The ISP Column
A monthly column on things Internet

March 2008

Geoff Huston

Tubular Routing

I suppose it had to happen one of these days. Sooner or later a routing hijack would get its 15 seconds of fame in the industry press, and the incident relating to the YouTube prefix just happened to be the one that was selected by the media because of the players involved rather than the rather mundane characteristics of the routing leak itself.

For those of you who were on another planet at the time, the incident itself was pretty straightforward. Pakistan Telecom leaked to the Internet a black hole route to the YouTube site, and YouTube quickly found itself to have become unreachable in most parts of the Internet.

One of the best summaries of the event can be found on the Renesys blog site (http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml).

Briefly, at around 18:48 UTC on the 24th February, AS 17557, a network operated by Pakistan Telecom, originated a route for 208.65.153.0/24 to its external upstream transit AS 3491 (operated by Pacific Century Cyberworks, or PCCW). YouTube conventionally advertises itself by a more general route advertisement, advertising 208.65.152.0/22, using as an origin AS 36351 (YouTube's AS). The /24 from AS 17557 took routing precedence across the Internet over the /22, which is entirely correct in terms of the operation of the routing system. All this change of routing happened within 2 minutes of the AS17557 route advertisement, which is what one would expect in terms of routing performance for propagation of a new route in BGP. YouTube appears to load balance its web traffic across three IP addresses, 208.65.153.251, 208.65.153.253 and 208.65.153.238, so redirecting 208.65.153.0/24 encompasses all of YouTube's public facing servers, effectively rendering YouTube unreachable.

By 20:07 UTC on the 24th February YouTube responded with a /24 advertisement from its origin AS. At this stage there were two /24 advertisement for the same prefix in the network, and those networks who were "close" to YouTube now believed the YouTube advertisement, but those networks that were "close" to AS3491 continued to believe the false AS17557 originated advertisement.

At 20:52 UTC the false route to AS17557 was altered to add a prepending of AS17557, lengthening the AS Path length of this black hole advertisement by one unit. Obviously, this still did not remove the false route from the entire network, and still did not completely eradicate the problem. At around 20:18 YouTube attempted the advertisement of even more specific routes, two more specific /25's, in order to take precedence over the rogue /24. This measure was not effective either, as most Internet Service Providers filter out all transit advertisements for prefixes of a /25 or smaller. A few minutes later at around 21:00 UTC AS3491 disconnected AS17557.

Was this a malicious act undertaken by hackers? Not really. As the adage goes, don't confuse malice for plain old incompetence! This incident appears to be a case of routing incompetence rather than anything more sinister. Pakistan Telecom was evidently attempting to obey orders from the Pakistan government, as news reports suggests, but using a rather flawed approach to the implementation of the order! (http://ca.news.yahoo.com/s/afp/080224/world/denmark_media_islam_pakistan_internet_youtube)

We may not have a network that is terribly secure in a routing sense, but we sure have some really excellent tools to show what happens after such events!

BGPlay using the RIPE NCC's Routing Information Service, (http://www.ris.ripe.net/bgplay/) is one of the best illustrations of the way in which the routing system reacted first to the bogus routing advertisement, and then to the various efforts that were tried in response. A report compiled by the RIPE NCC folk provides further insights into the efforts to repair the problem (http://www.ripe.net/news/study-youtube-hijacking.html).

The issue here appears to be the outcome of the combination of a number of factors. Firstly, using the inter-AS routing system to enforce local policies is a case of picking the wrong tool for the job. Using a blackhole route within AS17557, Pakistan Telecom, is entirely a local matter, but allowing the route to leak in the inter-AS routing fabric is the first serious issue. Secondly, AS3491, PCCW, did not appear to have in place the necessary route filters on its links to AS17557 to prevent it from learning this unauthorized route. And lastly, once the route entered into the transit core of the Internet the general framework of mutual trust between transit network operators ensured that the false network route was efficiently propagated across the rest of the Internet.

This is not the first case of route hijacking, nor will it be the last, but, because of the parties involved, its certainly the most prominent case for some time. Perhaps its prominence is a good foundation to highlight the continuing concerns over the pervasive vulnerability in the Internet's routing system, and just how easy and quickly attacks can be launched via the use of false routing information injected via a weak point that allows access into the mutually trusted transit core of the Internet.

Its not as equipping the routing system with adequate security defences is a new challenge, and we've spent many years examining various ways of making the routing system more resistant to various form of attack. We've tried route filters, Internet Route Registries, bogon filters and automated registry lookup systems to attempt to match some trusted external source of information about who has what rights of use of which addresses and AS numbers with the information contained in the routing system. We've even considered the use of strong cryptographic protection to validate such bindings, using public key cryptography. See "Securing Inter-Domain Routing" (http://www.potaroo.net/ispcol/2005-03/route-sec-2-ispcol.html) for a longer discussion about routing security and the outline of an approach to use X.509 public key certificates to assist in validating the authenticity of routing information, for example.

Certainly most of the time most of the network's routing system appears to be accurate. When we use the Internet what happens for each of us is pretty much what we expect to happen, and it appears that most of the information in the routing system is mostly authentic and accurate for most of the time. But it seems that the law of diminishing return applies here, and while we do a decent job in routing, we place too much faith in the good intentions of everyone else and don't seem to place enough value in comprehensive routing security to put the entire routing system on a comprehensively secure foundation. There are some 250,500 prefixes in the routing system in March 2008, and some 250,000 describe properly registered addresses. But as for the other 500 routing entries there are no public records that indicate that these addresses are routable. The CIDR Report (http://www.cidr-report.org) has a daily listing of some 500 addresses and 400 AS numbers what are advertised in the routing system without any from of supporting public registry information as to the validity of these addresses and AS numbers. And when we try to match addresses to originating ASs using Route Registry information the picture is even more incomplete.

If its still just way too easy for these forms of routing configuration mistakes to generate various forms of havoc on the Internet, then how vulnerable are we to efforts to deliberately sabotage of the routing system? Rather than enlisting a cloud of enlisted zombie end system to mount a large traffic surge on a victim site, how much easier is it to generate a black hole route and inject it via a weak point into the routing system? So mistakes happen, and unauthorized routes leak, and from time to time it appears that its not just fat finger trouble on the console, but indirect evidence of a larger attack that includes deliberate subversion of routing. And if we are all somewhat uncomfortable with this situation, just what should ISPs be doing to assist in securing the routing system?

Again, this is not exactly a new topic. One article in this column a few months ago, a perspective on routing security, (http://www.potaroo.net/ispcol/2005-02/route-sec.html) offers one perspective of what an ISP could consider, and there are many other resources that provide good pragmatic advice as to what constitutes decent routing security measures.

But we just don't seem to break through and move beyond various exhortations on how we should and could do a better job in routing. Something else may be broken here. It appears that while an operator can do a relatively robust job in protecting their routing infrastructure in terms of protecting routers and the integrity of operation of the routing protocol, the task of protecting the integrity of the payload is a much more frustrating task. Even if the ISP is prepared to devote considerable time and expense in being diligent about researching the authenticity of every routing request coming from their customer base, the ISP still is in the position of having to accept routes from their peers and upstreams without any particular assurance of the quality and authenticity of that routing information. And its not clear that the ISP is strongly incented to perform thorough and exhaustive checks on the authenticity of routing requests, particularly when they relate to non-locally assigned address space. The business proposition

here is that this activity is a net expense to the business, with no incremental revenue to offset the expense. So the ISP often performs cursory checks, but not to a level of detail that would detect a determined effort to inject incorrect information into the routing system. Unfortunately integrity of routing is one of the cornerstones of integrity of the operation of the Internet itself, and the picture today is that we are still not in a strong position to defend the Internet against determined efforts to disrupt it at this level, or even against the outcomes of various forms of operational errors.

Unless we can make good security better, faster and cheaper than the alternatives then we will continue to wrestle with this problem as an industry. And making robust security better, faster and cheaper than the alternatives is proving to be a real challenge for us!

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

About the Author

GEOFF HUSTON holds a B.Sc. and a M.Sc. from the Australian National University. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. He is author of a number of Internet-related books, and is currently the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He was a member of the Internet Architecture Board from 1999 until 2005, and served on the Board of the Internet Society from 1992 until 2001.

http://www.potaroo.net