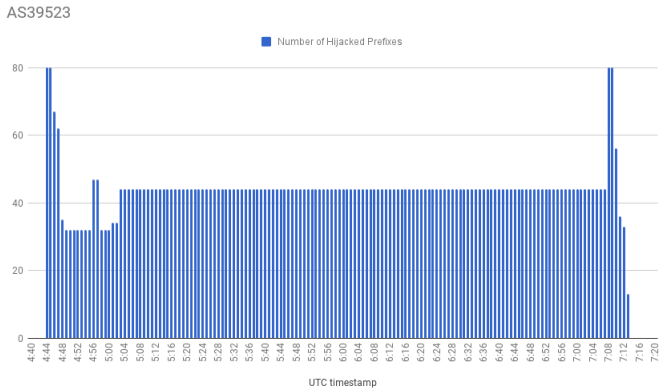
December 13th, 2017

Born to Hijack

New ISPs emerge every day, and 12 December was not an exception. A new interdomain routing ecosystem actor, AS39523 (DV-LINK-AS) started announcing its address space (one prefix), while at the same time this new network hijacked 80 high profile prefixes. The hijacked prefixes belonged to both Russian and International content providers such as Google, Facebook, Microsoft, Mail.ru, Vkontakte and many more.



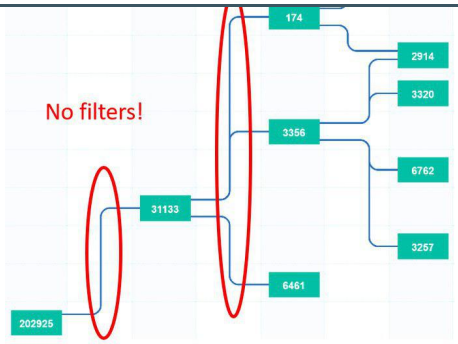
Incident lasted for more than 2 hours, starting at 4:44 UTC and peaking with 80 hijacked prefixes and ending at 7:19 with another peak at 7:04 UTC.

Due to the specific set of affected prefixes, we can assume static routes were leaked into BGP. We can only guess why these 80 prefixes were selected. Maybe some experiment leaked into the production network? However, the central question is: why these path announcements propagated at all? The fact that the hijacked prefixes propagated to every corner of the Internet demonstrates an absence of proper filters between the AS39523 and its direct upstream AS31133 (Megafon), and between

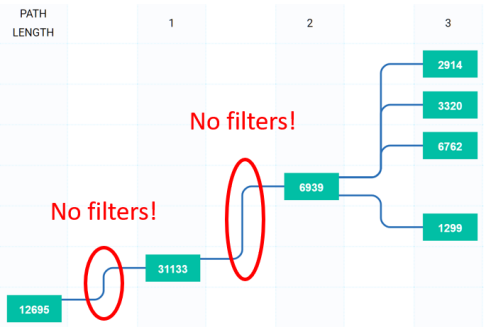
announcements were also accepted by major providers, such as Level3 (AS3356), Cogent (AS174), Zayo (AS6461), Hurricane Electric (AS6939) and others.

There are three common reasons for the absence of ingress prefix-based route filters at the customer-to-provider interconnection point. (1) Some transit ISPs have trouble convincing their customers to properly publish their route announcements. Since the customer is paying for the service, some ISPs don't feel empowered to enforce strict filters - and as a result, we have exceptions. (2) Another problem is that there is no authorization for AS-SETs. You can add any ASN to your AS-SET! There are ISPs that have thousands of ASNs in their AS-SET with only a dozen of prefixes actually being announced in BGP. The problem expands to the core of the Internet, where large Tier2 networks may have the size of their AS-SETs consist of more than hundred of thousand prefixes. Instead of working with customers on fixing this problem some providers prefer to just remove any filters applied to the ISP with the overly large AS-SET. (3) And lastly, some ISPs feel that AS_PATH based filters are adequate enough, and do not implement prefix based filters at all.

The lack of filters is not hard to prove: all we need is a globally visible prefix, which does not have any route object. Let's take a look at 91.243.129.0/24, this prefix does not have any route objects in any database. Still, it is propagated by Megafon and accepted by its upstream providers.



An IPv6 example can also be observed here. No route6 object exists for 2a03:34e0::/32 as can be seen in NLNOG's IRRExplorer, but in the Radar's 2a03:34e0::/32 overview we see the prefix is propagated without issues. So either no filters exist between AS 12695 and Megafon (AS 31133) or the filters are inadequate; and probably no prefix-based filtering exist between Megafon and Hurricane Electric (AS 6939).



This hijack highlights a common problem that arises due to lack of route filtering. We can blame AS39523 for the accident, but without proper filters at the intermediate transit providers boundaries we are doomed to see similar incidents again and again. We'd like to encourage all networks involved in this incident to review their route filtering strategy, and at the very least implement prefix-based BGP filters on all interconnections towards their customers.

A week ago at the Moscow Peering Forum, Alexander Azimov (head of Qrator's Radar project), presented on the specific topic - read the slides to learn more detailed information on how the absence of filters can become a

Check if your IP, AS or Domain was affected:

Facebook Google+ Twitter

Search: AS Number, IP, Doma