All Things D

News

How Somebody Forced the World's Internet Traffic Through Belarus and Iceland

Published on November 20, 2013
by **Arik Hesseldahl**

This is a deeply technical but potentially very troubling story. Imagine one day you're using the Internet the same way you do every day. Reading the news, shopping, sending email, checking your bank and credit card balances. Maybe even doing some work for your employer.

Typically, but not always, the bits being sent from your computer, tablet or phone will flow from where you are to where they need to be via the most direct route available.

But what if they didn't? What if someone slipped in between you and the various servers you're connecting with and diverted your traffic elsewhere, funneling it through a choke point of their choosing, so they could capture, copy and analyze it? Your data takes some extra — and imperceptible — milliseconds to get where it's going and ultimately everything you're doing online works just fine. But your traffic has been hijacked by parties unknown and you're none the wiser that it has happened.

In network security circles, this is what's known as a Man-In-The-Middle attack. And for years it has been understood to be possible in theory, but never seen in practice. That changed earlier this year when someone — it's unclear who — diverted Internet traffic from some 150 cities around the world through networks in Belarus and Iceland.

The troubling disclosure came yesterday from the research company Renesys. The firm specializes in tracking the operational health of global Internet infrastructure. When Internet traffic goes down in one country or another, whether because of a natural disaster or political unrest, Renesys is usually among the first to see it.

The attack — and Renesys maintains that it was an attack — targeted large Internet carriers in every major city in the U.S. and numerous major cities in Europe and around the world. (See their map here.)

The first incident took place during most of the month of February, when Internet traffic was silently redirected through an Internet service provider called GlobalOneBel, based in the Belarusian capital, Minsk.

The targets of these attacks included financial institutions, government agencies and network service providers.

Renesys tracked the attacks as they happened. Here's how its CTO Jim Cowie described one:

Here's an example of a trace from Guadalajara, Mexico, to Washington, D.C., that goes through Moscow and Minsk. Mexican provider Alestra hands it to PCCW for transit in Laredo, Texas. PCCW takes it to the Washington, D.C., 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 D.C., and the traffic is delivered.

So if you were in Mexico, sending an email to someone in Washington, D.C., it got diverted in Virginia and sent to London, Moscow and Minsk before taking a return trip through Frankfurt, New York and ultimately to its intended destination. Renesys thinks the chances are pretty good it was read along the way.

It's helpful at this point to understand something called Border Gateway Protocol. It's one of those things that make the Internet work, but is a little hard to get your head around if you don't live with it day to day.

Basically, BGP is a method by which Internet service providers tell the world what other networks they're connected to and how they themselves can be reached. Because the Internet is built for resiliency and reliability, there are usually multiple ways for traffic to get from one place to another, and those routes are published in something called the Global Routing Table.

Imagine the Internet is a long series of intersecting lines of people going in multiple directions, and you can only pass handwritten messages to three or four different people standing next to you, and each of them are in lines headed in different directions. BGP is sort of a way of announcing to the world where you're located in that chain, which people you can reach and which directions they're heading.

But imagine what would happen if one of those three people you can reach lies to you about who *they can reach*. With no reason to question that information, you would probably pass a message on to them, unaware that it would be handed off to additional actors that might just peek at it before they send it on its way.

That's essentially what Renesys said has been happening here. These attacks occurred throughout February and into March. Then they stopped for awhile.

The attacks resumed in May, and almost right away the choke point switched from Belarus to Iceland. For about five minutes — literally — traffic was routed through was an Icelandic ISP called Nyherji hf.

Then they stopped again — until July. This time, the venue was again in Iceland. Beginning on July 31, traffic from a large VOIP company — Renesys wouldn't name it — was diverted through an Internet service provider called Opin Kerfi that oddly announced access to 597 different IP blocks versus its usual three.

The result caused routine Internet traffic to take some routes that were so indirect as to be absurd. For a brief time on Aug. 2, data traffic between two providers in Denver didn't just flow across town as it normally would. Instead the bits went to Iceland first, with stops in London, Montreal, New York, Dallas and Kansas City along the way.

So who did it? It's hard to say. I talked to Cowie last night and he didn't seem to have much of an idea. "We can track whose infrastructure was used to carry out these attacks because they leave their footprints in the global routing table," he said. "Tracing it back to who engineered this attack is another thing entirely."

The targets of the attack have been notified. The motivation was likely a financial one.

This sort of attack should not happen, Renesys contends. But when it does, it leaves a permanent, indelible mark that is visible to those who know how to look for it. While sometimes these bad traffic routes are

advertised in error and by accident — someone mistypes a digit in configuring networking equipment — when they are sustained and as wide-ranging as this, something bad is likely taking place, Cowie said, something that can and should be stopped.

"If you're watching, this sort of attack is instantly visible to those people who monitor BGP," Cowie said. "But no one is looking."

While it's a fair bet that some kind of crime was at least attempted if not committed in carrying out these attacks, the legal jurisdictions will be kind of tricky to sort out. The attackers could be anywhere in the world and might have used ISPs in Belarus and Iceland without their knowledge. With possible victims in a variety of countries, prosecution of a crime — if one was indeed committed — would likely be difficult.

But there is a way to stop this from happening again. Cowie said the really big Internet service providers — the ones who resell their traffic to smaller regional and national providers — should be watching for when smaller players advertise false routes. "If big ISPs monitored their customers and filtered their traffic when they advertise these false routes, this would be over. This kind of attack could not occur. … In each one of these attacks there was someone, usually a very large ISP, who failed to filter."

"Our motivation is to shed some light on this," he said. "We really want people to start raising their game a bit and start watching out for this."

Return to: How Somebody Forced the World's Internet Traffic Through Belarus and Iceland

URL: http://allthingsd.com/20131120/how-somebody-forced-the-worlds-internet-traffic-through-belarus-and-iceland/
