ロシアISPによる Twitter経路ハイジャックの影響調査

JANOG 51 LT

NTT コミュニケーションズ株式会社
當間 拓矢

自己紹介　當間拓矢

- AS 2914のCustomer Engineer
- Transitサービスの開通やROA管理。数年はSIerでSASEなどをやっていました。
- JANOGはこれまでオンライン参加のみ。
- サッカーを見るのが好きで Liverpoolファン。W杯惜しかった。。

- NANOG86に参加してきました！
- 「経路ハイジャックが確認されましたが、RPKIによって広範囲への経路伝搬は起こりませんでした！」で拍手喝采。

Internet impacts due to the war in Ukraine
by Doug Madory, Kentik

Twitter経路 104.244.42.0/24のタイムライン

ミャンマーISPによるハイジャックの約9ヶ月後にROAが作成された。

RADB
Last Changed

2015.07.24

AS 136168
Hijack

2021.2.5

AS 13414
Create ROA

2021.11.25

AS 8342
Hijack

2022.3.28

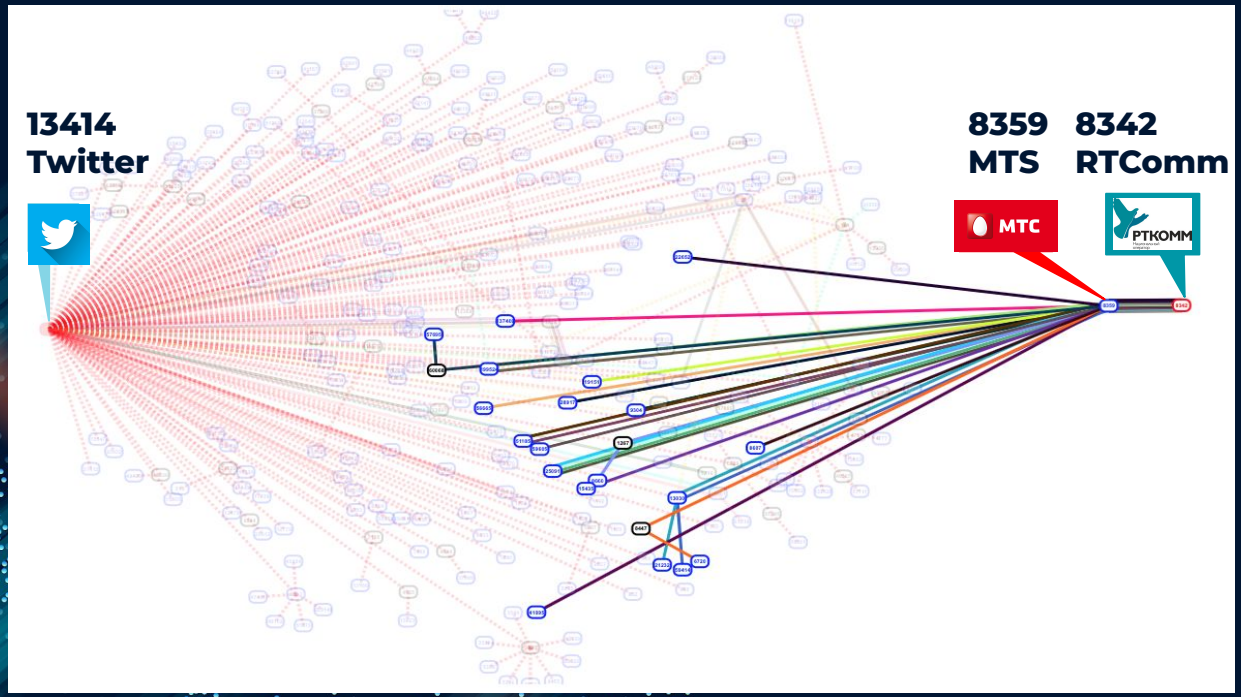
AS 8342による経路ハイジャック 2022.3.28 12:06 UTC

- AS 8342 RTCommはロシア最大手ISPのRostelecomのグループ会社。
- 複数のピアのうちAS 8359 Mobile TeleSystemsのみがinvalid経路を他ASでの伝搬。その 他のピアはドロップしたが、ROVによるものかは不明。
- AS 8359はHPによるとロシア最大のモバイル事業者。CAIDA AS RANK #45

  Looking GlassでTwitterのセグメントがプライベートASから広報されていることが確認できるため、AS 8359配下ではTwitterにアクセスできない？

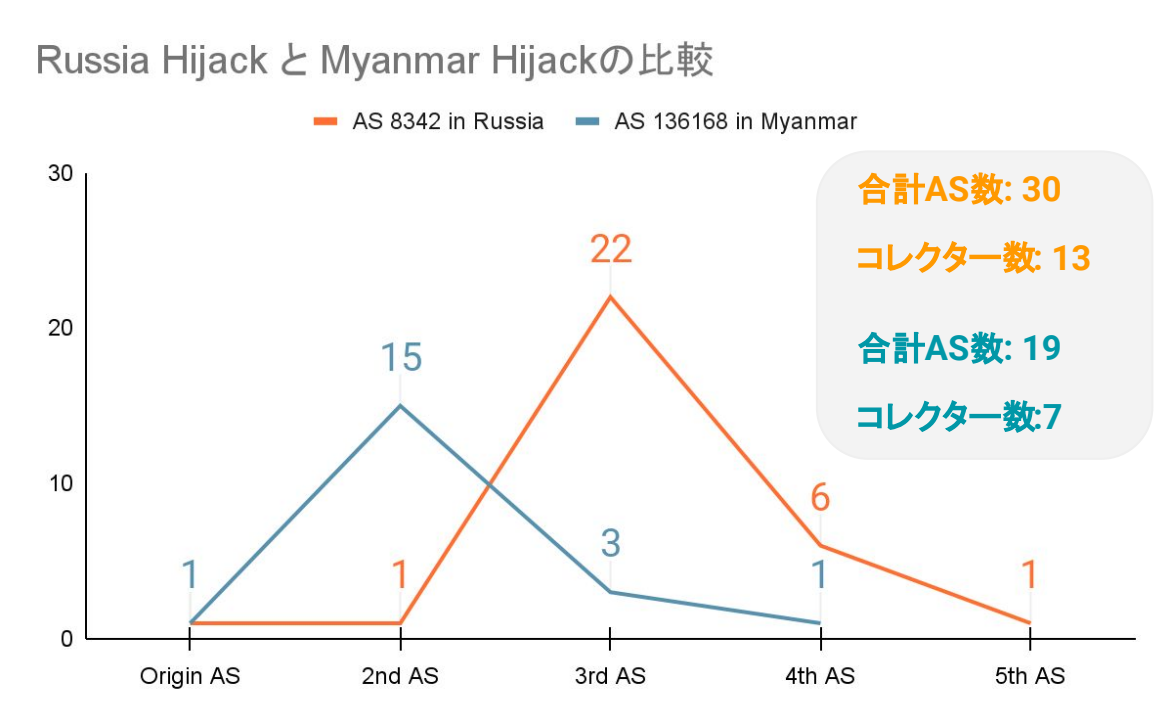
ピアAS	管理者	invalid経路の伝搬
8359	Mobile TeleSystems	複数ASに伝搬
12389	Rostelecom	X
8920	RTComm	X
25091	IP-Max	X
6939	Hurricane Electric	X

BGPlayによる影響範囲の可視化



- 左端にあるノードが本来経路を広報すべきTwitterのAS
- 薄い赤破線は影響を受けなかった経路
- 右端にあるノードがハイジャック経路を広報したRTCommのAS
- カラフルな実線はRTCommとハイジャック経路を受け取ったASを結んでいる
- 影響を受けたAS全てを示しているわけではない。

ハイジャック経路を伝搬したAS数の比較



- データソースはRISとRoute Viewsのコレクターが受信したupdateメッセージのAS-PATH
- AS-PATHのx番目に現れたASの数をプロットした。

例. AS-PATH: 22652 8359 8342
↓ 3rd ↓ 2nd ↓ Origin

- 合計値としてはROAを作成した後に起こったロシアハイジャックの方が影響を受けたAS数が多い。
- ミャンマーの時には2nd ASの数が多い。

今回の比較結果について

ROAの効果によって影響を受けたASがロシアハイジャックの方が少ないと予想したが、、、

比較に利用したデータについて

- RISとRoute Viewsのコレクターは東アジア圏だとシンガポールと東京のみ。ちなみに東京ではinvalid経路を観測しなかった。
- 一方、ヨーロッパ圏の IXにはコレクターが多いのでロシアハイジャックの方が比較的細かいデータが取れている。

考察

- Tier1等のROV導入で上流からのハイジャックリスクは低くなってきている？パブリックピア等を経由したinvalid経路のリスクは続くのでは。ROA登録、ROVの導入を。
- AS8359 MTSのような大規模なASがハイジャックに関わると厄介。実際に 2023年1月現在も複数のASがMTSを経由してinvalid経路を広報している。監視には PacketVisが便利。BGP、RPKIのリアルタイム監視＆通知ツール PacketVisを使ってみた (hatenablog.com)

教えてください！

- JANOG Slack #03_自己紹介に現れているのでコメントいただけると嬉しいです！