGP peers carried this route in their table for about two weeks.



AS62228 announced about 45 routes of mostly unused address space.



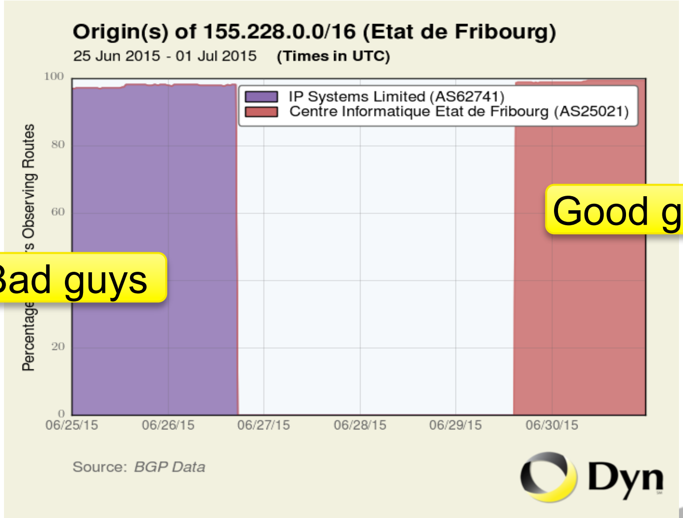
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team

Cantonal IP space in Switzerland hijacked by Spammers

Published on 2015-08-13 07:05:00 UTC by GovCERT.ch (permalink)
Last updated on 2015-08-13 07:05:37 UTC

In June 2015, GovCERT.ch was informed about Border Gateway Protocol (BGP) IP hijacking of IP space that is owned by a cantonal administration in Switzerland. We received the initial hint from The Spamhaus Project, an international non-profit organization that fights spam. MELANI / GovCERT.ch informed the affected canton immediately after being informed by Spamhaus.



Source: *BGP Data*

Bad guys

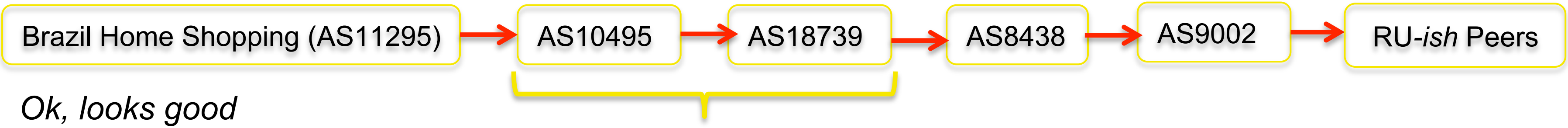
Good guys

- **Improved Technique: Phony, but plausible AS origins used to throw off the scent**
- Previous Russian-based activity (disappeared on Nov 5, 2014)
  - Example: British Telecom address space was originated by British Telecom ASNs (AS5400, AS3300), but routed from Russia
- Similar activity began in Ukraine in December 2014 and is currently on-going

Example: 200.202.64.0/19 (Brazil Home Shopping Ltd)

Originated by:

Exclusively transited along following path:



Brazil Home Shopping (AS11295) → AS10495 → AS18739 → AS8438 → AS9002 → RU-*ish* Peers

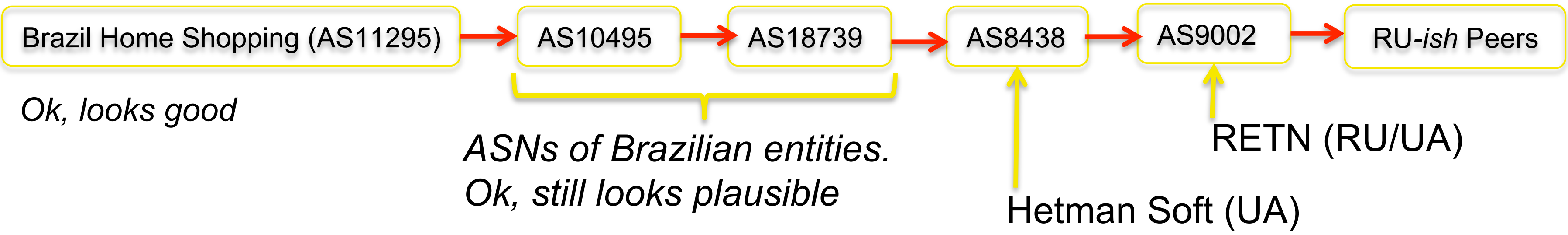
Ok, looks good

ASNs of Brazilian entities.
Ok, still looks plausible

Example: 200.202.64.0/19 (Brazil Home Shopping Ltd)

Originated by:

Exclusively transited along following path:



Brazil Home Shopping (AS11295) → AS10495 → AS18739 → AS8438 → AS9002 → RU-*ish* Peers

Ok, looks good

ASNs of Brazilian entities.
Ok, still looks plausible

Hetman Soft (UA)

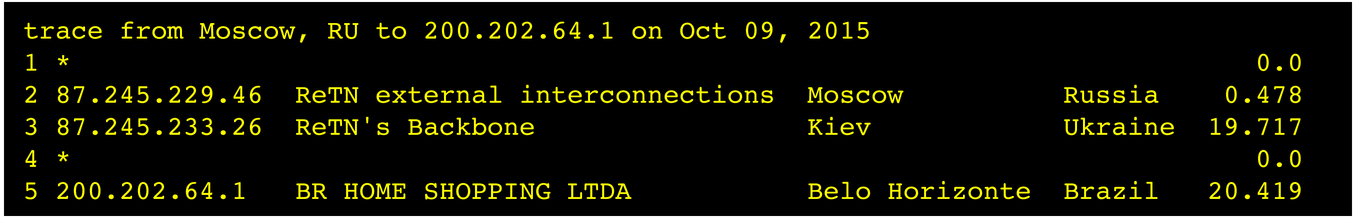
RETN (RU/UA)

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

- What does a traceroute into this space look like?

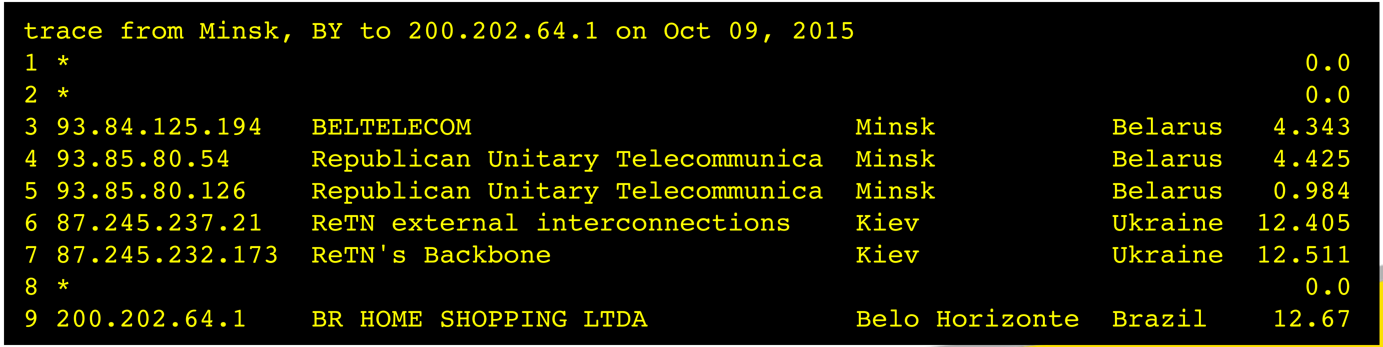
Example: 200.202.64.0/19 (Brazil Home Shopping Ltd)

… 9002 8438 18739 10495 11295 200.202.64.0/19



```
trace from Moscow, RU to 200.202.64.1 on Oct 09, 2015
1 *                                                                        0.0
2 87.245.229.46   ReTN external interconnections  Moscow          Russia    0.478
3 87.245.233.26   ReTN's Backbone                 Kiev            Ukraine  19.717
4 *                                                                        0.0
5 200.202.64.1    BR HOME SHOPPING LTDA           Belo Horizonte  Brazil   20.419
```

20ms from Moscow



```
trace from Minsk, BY to 200.202.64.1 on Oct 09, 2015
1 *                                                                           0.0
2 *                                                                           0.0
3 93.84.125.194    BELTELECOM                       Minsk           Belarus   4.343
4 93.85.80.54      Republican Unitary Telecommunica Minsk           Belarus   4.425
5 93.85.80.126     Republican Unitary Telecommunica Minsk           Belarus   0.984
6 87.245.237.21    ReTN external interconnections   Kiev            Ukraine  12.405
7 87.245.232.173   ReTN's Backbone                  Kiev            Ukraine  12.511
8 *                                                                           0.0
9 200.202.64.1     BR HOME SHOPPING LTDA            Belo Horizonte  Brazil    12.67
```

12ms from Minsk

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

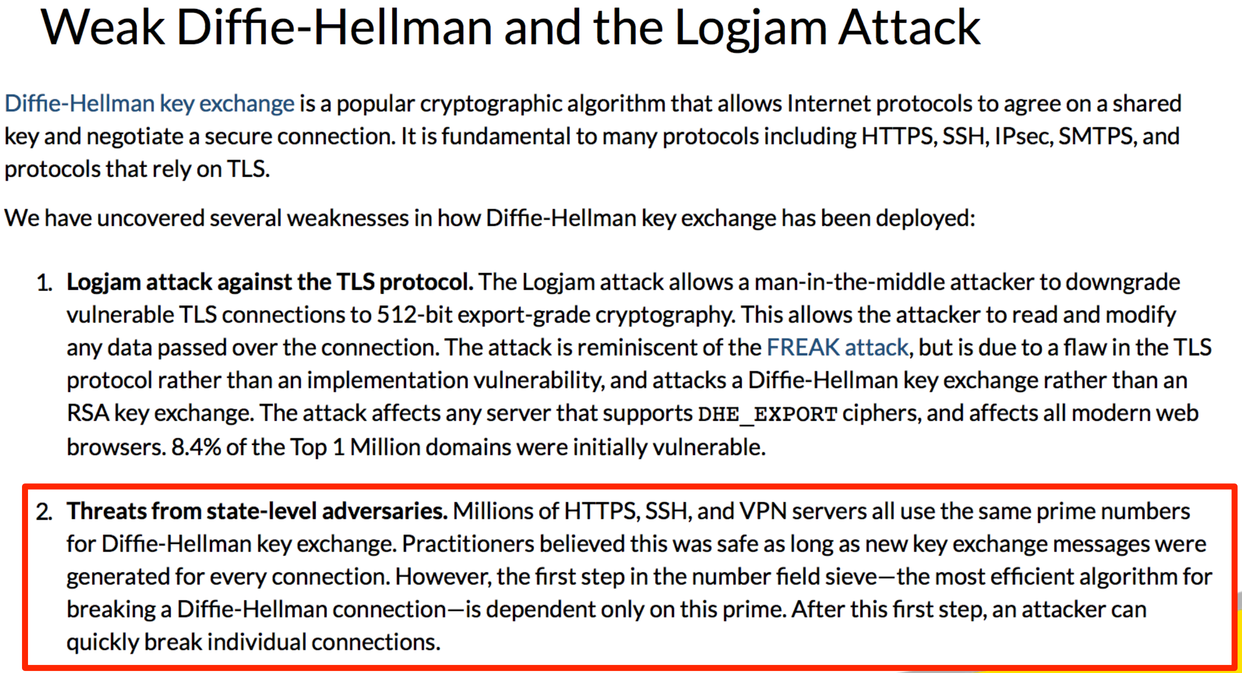
Prefix	Plausible, but Phoney Origin
187.239.0.0/16 (Uninet, MX)	AS8151 (Uninet, MX)
177.90.0.0/16 (Universidade De Sao Paulo, BR)	AS28571 (Univ De Sao Paulo, BR)
200.200.0.0/16 (Embratel, BR)	AS4230 (Embratel, BR)
181.56.0.0/16 (Telmex Colombia, CO)	AS10620 (Telmex Colombia, CO)
161.255.0.0/16 (Movistar (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 (Centro Int. de Telemática do Exército,BR)	AS52890 (Centro Int. de Telemática do Exército,BR)

... many more

With fraudulent routing, IP address-based attribution becomes more difficult

Traffic misdirection also still happening…

- *“But my traffic is all encrypted”*



Weak Diffie-Hellman and the Logjam Attack

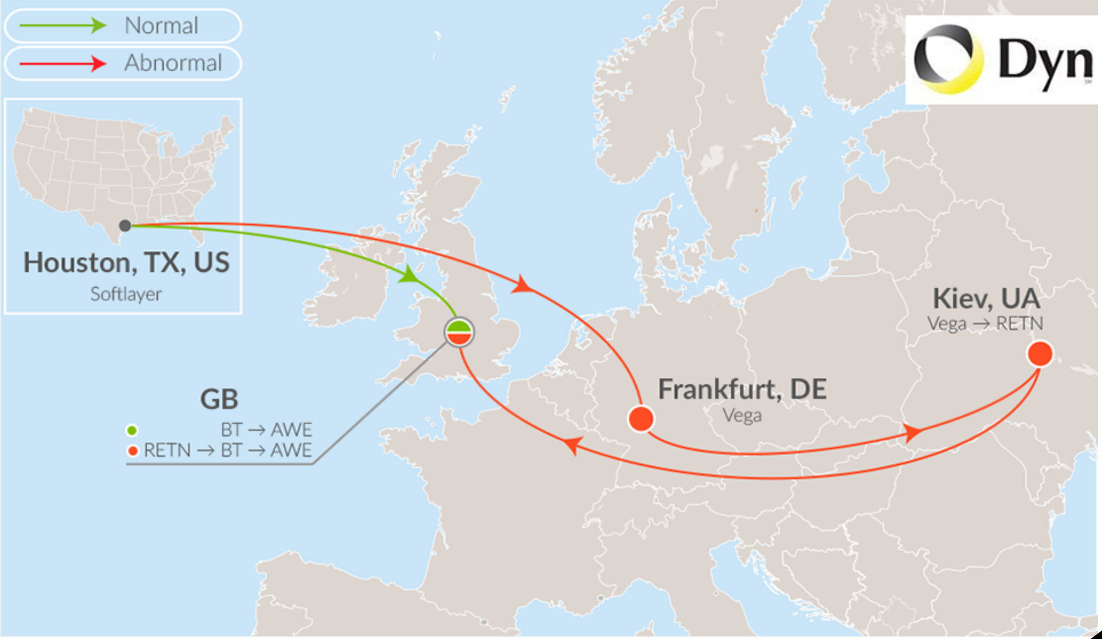
Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, IPsec, SMTPS, and protocols that rely on TLS.

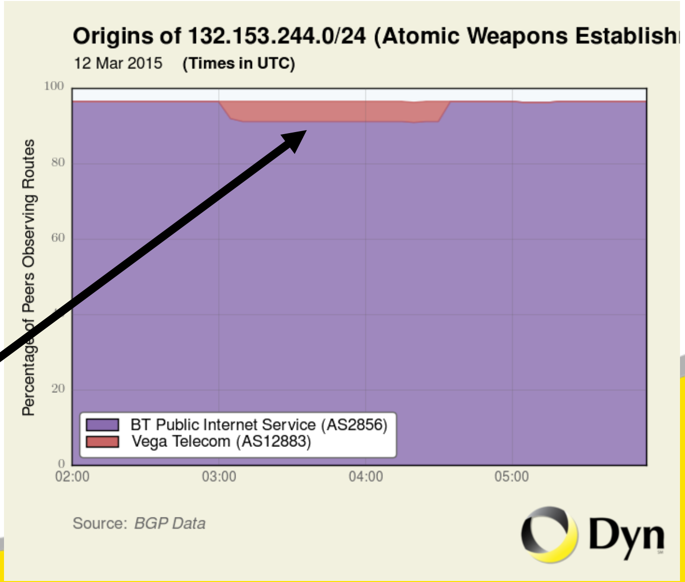
We have uncovered several weaknesses in how Diffie-Hellman key exchange has been deployed:

1. **Logjam attack against the TLS protocol.** The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection. The attack is reminiscent of the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability, and attacks a Diffie-Hellman key exchange rather than an RSA key exchange. The attack affects any server that supports `DHE_EXPORT` ciphers, and affects all modern web browsers. 8.4% of the Top 1 Million domains were initially vulnerable.

2. **Threats from state-level adversaries.** Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections.

Redirected traffic to **UK Atomic Weapons Establishment**

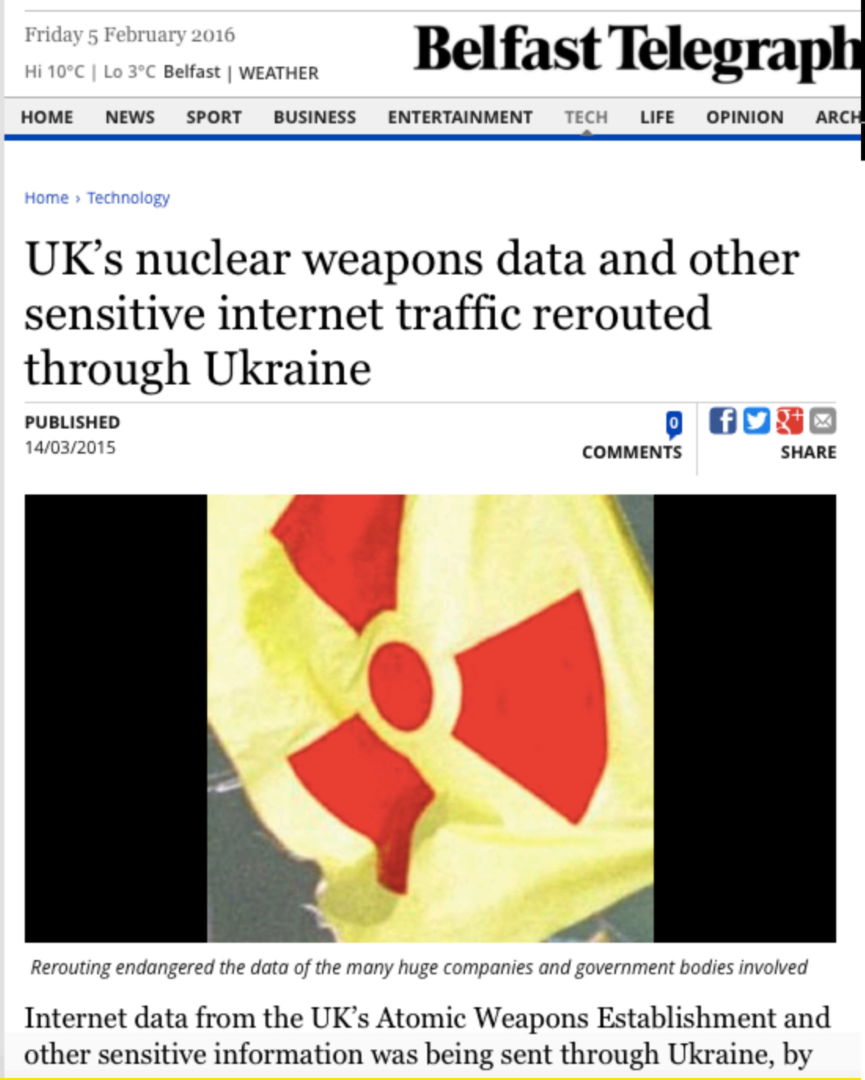



Origins of 132.153.244.0/24 (Atomic Weapons Establish

12 Mar 2015 **(Times in UTC)**

Source: *BGP Data*

About 10% of our BGP peering carried this route in their table for about 1.5 hrs.
Other routes persisted for over a week.



Friday 5 February 2016
Hi 10°C | Lo 3°C Belfast | WEATHER

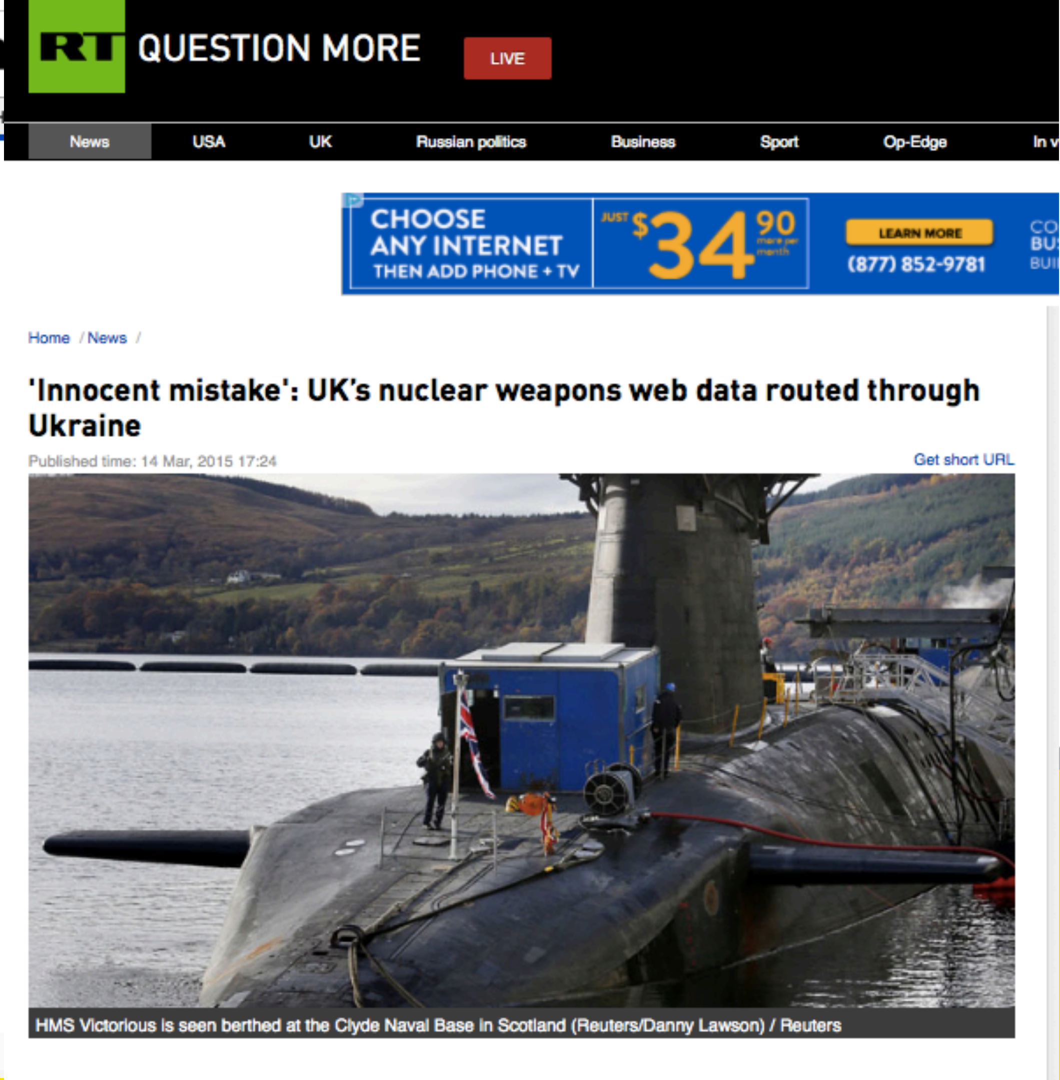
Belfast Telegraph

UK’s nuclear weapons data and other sensitive internet traffic rerouted through Ukraine

PUBLISHED
14/03/2015

Rerouting endangered the data of the many huge companies and government bodies involved

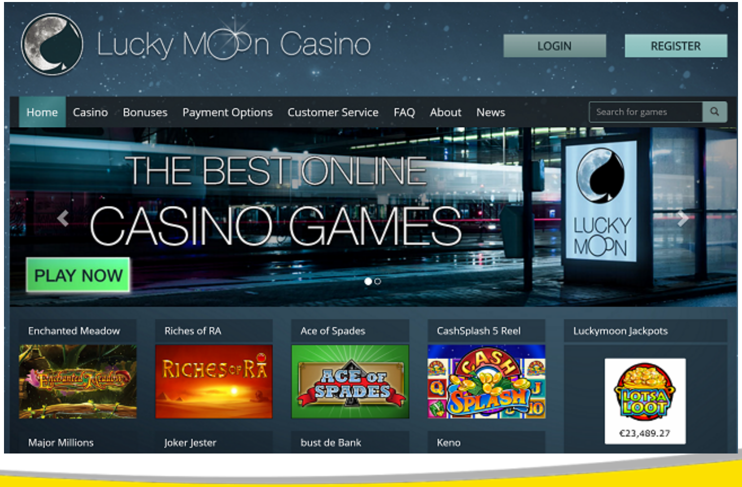
Internet data from the UK’s Atomic Weapons Establishment and other sensitive information was being sent through Ukraine, by



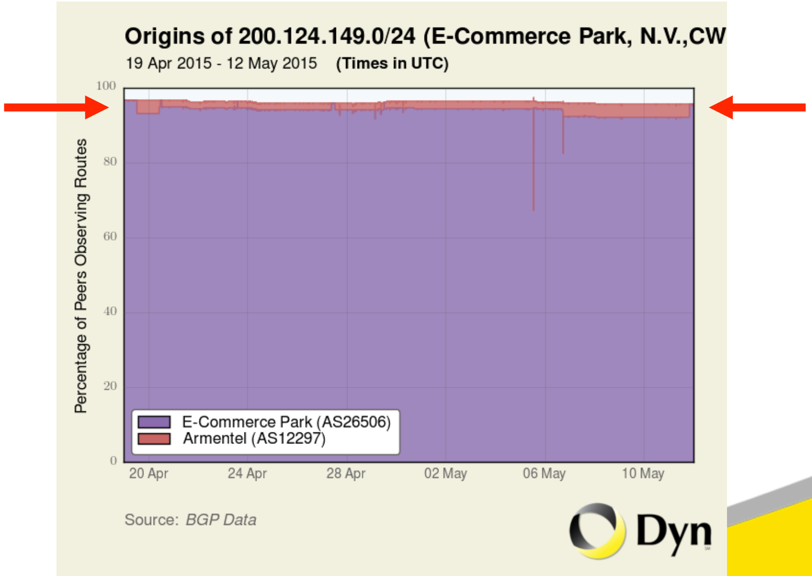
'Innocent mistake': UK's nuclear weapons web data routed through Ukraine

Published time: 14 Mar, 2015 17:24

HMS Victorious is seen berthed at the Clyde Naval Base in Scotland (Reuters/Danny Lawson) / Reuters

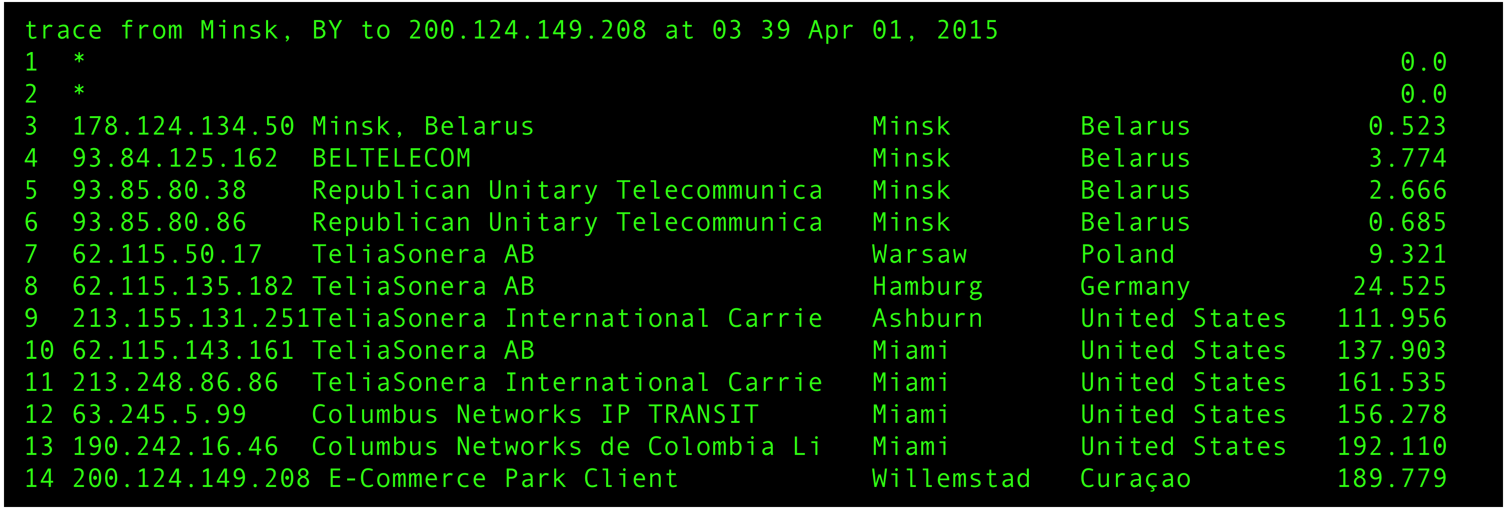


- Less than 10% of our BGP peers carried this route in their table for over 3 weeks.
- Peers accepting this route were mostly in Russia and Eurasia.



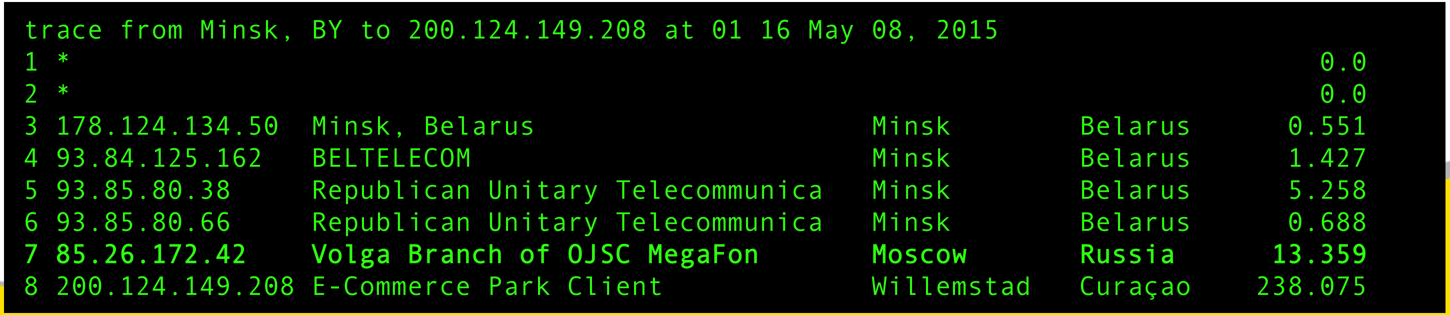
Source: *BGP Data*

- Normal traceroute from Minsk to E-Commerce Park:



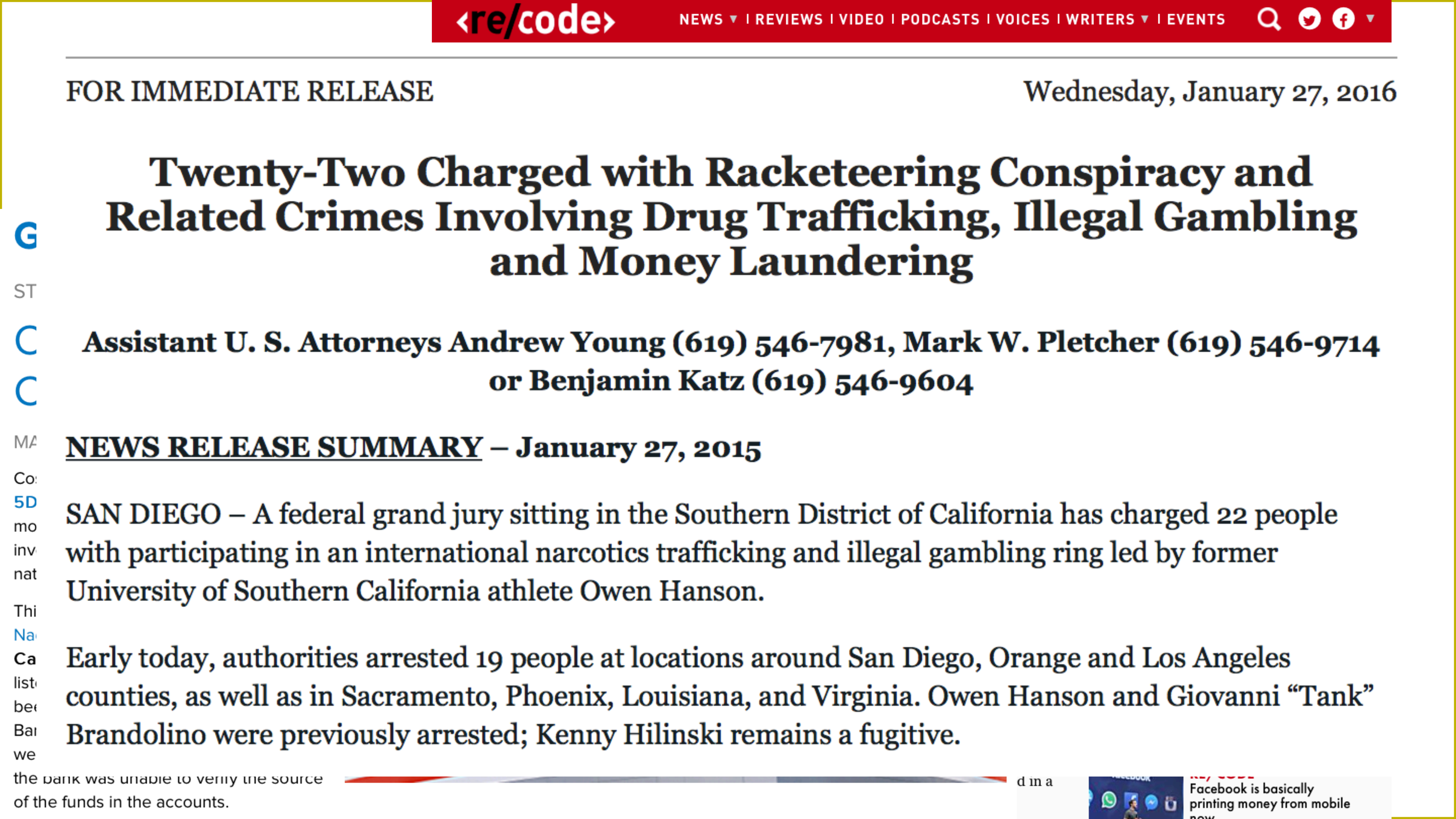
```
trace from Minsk, BY to 200.124.149.208 at 03 39 Apr 01, 2015
1  *                                                                                  0.0
2  *                                                                                  0.0
3  178.124.134.50 Minsk, Belarus                     Minsk        Belarus           0.523
4  93.84.125.162  BELTELECOM                         Minsk        Belarus           3.774
5  93.85.80.38    Republican Unitary Telecommunica   Minsk        Belarus           2.666
6  93.85.80.86    Republican Unitary Telecommunica   Minsk        Belarus           0.685
7  62.115.50.17   TeliaSonera AB                     Warsaw       Poland            9.321
8  62.115.135.182 TeliaSonera AB                     Hamburg      Germany          24.525
9  213.155.131.251TeliaSonera International Carrie   Ashburn      United States   111.956
10 62.115.143.161 TeliaSonera AB                     Miami        United States   137.903
11 213.248.86.86  TeliaSonera International Carrie   Miami        United States   161.535
12 63.245.5.99    Columbus Networks IP TRANSIT       Miami        United States   156.278
13 190.242.16.46  Columbus Networks de Colombia Li   Miami        United States   192.110
14 200.124.149.208 E-Commerce Park Client            Willemstad   Curaçao         189.779
```

- Traceroute during routing hijack:



```
trace from Minsk, BY to 200.124.149.208 at 01 16 May 08, 2015
1 *                                                                              0.0
2 *                                                                              0.0
3 178.124.134.50  Minsk, Belarus                     Minsk        Belarus      0.551
4 93.84.125.162   BELTELECOM                         Minsk        Belarus      1.427
5 93.85.80.38     Republican Unitary Telecommunica   Minsk        Belarus      5.258
6 93.85.80.66     Republican Unitary Telecommunica   Minsk        Belarus      0.688
7 85.26.172.42    Volga Branch of OJSC MegaFon       Moscow       Russia      13.359
8 200.124.149.208 E-Commerce Park Client             Willemstad   Curaçao    238.075
```

New path through Megafon in Moscow


‹re/code›
NEWS ▾ | REVIEWS | VIDEO | PODCASTS | VOICES | WRITERS ▾ | EVENTS

FOR IMMEDIATE RELEASE

Wednesday, January 27, 2016

Twenty-Two Charged with Racketeering Conspiracy and Related Crimes Involving Drug Trafficking, Illegal Gambling and Money Laundering

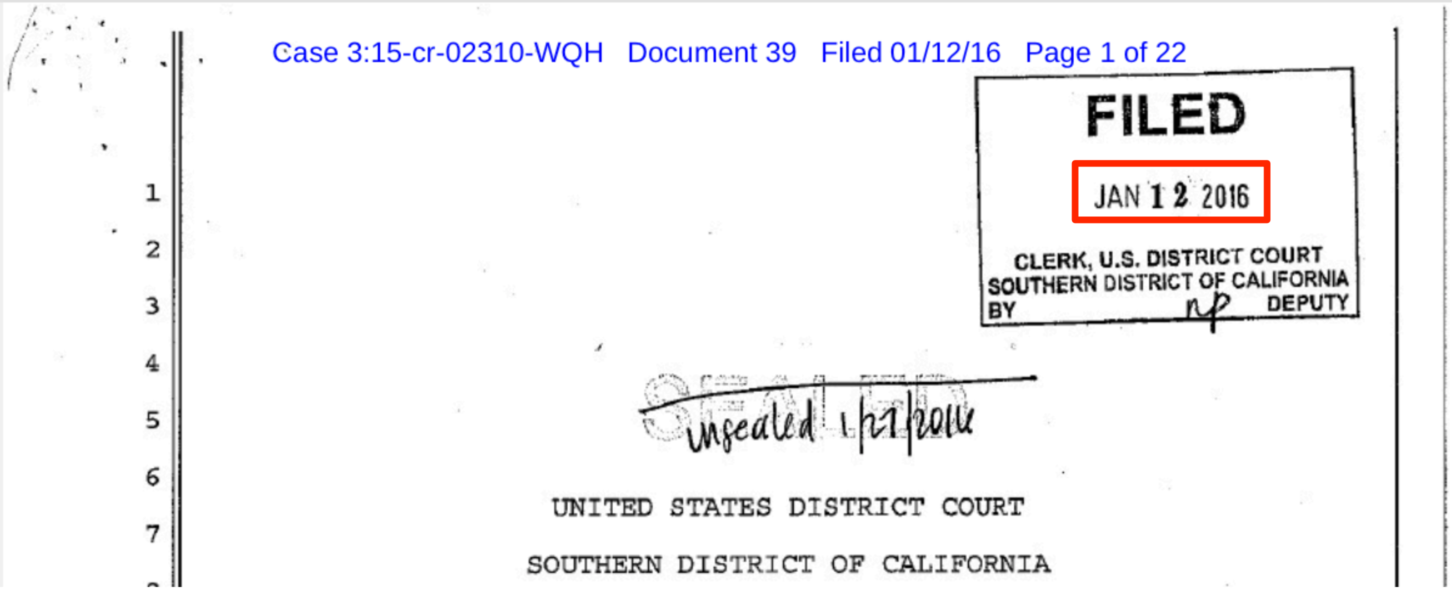
Assistant U. S. Attorneys Andrew Young (619) 546-7981, Mark W. Pletcher (619) 546-9714 or Benjamin Katz (619) 546-9604

NEWS RELEASE SUMMARY – January 27, 2015

SAN DIEGO – A federal grand jury sitting in the Southern District of California has charged 22 people with participating in an international narcotics trafficking and illegal gambling ring led by former University of Southern California athlete Owen Hanson.

Early today, authorities arrested 19 people at locations around San Diego, Orange and Los Angeles counties, as well as in Sacramento, Phoenix, Louisiana, and Virginia. Owen Hanson and Giovanni “Tank” Brandolino were previously arrested; Kenny Hilinski remains a fugitive.

the bank was unable to verify the source of the funds in the accounts.



Case 3:15-cr-02310-WQH Document 39 Filed 01/12/16 Page 1 of 22

FILED

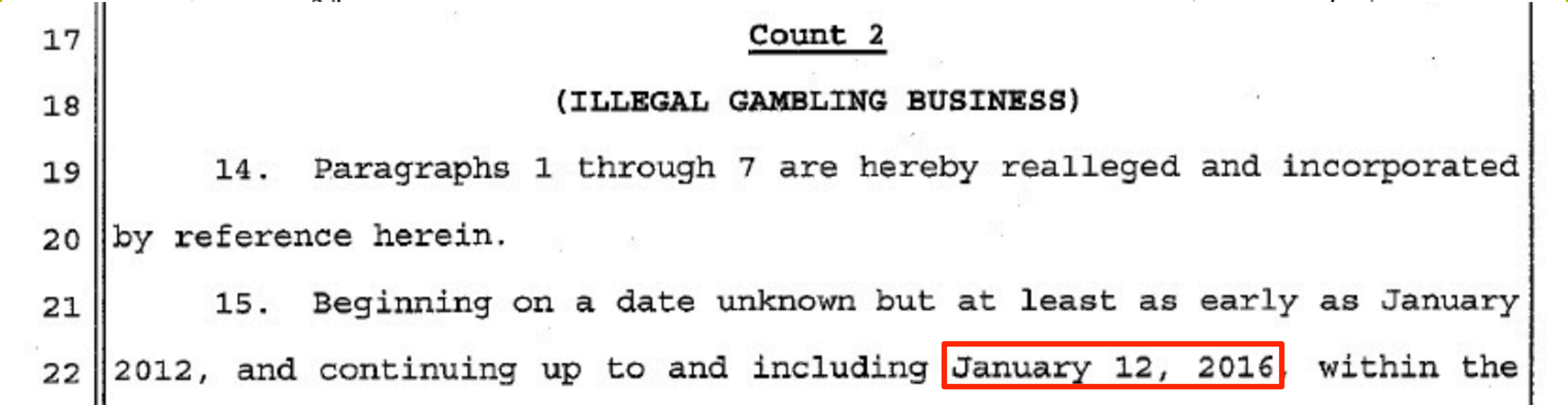
JAN 12 2016

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY np DEPUTY

~~SEALED~~ unsealed 1/21/2016

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA



Count 2

(ILLEGAL GAMBLING BUSINESS)

14. Paragraphs 1 through 7 are hereby realleged and incorporated by reference herein.

15. Beginning on a date unknown but at least as early as January 2012, and continuing up to and including January 12, 2016 within the

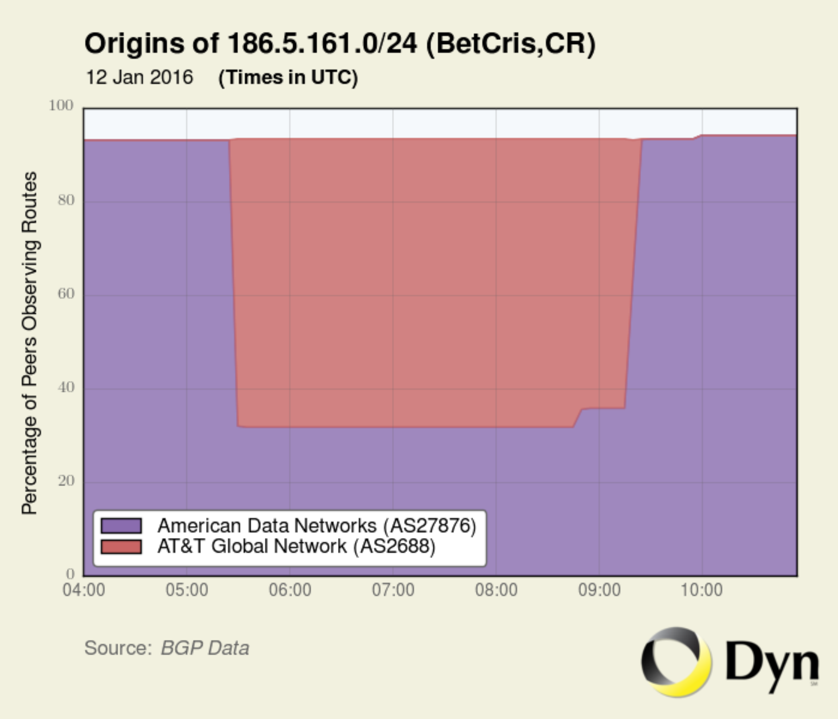
AT&T Hijack of BetCRIS on 12-Jan

BetCRIS

- Online gambling operation
- Hosted in Costa Rica
- Frequent Target of US Law Enforcement

- Route hijacked by AT&T hours before FBI files indictment of ODOG Enterprises
- Traffic redirected to AT&T in Europe

- A simple router misconfig?



Source: *BGP Data*

@DynResearch

- **What to do? No silver bullet.**
- Mutually Agreed Norms for Routing Security (MANRS)
  - Effort by Internet Society
  - Collection of Best Practices for Operators
- Effective route monitoring

Summary

- Global Internet routing is vulnerable to manipulation
- Hijacks and routing errors can (and do) misdirect traffic
- Fraudulent BGP routing occurring at a near constant pace
- Attribution based on IP addresses and reputation based on ASN are not so simple
- Enterprises and ISPs would do well to monitor their routes

THANK YOU!

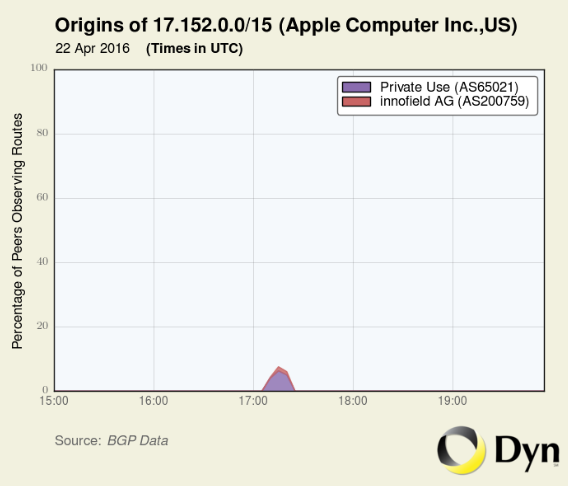
Dyn INTERNET PERFORMANCE. DELIVERED.

Doug Madory

dmadory@dyn.com

@dynresearch

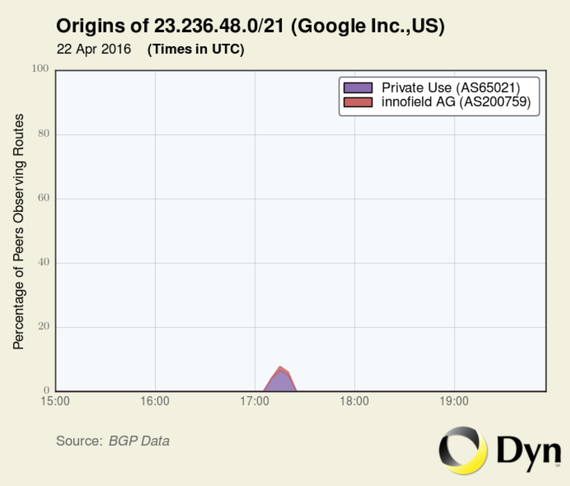
Extra slides



Origins of 17.152.0.0/15 (Apple Computer Inc.,US)

22 Apr 2016 **(Times in UTC)**

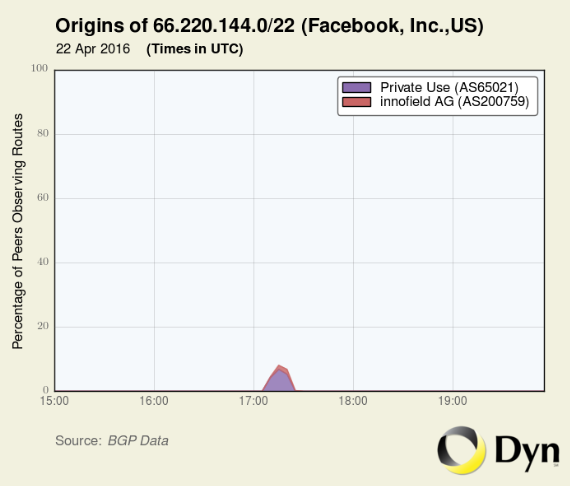
Source: *BGP Data*



Origins of 23.236.48.0/21 (Google Inc.,US)

22 Apr 2016 **(Times in UTC)**

Source: *BGP Data*



Origins of 66.220.144.0/22 (Facebook, Inc.,US)

22 Apr 2016 **(Times in UTC)**

Source: *BGP Data*