Internet Routing Vulnerability

Doug Madory, Director of Internet Analysis, Dyn
Kaspersky Security Analyst Summit
Cancun, Mexico
February 17, 2015
Who we are?

- Analyze global Internet routing and infrastructure
- Renesys acquired by Dyn in May 2014
Dyn’s Measurement Infrastructure

NOTE: Some cities host multiple collectors. Cable Map credit: Telegeography

dyn.com
BGP governs movement of Internet traffic

• 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

• However, each AS also has the ability to announce any other AS’s IP address space!

Why Is It Taking So Long to Secure Internet Routing?
http://queue.acm.org/detail.cfm?id=2668966
BGP MITM hijacks

- **Beltelecom (AS6697)**
  - Belarus incumbent
  - 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/
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

Traffic misdirection also due to routing errors

Peering - Normal Behavior

- ISP A & ISP B peer
- ISP A sends announcements from only its customers to ISP B
- ISP B sends announcements from ISP A to only its customers

Peering - Routing Leak (Scenario 1)

- ISP A & ISP B peer
- ISP A sends announcements from only its customers to ISP B
- ISP B sends announcements from ISP A to its peers and/or providers

ISP B is inserted into inbound traffic to ISP A
Peering - Routing Leak (Scenario 2)

- ISP A & ISP B peer
- ISP B sends announcements from its peers and/or providers to ISP A

ISP B is inserted into **outbound** traffic **from** ISP A
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)
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

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.
Redirecting traffic through a faraway ISP can have big impacts on latency.
Examples: ISPs leaking CDN routes

No one is immune

At 18:15 UTC on 6-Nov-14, Vocus (AS4826) begins leaking Microsoft (AS12076) routes:

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

Condition persisted for 6 days
San Jose to Microsoft (Redmond) redirected through Australia
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

Vast World of Fraudulent Routing

- Techniques vary by entity
  - AS198596 rapidly rotates different IP address ranges
  - AS197426 continuously announces for days on end
  - AS197923 used plausible origin ASNs to elude detection
    - Modified AS path to make AS3300 (BT Infonet) appear to originate unused IP address space registered to BT Infonet
Summary

1. Global Internet routing is vulnerable to manipulation
2. Hijacks and routing errors can misdirect traffic
3. Fraudulent BGP routing occurring at a near constant pace
4. Attribution based on IP addresses and reputation based on ASN are not so simple
5. Enterprises and ISPs would do well to monitor their routes
Thank you!

Doug Madory
dmadory@dyn.com
@dynresearch