Posted by Andree Toonk - December 12, 2017 - Hijack - No Comments

Early this morning (UTC) our systems detected a suspicious event where many prefixes for high profile destinations were being announced by an unused Russian Autonomous System.

Starting at 04:43 (UTC) 80 prefixes normally announced by organizations such Google, Apple, Facebook, Microsoft, Twitch, NTT Communications and Riot Games were now detected in the global BGP routing tables with an Origin AS of 39523 (DV-LINK-AS), out of Russia.

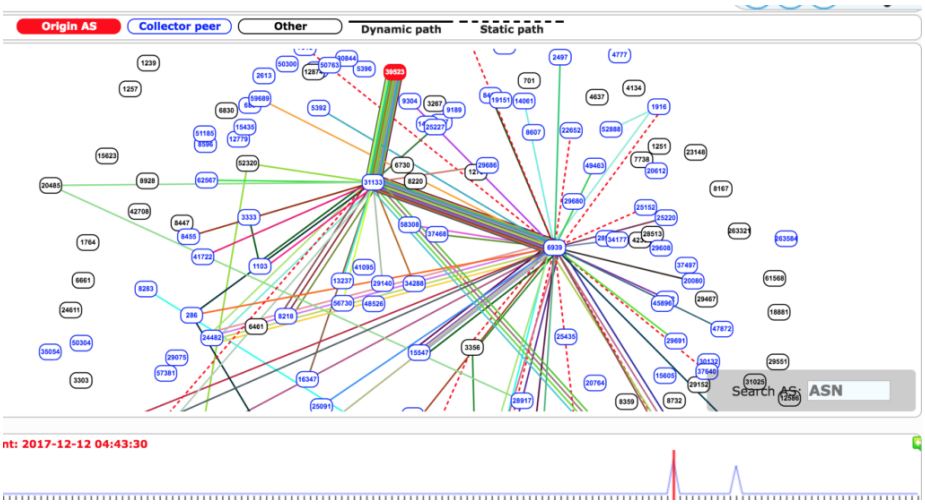
Looking at timeline we can see two event windows of about three minutes each. The first one started at 04:43 UTC and ended at around 04:46 UTC. The second event started 07:07 UTC and finished at 07:10 UTC.

Even though these events were relatively short lived, they were significant because it was picked up by a large number of peers and because of several new more specific prefixes that are not normally seen on the Internet. So let's dig a little deeper.

One of the interesting things about this incident is the prefixes that were affected are all network prefixes for well known and high traffic internet organizations. The other odd thing is that the Origin AS 39523 (DV-LINK-AS) hasn't been seen announcing any prefixes for many years (with one exception below), so why does it all of sudden appear and announce prefixes for networks such as Google?

If we look at a few AS paths we see that 39523 is always the origin, while the next hop transit AS is always 31133 PJSC MegaFon. We also see that the announcements were picked up further and made reachable by a few large ISP's such as:

xx 6939 31133 39523 (path via Hurricane Electric)
xx 6461 31133 39523 (path via Zayo)
xx 2603 31133 39523 (path via Nordunet)
xx 4637 31133 39523 (path via Telstra)

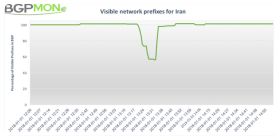


What makes this incident suspicious is the prefixes that were affected are all high profile destinations, as well as several more specific prefixes that aren't normally seen on the Internet. This means that this isn't a simple leak, but someone is intentionally inserting these more specific prefixes, possibly with the intent the attract traffic.
Loyal readers will remember our blog post from earlier this year involving another Russian network: "The curious case of as12389". This event is somewhat similar in that it appears targeted.

Tweets by @bgpmon

BGPmon.net
@bgpmon

Close to 50% drop in announced BGP routes as well as a traffic drop from Iran between 13:23 UTC - 13:35 UTC. Also see @bgpstream bgpstream.com/event/122241



Jan 1, 2018

BGPmon.net Retweeted

bgpstream
@bgpstream

BGP,OT,IR,Iran, Islamic Republic of,-,Outage affected 2017 prefixes, bgpstream.com/event/122241

Jan 1, 2018

BGPmon.net Retweeted

Embed View on Twitter

```
$ whois -h whois.ripe.net AS39523


% Information related to 'AS39523'

% Abuse contact for 'AS39523' is 'support@dv-link.ru'

aut-num: AS39523
as-name: DV-LINK-AS
org: ORG-VII2-RIPE
sponsoring-org: ORG-ATS13-RIPE
import: from AS31133 accept ANY
export: to AS31133 announce AS39523
import: from AS3216 accept ANY
export: to AS3216 announce AS39523
admin-c: VIIN1-RIPE
tech-c: VIIN1-RIPE
status: ASSIGNED
mnt-by: RIPE-NCC-END-MNT
mnt-by: RIPE-DB-MNT
mnt-by: MNT-DV-LINK
mnt-routes: RIPE-DB-MNT
mnt-routes: MNT-DV-LINK
created: 2017-11-24T14:49:44Z
last-modified: 2017-11-24T14:49:44Z
source: RIPE
```

When checking the RIPE whois data (above) we see that this AS 39523 has only recently been assigned. However, while going through our historical data, we also noticed that AS 39523 was in fact once active earlier this year although it could be that it intended to stay hidden.
Let's go back to another blog post from earlier this year: The Google - Verizon leak in August.
During that incident we got some interesting insights into Google's peering relationships. Interestingly one of the paths that appeared during that leak was the prefix 66.232.224.0/24 with the following ASpath 701 15169 32007 39523.

39523 is the same Russian AS that appeared as the origin AS today. 32007 is an Equinix AS 15169 is Google and 701 verizon. So in august Google learned a path to 66.232.224.0/24 (Kohls Department store) with origin 39523. Without knowing more about this prefixes, it looks strange and unexpected for Google to learn a 'Kohls Department store' Prefix via this path.

Whatever caused the incident today, it's another clear example of how easy it is to re-route traffic for 3rd parties, intentionally or by accident. It also is a good reminder for every major ISP to filter customers.

No comments

Leave a Reply

Comment

Name

Email

Website

Post Comment