The New Threat: Targeted Internet Traffic Misdirection

Nov 19, 2013 // Jim Cowie

Traffic interception has certainly been a hot topic in 2013. The world has been focused on interception carried out the old fashioned way, by getting into the right buildings and listening to the right cables. But there's actually been a significant uptick this year in a completely different kind of attack, one that can be carried out by anybody, at a distance, using Internet route hijacking.

After consultations with many of the affected parties, we're coming forth with some details in the hope that we can make this particular vulnerability obsolete.

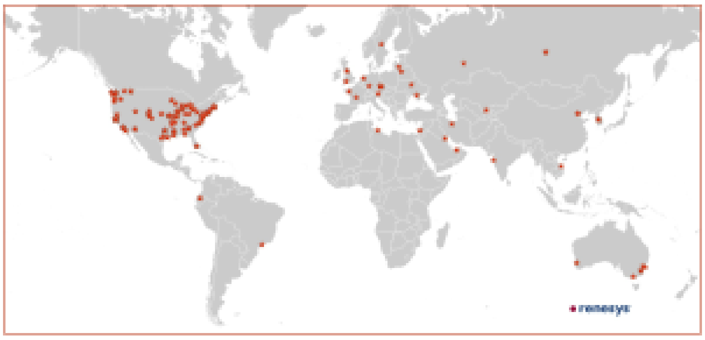
Understanding the Threat

At Renesys, we watch the Internet 24/7 for our enterprise customers, to help them understand and respond to Internet impairment before it affects their businesses. Many of those impairments are the result of someone else's well-intended Internet traffic engineering. Some are accidents, like cable cuts or natural disasters, and that's what you typically see us blog about. But a number of Internet impairments are hard to explain by blind chance or bad luck, and that's our focus today.

For years, we’ve observed that there was potential for someone to weaponize the classic Pakistan-and-Youtube style route hijack. Why settle for simple denial of service, when you can instead steal a victim’s traffic, take a few milliseconds to inspect or modify it, and then pass it along to the intended recipient?

This year, that potential has become reality. We have actually observed live Man-In-the-Middle (MITM) hijacks on more than 60 days so far this year. About 1,500 individual IP blocks have been hijacked, in events lasting from minutes to days, by attackers working from various countries.

Simple BGP alarming is *not* sufficient to distinguish MITM from a generic route hijacking or fat-finger routing mistake; you have to follow up with active path measurements while the attack is underway in order to verify that traffic is being simultaneously diverted and then redelivered to the victim. We’ve done that here.



Here’s a map of 150 cities in which we’ve observed at least one victim of a validated MITM route hijacking attack so far this year (click to inspect). The victims have been diverse: financial institutions, VoIP providers, and world governments have been prominent targets.

What makes a Man-in-the-Middle routing attack different from a simple route hijack? Simply put, the traffic keeps flowing and everything looks fine to the recipient. The attackers keep at least one outbound path clean. After they receive and inspect the victim's traffic, they release it right back onto the Internet, and the clean path delivers it to its intended destination. If the hijacker is in a plausible geographic location between the victim and its counterparties, they should not even notice the increase in latency that results from the interception. It's possible to drag specific Internet traffic halfway around the world, inspect it, modify it if desired, and send it on its way. Who needs fiberoptic taps?

It's even possible to see these attacks as they are occurring, if you have the right global measurement infrastructure. Renesys maintains a realtime view of the Internet from hundreds of independent BGP vantage points. We have to, because that's how we can detect evidence of Internet impairment worldwide, even when that impairment is localized. We also maintain an active measurement infrastructure that sends out billions of measurement packets each day, crisscrossing the Internet in search of impaired or unusual paths like these. Finally, we have a distributed realtime-taskable measurement system that allows us to trigger quick measurements from all over the planet when trouble is detected in a region, so that we can immediately evaluate its significance.

Example 1: Belarusian Traffic Diversion

In February 2013, we observed a sequence of events, lasting from just a few minutes to several hours in duration, in which global traffic was redirected to Belarusian ISP GlobalOneBel. These redirections took place on an almost daily basis throughout February, with the set of victim networks changing daily. Victims whose traffic was diverted varied by day, and included major financial institutions, governments, and network service providers. Affected countries included the US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran.

We recorded a significant number of live traces to these hijacked networks while the attack was underway, showing traffic detouring to Belarus before continuing to its originally intended destination.

Here's an example of a trace from Guadalajara, Mexico to Washington, DC that goes through Moscow and Minsk. Mexican provider Alestra hands it to PCCW for transit in Laredo, Texas. PCCW takes it to the Washington, DC metro area, where they would normally hand it to Qwest/Centurylink for delivery.

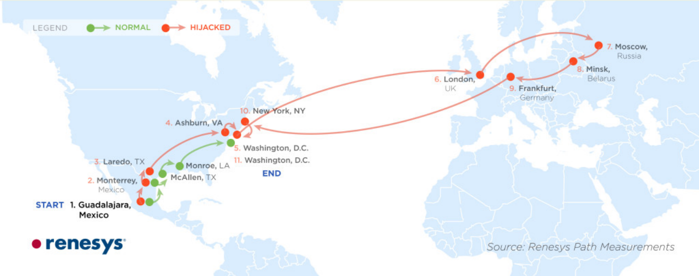
Instead, however, PCCW gives it to Level3 (previously Global Crossing), who is advertising a false Belarus route, having heard it from Russia's TransTelecom, who heard it from their customer, Belarus Telecom. Level3 carries the traffic to London, where it delivers it to Transtelecom, who takes it to Moscow and on to Belarus. Beltelecom has a chance to examine the traffic, and then sends it back out on the "clean path" through Russian provider ReTN. ReTN delivers it to Frankfurt and hands it to NTT, who takes it to New York. Finally, NTT hands it off to Qwest/Centurylink in Washington DC, and the traffic is delivered.

217.150.62.233228.461BelTelecom-gw.transtelecom.net (Minsk, Belarus)

27 February 2013: Traceroute from Guadalajara, Mexico to Washington, DC via Minsk

IP	Delay (ms)	Notes
201.151.31.149	15.482	pc-gdl2.alestra.net.mx (Guadalajara, MX)
201.163.102.1	17.702	pc-mty2.alestra.net.mx (Monterrey, MX)
201.151.27.230	13.851	igmty2.alestra.net.mx (Monterrey, MX)
63.218.121.49	17.064	ge3-1.cr02.lar01.pccwbtn.net (Laredo, TX)

IP	Delay (ms)	Notes
63.218.44.78	64.012	TenGE11-1.br03.ash01.pccwbtn.net (Ashburn, VA)
64.209.109.221	84.529	GBLX-US-REGIONAL (Washington, DC)
67.17.72.21	157.641	lag1.ar9.LON3.gblx.net (London, UK)
208.178.194.170	143.344	cjs-company-transtelecom.ethernet8-4.ar9.lon3.gblx.net (London, UK)
217.150.62.234	212.869	mskn01.transtelecom.net (Moscow, RU)
87.245.233.198	225.516	ae6-3.RT.IRX.FKT.DE.retn.net (Frankfurt, DE)
*		no response
*		no response
129.250.3.180	230.887	ae-3.r23.nycmny01.us.bb.gin.ntt.net (New York, NY)
129.250.4.69	232.959	ae-1.r05.nycmny01.us.bb.gin.ntt.net (New York, NY)
129.250.8.158	248.685	ae-0.centurylink.nycmny01.us.bb.gin.ntt.net (New York, NY)
*		no response
63.234.113.110	238.111	63-234-113-110.dia.static.qwest.net (Washington, DC)



Traceroute Path 1: from **Guadalajara**, Mexico to **Washington**, D.C. via ***Belarus***

Source: Renesys Path Measurements

The recipient, perhaps sitting at home in a pleasant Virginia suburb drinking his morning coffee, has no idea that someone in Minsk has the ability to watch him surf the web. Even if he ran his own traceroute to verify connectivity to the world, the paths he'd see would be the usual ones. The reverse path, carrying content back to him from all over the world, has been invisibly tampered with.

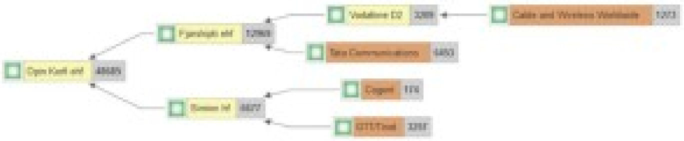
May 2013: Changing of the Guard

The Belarus traffic diversions stopped in March. They restarted briefly in May, using a different customer of BelTelecom as the source, and then ended for several months. Within the same hour as the final Belarus hijack of May, however, we saw a first BGP hijack lasting only five minutes from a completely new source: Nyherji hf (AS29689), a small Icelandic provider.

Example 2: Icelandic Traffic Diversion

After this "first light" from Iceland in May, there were no more route hijacks from Iceland for more than two months. Then, at 07:36:36 UTC on July 31st 2013, Icelandic provider Opin Kerfi (AS48685) began announcing origination routes for 597 IP networks owned by one of the largest facilities-based providers of managed services in the United States, a large VoIP provider. On a normal day, Opin Kerfi normally originates only three IP networks, and has no downstream AS customers.

Opin Kerfi has two ISPs: Fjarskipti (AS 12969) and Síminn (AS 6677). The faulty routes propagated exclusively through Síminn, never through Fjarskipti.



In fact, this was one of seventeen Icelandic events, spread over the period July 31 – August 19th. And Opin Kerfi was not the only Icelandic company that appeared to announce international IP address space: in all, we saw traffic redirections from nine different Icelandic autonomous systems, all customers of (or belonging to) the national incumbent Síminn. Hijacks affected victims in several different countries during these events, following the same pattern: false routes sent to Síminn's peers in London, leaving 'clean paths' to North America to carry the redirected traffic back to its intended destination.

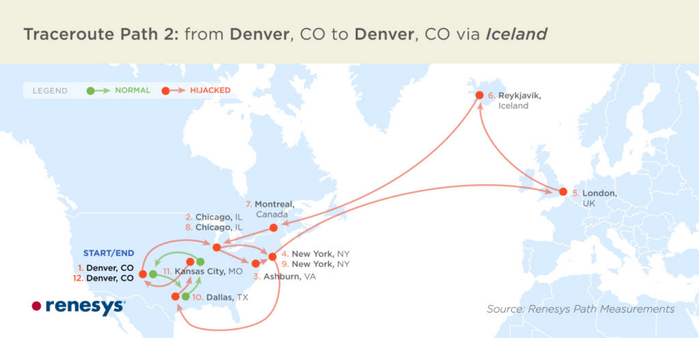
Here's an example in which traffic *between two locations in Denver, Colorado* actually ends up getting carried all the way to Iceland and back.The Icelandic providers have hijacked a block of address space belonging to Qwest/Centurylink in Denver. Atrato receives a false peer route to this block from Siminn Iceland, so when an Atrato customer needs to send content across town, Atrato instead carries their traffic to London. There they hand it off to Siminn, who takes it to Iceland before returning it to Montreal on the clean path to Cogent via the Greenland Cable.

Cogent gamely carries the traffic back from Montreal to Chicago, and then to New York, where they hand it to Qwest/Centurytel for delivery. Centurytel brings it back across the USA through Dallas and Kansas City, and on to the intended recipient in Denver.

August 2, 2013: Traceroute from Denver, Colorado to Denver, Colorado via Iceland

IP	Delay (ms)	Notes
78.152.46.241	9.872	Atrato customer (Denver, CO)
78.152.34.213	26.324	eth1-7.r2.chi1.us.atrato.net (Chicago, IL)
78.152.34.138	44.58	eth1-1.r1.ash1.us.atrato.net (Ashburn, VA)
78.152.34.118	47.464	eth1-3.edge1.nyc1.us.atrato.net (New York, NY)
78.152.44.201	48.477	eth4-3.core1.nyc1.us.atrato.net (New York, NY)
78.152.44.134	123.726	eth1-5.core1.lon1.uk.atrato.net (London, UK)
78.152.44.101	121.308	eth1-3.r1.lon1.uk.atrato.net (London, UK)

IP	Delay (ms)	Notes
195.66.225.26	203.445	siminn-linx-gw-1.isholf.is (Reykjavik, Iceland)
172.16.100.51	162.399	RFC1918
157.157.55.50	152.745	Landssimi/Siminn (Reykjavik, Iceland)
38.104.155.57	151.857	gi3-46.mag01.ymq02.atlas.cogentco.com (Montreal, CA)
154.54.82.241	151.899	te0-4-0-0.ccr21.ymq02.atlas.cogentco.com (Montreal, CA)
66.28.4.202	150.251	be2114.ccr21.ord01.atlas.cogentco.com (Chicago, IL)
154.54.44.70	150.945	be2326.ccr21.jfk04.atlas.cogentco.com (New York, NY)
154.54.11.182	150.596	qwest.jfk04.atlas.cogentco.com (New York, NY)
67.14.2.141	158.456	dal-edge-18.inet.qwest.net (Dallas, TX)
72.165.208.158	158.441	Qwest (Dallas, TX)
206.51.69.26	172.091	bb-kscbmonr-jx9-01-xe-11-1-0.core.centurytel.net (Kansas City, MO)
206.51.69.6	173.069	bb-kscbmonr-jx9-02-ae0.core.centurytel.net (Kansas City, MO)
206.51.69.201	185.738	bb-dnvtc056-jx4-02-ae2.core.centurytel.net (Denver, CO)



Source: Renesys Path Measurements

Attribution

It’s important to clarify that we base these conclusions on direct observation and active measurement. Various providers’ BGP routes were hijacked, and as a result, some portion of their Internet traffic was misdirected to flow through Belarusian and Icelandic ISPs. We have BGP routing data that show the second-by-second evolution of 21 Belarusian events in February and May 2013, and 17 Icelandic events in July-August 2013.

We have active measurements that verify that during the period when BGP routes were hijacked in each case, traffic redirection was taking place through Belarusian and Icelandic routers. These facts are not in doubt; they are well-supported by the data.

What's not known is the exact mechanism, motivation, or actors.

We first contacted the peering team at Iceland's Síminn in July, when their traffic redirection began in earnest, highlighting some of the erroneous routes. We received no response.

We contacted them again recently while researching this story. We were told that the problems were the result of a bug in vendor software, that the problem had gone away when patched, and that they did not believe this problem had a malicious origin. Despite repeated requests for supporting details, we received no further communication.

If this is a bug, it's a dangerous one, capable of simulating an extremely subtle traffic redirection/interception attack that plays out in multiple episodes, with varying targets, over a period of weeks. If it's a bug that can be exploited remotely, it needs to be discussed more widely within the global networking community and eradicated.

We believe it's unlikely that a single router vendor bug can account for the 2013 worldwide uptick in route hijacking with traffic redirection. These Belarusian and Icelandic examples represent just two of a series of MITM attack sequences that we've observed playing out in the last 12 months, launched from these and other countries around the world.

Implications

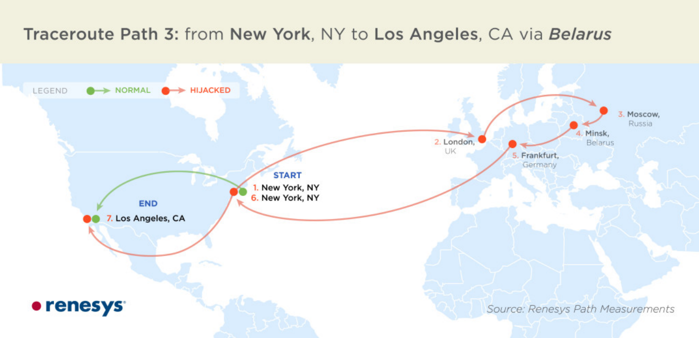
In practical terms, this means that Man-In-the-Middle BGP route hijacking has now moved from a theoretical concern to something that happens fairly regularly, and the potential for traffic interception is very real. Everyone on the Internet — certainly the largest global carriers, certainly any bank or credit card processing company or government agency — should now be monitoring the global routing of their advertised IP prefixes.

This kind of attack *should not happen.* You cannot carry out this kind of hijacking without leaving permanent, visible footprints in global routing that point right back to the point of interception. We believe that people are still attempting this because they believe (correctly, in most cases) that nobody is looking.

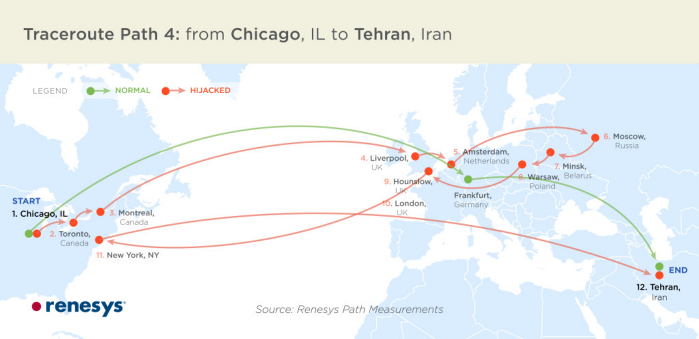
Renesys believes that increased transparency is the best answer, exactly the kind of collective security solution that the Internet is good at delivering. For our part, we've taken this seriously enough that we've spent the last year building a new system that can address the challenge of identifying bad traffic paths for the whole Internet, everywhere on Earth, simultaneously.

Until the day when all routes are signed and secured (and that day may never fully arrive), the best way to prevent manipulation of trust-based routing will be to help people expose violations of trust, and recognize those who implement best practices. We'll have more to say on this subject in coming months.

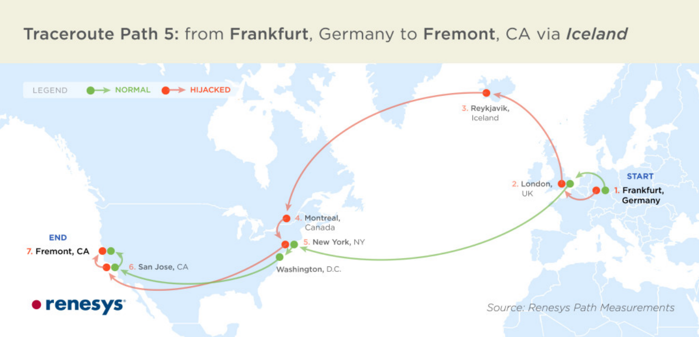
Additional example paths:


Traceroute Path 3: from New York, NY to Los Angeles, CA via *Belarus*

Source: Renesys Path Measurements


Traceroute Path 4: from Chicago, IL to Tehran, Iran

Source: Renesys Path Measurements


Traceroute Path 5: from Frankfurt, Germany to Fremont, CA via *Iceland*

Source: Renesys Path Measurements

SHARE NOW

Whois: Jim Cowie

Jim Cowie was the Chief Scientist at Dyn. Previously, Jim was the founder and CTO of Renesys, the Internet Intelligence Authority, which Dyn acquired in 2014.

Related Posts

RESEARCH

Dec 22, 2017 // Doug Madory

Recent Russian Routing Leak was Largely Preventable

Read More

RESEARCH

Dec 21, 2017 // David Belson

2017 Internet Intelligence Roundup

Read More

Read More

RESEARCH

Dec 7, 2017 // Doug Madory

Puerto Rico's Slow Internet Recovery

Read More