Learning from recent major BGP routing leaks

Doug Madory
Director of Internet Analysis, Oracle

Global Peering Forum
Seattle, WA
April 2018
Types of leaks *(mistaken routing announcements)*

“A route leak is the propagation of routing announcement(s) beyond their intended scope.” - RFC7908 (Problem Definition and Classification of BGP Route Leaks)

**Origination**

<table>
<thead>
<tr>
<th>Leaker</th>
<th>Correct origin</th>
</tr>
</thead>
</table>

**Transit/Peering**

Wrong export

BGP announcements
Major internet outage hits the U.S.

No, it's not just you.

Large swaths of the United States experienced internet connection problems today, with several major ISPs apparently affected. Comcast, Verizon, and AT&T all appeared to have issues, with Comcast blaming the outage on an “external network issue.”

SEE ALSO: Sites across the internet suffer outage after cyberattack

This outage falls just after the one-year anniversary of a major DDOS attack on Dyn that crippled the internet for a day in October of 2016.
Level 3 routing leak (Nov 2017) – What happened?

• At 17:47:05 UTC on 6 November 2017), Level 3 (AS3356) began globally announcing thousands of routes learned from customers and peers
  – Routes that were intended to stay internal to Level 3
• Routes stayed in circulation until 19:24 UTC leading to over 90 minutes of problems
• Result was internet traffic to several large networks and content providers were mistakenly sent through Level 3
• Type 6: Accidental Leak of Internal Prefixes and More-Specific Prefixes (RFC7908)

https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/
Level 3 routing leak (Nov 2017) – What happened?

- Bell Canada (AS577) impacts
  - Typically sends AS3356 ~2400 prefixes for circulation into Level 3’s customer cone
  - During the routing leak, that number jumped up to 6,459 prefixes – mostly more-specifics
  - AS3356 passed these routes on its Tier 1 peers like NTT (AS2914) and XO (AS2828, now a part of Verizon)
- More-specifics intentionally used here to ensure a direct return path of traffic from a Tier1
  - Routing tactic that comes with some risk
Level 3 routing leak (Nov 2017) – What happened?

• Bell Canada (AS577) impacts (cont’d)
  – Visualization of the latency impact of the routing leak.

*Traffic engineering is a delicate process, sending a large amount of traffic down an unexpected path is a recipe for service degradation.*
Level 3 routing leak (Nov 2017) – What happened?

• Example propagation of a AS577 route leaked by AS3356
  – 50.100.32.0/22 is not normally in the global routing table (is a more-specific of 50.100.0.0/16)
  – During leak, this route (along with about 4,000 others) appeared in the global routing table as originated by AS577, transited by AS3356
  – ~40% of our BGP sources had these leaked routes in their routing tables and most chose NTT (AS2914) to reach AS3356 en-route to AS577 (below right)
Level 3 routing leak (Nov 2017) – What happened?

• Level 3 leaked over 3000 prefixes from 18 of Comcast’s ASNs
  – AS33491 (356 leaked prefixes)
  – AS7725 (252 leaked prefixes)
  – AS7015 (248 leaked prefixes)
  – AS33287 (241 leaked prefixes)
  – AS33651 (235 leaked prefixes)
  – 13 more ASNs
Level 3 routing leak (Nov 2017) – What happened?

- Comcast performance impact
Level 3 routing leak (Nov 2017) – What happened?

• Various other providers impacted

• **But what about IPv6?!!**
Level 3 routing leak (Nov 2017) – What happened?

- Routing leak analyses **rarely** look at the IPv6 side
- Level 3 leaked the following in IPv6:
  - 2000+ Comcast prefixes
  - 36 Netflix prefixes
  - 22 QSC prefixes (German ISP)
  - 1 Craigslist prefix 😊

- Interesting similarities and differences!
  - Comcast and Netflix had similar impacts
  - Bell Canada: 4000+ IPv4 prefixes leaked, 0 IPv6 prefixes leaked
Level 3 routing leak (Nov 2017) – What happened?

Level 3 routing leak (Nov 2017) – What happened?

- IPv6 performance on Netflix (subtle, but there)
“Suspicious” event routes traffic for big-name sites through Russia

Google, Facebook, Apple, and Microsoft all affected by “intentional” BGP mishap.

DAN GOODIN - 12/13/2017, 5:43 PM
Russia routing leak (Dec 2017) – What happened?

• On 12 December 2017, AS39523 announced 80 prefixes (only one of which was theirs) for two different 3-4 minute intervals

• Routes were exclusively announced through Russian network Megafon (AS31133)

• Type 5: Prefix Re-origination? (RFC7908)

https://dyn.com/blog/recent-russian-routing-leak-was-largely-preventable/
Russia routing leak (Dec 2017) – What happened?

- Leaked **Russian** networks were carried by *all* of Megafon’s transit providers such as this prefix from Rostelecom
Russia routing leak (Dec 2017) – What happened?

• But for prefixes belonging to major US internet companies, only Hurricane Electric carried these routes on to the greater internet.
Russia routing leak (Dec 2017) – What happened?

• Setting aside the “Russia Attacks!” rhetoric around this incident, there are some things we can learn from it.
• This is an almost good news story!
• 6 of the 7 transit providers for Megafon were still able to block erroneous BGP announcements pertaining to numerous major internet companies
  – Had the 7th also done so, we might not all be discussing this incident
Lessons Learned

• The same large leak incidents can take different forms in IPv4 and IPv6
  – Google leak in August that impacted Japan had no IPv6 component to it
  – Large TMNet leak of 2015 had no IPv6 component
  – Large Indosat leak of 2014 had no IPv6 component
Lessons Learned

• Many (but not all) large providers conduct some sort of filtering to prevent inadvertent hijacks due to routing leaks

• See Job Snijders (NTT) work on filtering:
  – BGP Security IRR AS-SET can be used to build a per-customer prefix whitelist based on route objects discovered using AS-SET definitions.
  – “Peer-lock” to filter certain bad AS Paths.

• MAXPREF would have prevented recent Colt leak
Conclusions

• In every case, there is more than one party involved.
• There is a leaker, of course, but there is also always another network that distributes leaked routes out onto the internet.
• Mistakes inevitably occur, we have to do better to look out for each other.
• The internet is a team effort!
Thank you!

douglas.madory@oracle.com
@dougmadory