The Internet's Biggest BGP Incidents

A Brief History



The network observability company

Justin Ryburn Field CTO

Who's this guy?

Current Field CTO - Kentik

Past

25 years in networking Ran networks (including peering) before migrating to the vendor side

More details



/in/justinryburn

Credit Where Due

Talk based on the work of Doug Madory, "The Man Who Sees the Internet"



<u>@DougMadory</u>

/in/dougmadory

Great resource to follow on social media for news on this topic.

A BRIEF HISTORY OF BGP INCIDENTS

FROM BGP HIJACKS TO BLACK HOLES

DOUG MADORY



BGP Incident Definitions

Hijacks

- Prefix hijacking happens when a network, whether intentionally or mistakenly, originates a prefix that belongs to another network without its permission. [MANRS]
- Presumes malicious intent
- Generally used to describe an illegitimate origination of a prefix

Route Leaks

- A route leak is the propagation of routing announcement(s) beyond their intended scope. [RFC7908]
- Often occur accidentally due to configuration errors
- Malicious actors may also attempt to hide attacks as a leak
- Generally used to describe a leak of prefixes upstream for the legitimate origin of the prefix

Even experts debate the definitions

Definitions for Our Purposes

Origination Errors

- Occurs when an AS originates (announces with its ASN as the origin) a new advertisement of a route to an IP address block over which it does not possess legitimate control
- Solicits traffic destined to those IP addresses to the new ASN

AS Path Errors

- Occurs when an AS inserts itself as an illegitimate intermediary into the forwarding path of traffic bound for a different destination
- Traffic may still reach its ultimate destination, albeit along a sub-optimal path

IP Squatting

- Occurs when an AS announces IP address ranges that are normally unrouted on the global Internet
- Typically for the purpose of evading IP-based blocklists and complicating attribution

Origination Error



Pakistan Telecom Hijack of YouTube (2008)

- Government of Pakistan ordered access to YouTube to be blocked in the country due to a video it deemed anti-Islamic
- Pakistan Telecom intended to blackhole traffic inside their network
- Leaked it to their upstream providers

Image source: https://dl.acm.org/doi/fullHtml/10.1145/2668152. 2668966



Russian Hijack of Twitter (2022)

- Twitter prefix (104.244.42.0/24) announced by Russian Telecom RTComm during the Russian invasion of the Ukraine
- Same prefix was hijacked during the military coup in Myanmar in 2021
- Less propagation this time due to RPKI ROA

SYNTH	HETICS > Test Contro	Center > RU hijack	of Twitter						I↔I Full width	🗹 Edit Test 🔳	Pause Test 🕂 Exp	port 💌
BGP MONITO	ack of Twit	ter									Time Range (UTC) Mar 28 12:00 to 13	:00 *
12:00	12:05	12:10	12:15	12:20	12:25 2022-03-	12:30 28 UTC (1 minute increments	12:35	12:40	12:45	12:50	12:55	13:00
Show Read	chability / Visibility	× 104.244.42.0/24	v	•							Hide T	imelines
Reachab Percentage	ility / Visibility of Kentik's BGP vantag	e points (VPs) with ro	outes to the monitore	d prefixes (27 total VPs)								
100%					•							
50%				By Origin ASN: Mar Twitter,US (13414 RTComm,RU (83	28, 12:27): 96.3% 42): 3.7%							
<u>0%</u> 12:00	12:05	12:10	12:15	12:20	12:25 2022-03-	12:30 28 UTC (1 minute increments)	12:35)	12:40	12:45	12:50	12:55	13:00
Show AS F	Path Visualization	•								Hide ASN	Name 🗌 Hide Path	ns Graph
AS Path	Visualization aph showing all key AS	paths associated with	the monitored prefix	xes. Hover over any AS no	de or link to see	more information						
<i>8</i> в Спад	AS211396 YGROUP-AS,BE	*		68 AS1103 SURFNet (N etwork 68 AS3356 Lumen (Level3),US Lumen (Level3),US AS34854 Stackar Ca igital),IS Stackar Ca igital),IS).NL		88 88	AS8342 RTComm.RU AS13414 Twitter.US			104.244.4	2.0/24
					20	22-03-28 12:10 UTC						

Net Way Leak (2023)

- AS266970

 originated nearly
 every prefix in the
 IPv6 global table
- Lasted for ~10 mins
- Resulted in the misdirection of a significant amount of internet traffic
- Less propagation this time due to RPKI ROA (more on this in a moment)



AS Path Error



AS7007 Incident (1997)

- The OG of BGP Incidents
- Code bug caused a router inside AS7007 (MAI Network Services) to leak routes to the internet
- Existing prefixes de-aggregated to /24 prefixes and originated from AS7007
- Routes remained even after the originating router had been taken offline

Allegheny Leak (2019)

- BGP Optimizer inside DQE split 104.16.16.0/20 into two /21 prefixes
- Advertised those routes to their customer, Allegheny
- Allegheny in turn advertised upstream to Verizon
- BGP prefers a /21 over a /20 so all of the Internet connected to Verizon preferred the route through DQE



Earth Telecom Leak (2023)

- AS58715 leaked ~30k routes to its transit provider BTCL (AS17494)
- Misdirected traffic from around the world to Bangladesh
- Amazon (AS16509) prefix 13.32.249.0/24 was largest volume of misdirected traffic
- Microsoft (AS8075) prefix 20.46.144.0/20 learned from one transit provider passed to AS17494 - 85.4% propagation



IP Squatting



Bitcanal

- IP Squatting on 101.124.128.0/18 until Cogent disconnected them
- Then moved to 185.212.176.0/22 via GTT and BICS
- Used IPs as source of spam to avoid IP Blacklist



Impact of a BGP Incident



Frequency



Source: <u>https://bgpstream.com</u>

What can operators do?



We are making progress



Source: https://rpki-monitor.antd.nist.gov/

We are making progress



Source: https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/

Net Way Leak (2023)

We are making progress

ug 29th	00:10	00:20	00:30	00:40	00:50 2023-08	01:00 -29 UTC (1 minute incr	01:10 ements)	01:20	01:30	01:40	01:50	02
Show Reach	ability / Visibility	* 2a02:e	e80:4270::/48	•							🗌 Hide	Timeline
eachabi ercentage c	lity / Visibilit	Y (by Origin) rantage points (\	/Ps) with routes t	to the monitored p	refixes (206 tota	I VPs)						
%				Aug 29, 0 • NET W	00:39 (AY PROVEDOR DE	INTERNET DE CACOAL	LTDA,BR (266970):	: 60.7%				
g 29th	00:10	00:20	00:30	00:40	00:50 2023-08	01:00 -29 UTC (1 minute incr	01:10 ements)	01:20	01:30	01:40	01:50	0
ick any poir	nt on the charts to :	see the AS Paths a	t that time							Hide ASN	Name 🗌 Hide Pa	aths Gra
ick any poir S Path V twork grag	nt on the charts to 'isualization ph showing all k	see the AS Paths a	t that time ociated with the	monitored prefixes	s. Hover over any	y AS node or link to	see more inform	ation		Hide ASN	Name 🗌 Hide Pa	aths Gra
ick any poir S Path V twork grap	nt on the charts to : fisualization ph showing all k	see the AS Paths a ey AS paths ass AS37271 forkonline,ZA	t that time ociated with the	monitored prefixer	s. Hover over an	y AS node or link to	see more inform	ation		Hide ASN	Name 🗌 Hide Pa	aths Gra
lick any poir S Path V twork graj	fisualization ph showing all k db Arelio	see the AS Paths ar ey AS paths ass AS37271 forkonline,ZA AS1299 n (T arrier),SE	t that time ociated with the s	monitored prefixes	s. Hover over an	y AS node or link to	see more inform	ation		Hide ASN	Name 🗌 Hide Pa	aths Gra
ick any poir	nt on the charts to in the charts to in the charts to in the charts to in the chart of the chart	ey AS paths as AS37271 orkonline,ZA AS1299 n (T arrier),SE AS2914 T America,US	t that time	Monitored prefixes AS49544 I3D.net.NL	s. Hover over any	y AS node or link to	see more inform	ation		Hide ASN	Name 🗌 Hide Pa	aths Gr
lick any poir	nt on the charts to : fisualization ph showing all k	ey AS paths as AS37271 Jorkonline,ZA AS1299 AS2914 T America,US AS6762 m Italia Sparke,JT	t that time	AS49544 3D.net.NL Vedatore,EU	s. Hover over any	AS node or link to AS4230 0 (Embrase),BR	see more inform	ation S12357 (Spain),ES	Acco	Hide ASN	Name Hide Pr	aths Gr
lick any poir S Path V twork gray twork gray	ti on the charts to ' fisualization bh showing all k db w db Arelio db NT db Teleco	eee the AS Paths as ey AS paths as AS37271 AS1299 n (T america.US AS5162 m Italia Spanke,IT AS1762 AS174 AS174	that time	AS49544 I3D net.NL AS1273 Votatone.EU AS453 ommunications,US	5. Hover over any de Clan	AS node or link to AS4230 (Embradel),BR AS1230 Inore (Bpain),ES	See more inform	stion St2357 (Spain).ES S61678 ECA LTDA.BR	Acce	Hide ASN	Name Hide Pe	aths Gi

2a02:ee80:4270::/48 lacked a ROA

• 60.7% of BGP sources saw the leak (AS266970 as the origin)



2801:1f0:4017::/48 has a ROA that asserts AS3573 as the valid origin

• 2.4% of BGP sources saw the leak (AS266970 as the origin)

Additional Resources

- A Brief History of the Internet's Biggest BGP Incidents <u>https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/</u>
- AS7007 Incident <u>https://en.wikipedia.org/wiki/AS_7007_incident</u>
- Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net <u>https://www.wired.com/2008/02/pakistans-accid/</u>
- How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today <u>https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/</u>
- Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap <u>https://arstechnica.com/information-technology/2022/03/absence-of-malice-russian-isps-hijacking-of-twitter-ips-appears-to-be-a-goof/</u>
- Shutting Down the BGP Hijack Factory <u>https://blog.apnic.net/2018/07/12/shutting-down-the-bgp-hijack-factory/</u>
- MANRS <u>https://www.manrs.org/</u>
- How much does RPKI ROV reduce the propagation of invalid routes? <u>https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/</u>
- Exploring the Latest RPKI ROV Adoption Numbers <u>https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/</u>
- Problem Definition and Classification of BGP Route Leaks <u>https://www.ietf.org/rfc/rfc7908.txt</u>
- BGP Operations and Security <u>https://www.ietf.org/rfc/rfc7454.txt</u>
- Autonomous System Provider Authorization (ASPA) <u>https://www.ietf.org/archive/id/draft-ietf-sidrops-aspa-verification-15.txt</u>
- Unknown Attribute 23 https://labs.ripe.net/author/emileaben/unknown-attribute-28-a-source-of-entropy-in-interdomain-routing

Questions?

Thank you!

Justin Ryburn jryburn@kentik.com



@JustinRyburn





Join Kentik on Slack

