How prevalent is prefix hijacking on the internet?

It's a major worry for network operators, but is it an actual problem?

Peter Boothe, James Hiebert
Supervised by Randy Bush

Intro / What is Prefix-Hijacking?

Prefix hijacking is a type of network attack that can give malicious parties access to untraceable IP addresses. On the internet, networks under control of a single entity constitute an Anonymous System (AS), each of which has a unique numerical ID assigned to it by its Regional Internet Registry. Each AS has one or more routers on the edge of its network which routes traffic to all of its peer ASs. ASs then communicate routing information and establish peering relationships using the Border Gateway Protocol (BGP). This is all done in an effort to allow each AS to make announcements about the IP address space it controls.

IP space is allocated and announced in blocks, so if an AS controls all IP addresses between 3.0.0.0 and 3.255.255.255, then it could announce the block 3.0.0.0/8. The numbers before the slash indicate the IP address mask, and the number after the slash is how many bits of the mask should be considered important. Lower numbers indicate larger blocks - 3.0.0.0/8 contains 16 million IP addresses, while 3.1.2.0/24 contains only 256.

ASs that exchange BGP information directly - “Peering ASs” - are assumed to be friendly with each other, so BGP implements no security against receiving bad or invalid routing info from other routers.

Prefix-hijacking occurs when a malicious or misconfigured AS announces to its peers that a block of IP-address space belongs to themselves, when, in fact, it does not. After a short delay, routes based on this bad announcement propagate through the internet at large and the malicious AS may be able to send and receive traffic using addresses it does not own. This hijacked space can be - and hase been - used to send unsolicited mass e-mails, download copyrighted works, launch break-in attempts, or anything else generally considered to be illegitimate network use.

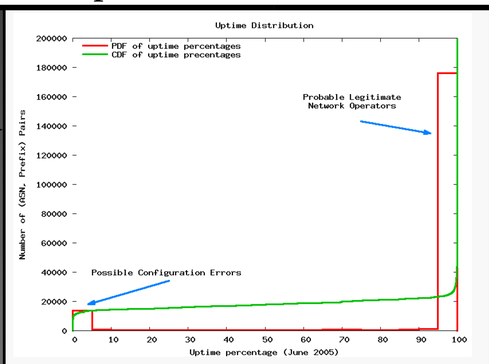
Should anybody ever see this traffic, blame will generally fall on the owner of the IP space, rather than the hijacker. Indeed, network operators have received cease-and-desist letters for activity relating to IP addresses in their own blocks that have never actually been assigned to a computer.

What Characterizes Prefix Hijacking?

Prefix hijacking can happen in one of three ways - a block containing unallocated space can be announced, a subblock of an existing allocation can be announced, or a competing announcement for exactly the same space as an existing allocation can be announced. Because of the vagaries of the BGP protocol, subblock hijacking is the easiest and most dependable attack, and is therefore the one of greatest concern to network operators.

No matter what the style of attack, the announcements will probably be short lived, relative to legitimate announcements. This is because attackers, wishing to hide their tracks, will withdraw their announcement once they are done, as opposed to legitimate network operators who generally strive for as much uptime as possible. Not only that, but because of extant filtering methods (BOGON filters, etc.), we would expect that malicious announcements will occur in space that is already allocated, and so will generally be subblocks of announced space.

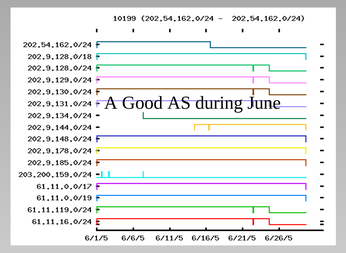
Short uptime! We can look for that!



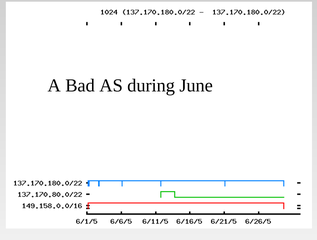
Note that a few things are pretty clear from this graph - most prefixes are almost always up and announced by the same AS, and the ones that aren't, are generally not up for very long at all. In our initial survey, every single one of the short-lived blocks that we checked by hand was probably a misconfiguration.

Invading space! We can look for that!

Looking over the data for June, 9,697 separate prefixes were announced inside of another AS's announced space. When we examined the data further, however, we saw that a common misconfiguration was to announce a netblock that was far too large and then immediately notice your mistake and withdraw the announcement. So, we restricted our search to only check whether an announcement was inside one of the blocks that was up more than 90% of the time and found that there were “only” 5,625 announcements that invaded another person's space.



A Good AS during June



A Bad AS during June

Paranoia vs. Common(?) Sense

Combining our short-lived data and our space-invading data, we can see that there are 5,625 potential hijackings out of 199,393 total (AS, prefix) pairs. Sampling the data by hand, however, we still see that the data set is dominated by events that are explainable by misconfigurations. A paranoiac might conclude that the malicious parties are hiding their tracks very well, but common sense tells us that these announcements are probably not malicious. So we need to further cull our results into ones that are definitely malicious, but right now we have a nice upper bound of 5,625 potential hijacks in the month of June, 2005.

Culling our result set

Our “percent uptime” heuristic will give us false positives if the prefixes were up in the beginning of the month, and were brought down mid month, never to be reannounced. Therefore, we will reject from our set of low-uptime announcements any prefix that was up at the beginning of the month. This leaves us with 2,031 potential hijackings. We can further cull this data, by examining AS names in whois, in an effort to establish whether or not those two entities have some form of business relationship.

Furthermore, we assume that any long lived announcement inside another AS's space is legitimate. Even the most avaoidant of network operators should notice if some of their space has been hijacked for 20+ days. Using these techniques, we pared the list down to 420 instances in which it is at probable that hijacking took place.

Conclusion

After going through a random sampliing of 10% of the 420 remaining events, we found that 9 were impossible to distinguish from genuine hijackings. Indicating that approximately 90 prefix hijacks took place in the month of June.

Thus, out of almost 200,000 separate (AS, prefix) pairs in the month of June, 90 of them appear to be malicious. In this same time, there were over 4,000 (AS, prefix) pairs that were obviously erroneous due to misconfiguration errors. Therefore, our conclusion is that, for the time being, router user interfaces are a much larger threat to the BGP-layer of the internet than malicious operators.