Investigating Autonomous Systems Behavior in Russia and Ukraine using GRIP

Aviva Smith

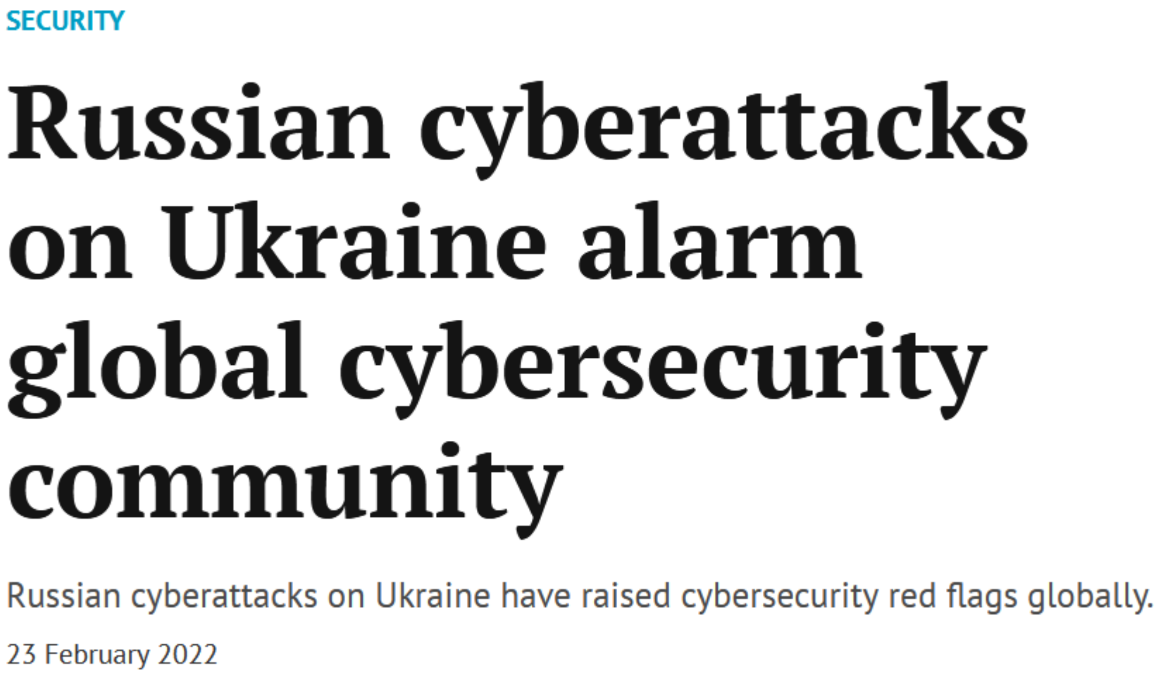
Georgia Tech

Presentation Overview

- Project Relevance
- Topic + Methodology Review
- GRIP Overview
- Methology
    - Documentation Parameters
    - Pulling data from API using curl queries
    - Parsing .json files (file parsing, type data accessed, challenges)
    - Event Tags
- Interesting Results
- Future Work

Project Relevance

- Pre-invasion on Feb. 24, 2022, Russia allegedly launched several cyberattacks targeting Ukraine's critical infrastructure
- Upon further investigation, none of these alleged attacks could be definitively classified as BGP Hijacking Attacks, even if behavior was Suspicious.
- Nature of attacks cannot always be proven malicious, even if behavior is suspicious
- Possible Reasons:
  - Cyberattack could trigger military action on the part of Ukrainian alies
  - Russian motives possibly more focused on razing country to rebuild
  - Cyberattacks occurring, but not detected as focus on more espionage related activities



SECURITY

Russian cyberattacks on Ukraine alarm global cybersecurity community

Russian cyberattacks on Ukraine have raised cybersecurity red flags globally.

23 February 2022

Topic + Methodology

Topic: Investigate BGP data from 2022 and determine if there was an increase in suspicious behavior of ASes in Ukraine and Russia pre-invasion

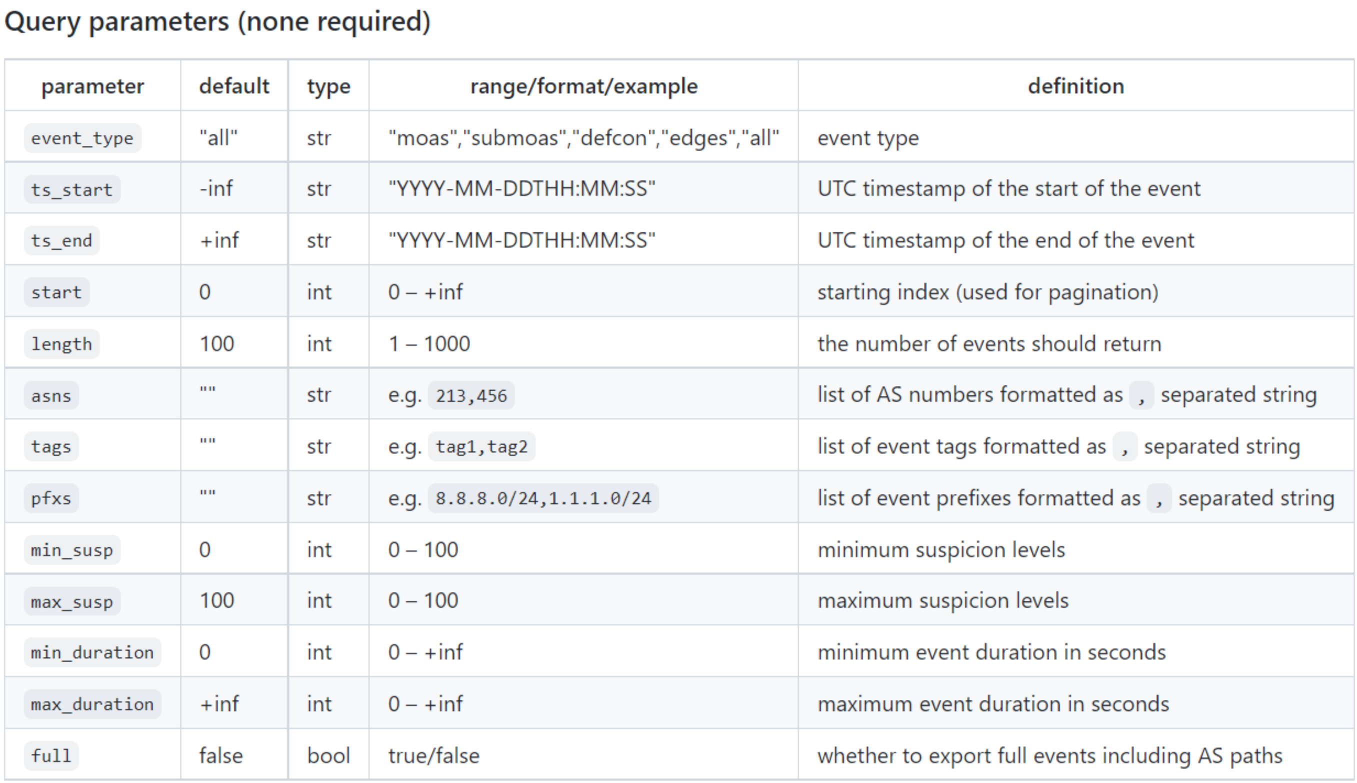
- **Learn how GRIP API works**
- **Create notebook for interacting with GRIP API**
- **Use CURL bindings to make an HTTP query to return data collected over last two months**
- **Write python script to parse output (.json files)**
- **Determine if data returned by query includes nationality information**
  - **Yes! Geographic Information returned by GRIP API**
- **Graphically visualize notable trends (if any)**
- **Bonus: Investigate behavior that constitutes increase in activity**

GRIP

- System that continuously monitors BGP data for attacks
  - From Route Views and RIPE RIS
- Detects different types of attacks (MOAS, SUBMOAS, Defcon, NewEdge)
- Tags attack events with labels
  - Information on ASN history, path, fat-finger, ASN type, blacklist, prefix, AS relationship, RPKI
- Infers a risk level for the event

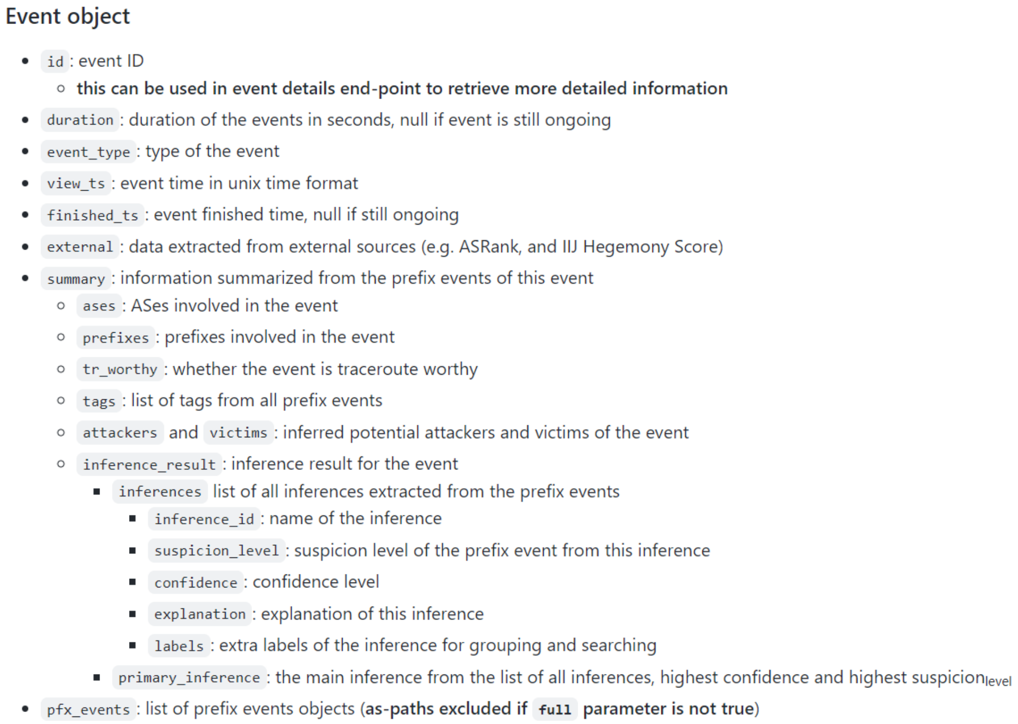
GRIP API Documentation Parameters

- Access UI: GRIP - Global Routing Intelligence Platform (gatech.edu)
- API Documentation: grip-api/api-spec.md at master · InetIntel/grip-api · GitHub



Query parameters (none required)

parameter	default	type	range/format/example	definition
`event_type`	"all"	str	"moas","submoas","defcon","edges","all"	event type
`ts_start`	-inf	str	"YYYY-MM-DDTHH:MM:SS"	UTC timestamp of the start of the event
`ts_end`	+inf	str	"YYYY-MM-DDTHH:MM:SS"	UTC timestamp of the end of the event
`start`	0	int	0 – +inf	starting index (used for pagination)
`length`	100	int	1 – 1000	the number of events should return
`asns`	""	str	e.g. `213,456`	list of AS numbers formatted as `,` separated string
`tags`	""	str	e.g. `tag1,tag2`	list of event tags formatted as `,` separated string
`pfxs`	""	str	e.g. `8.8.8.0/24,1.1.1.0/24`	list of event prefixes formatted as `,` separated string
`min_susp`	0	int	0 – 100	minimum suspicion levels
`max_susp`	100	int	0 – 100	maximum suspicion levels
`min_duration`	0	int	0 – +inf	minimum event duration in seconds
`max_duration`	+inf	int	0 – +inf	maximum event duration in seconds
`full`	false	bool	true/false	whether to export full events including AS paths



Event object

- `id` : event ID
  - **this can be used in event details end-point to retrieve more detailed information**
- `duration` : duration of the events in seconds, null if event is still ongoing
- `event_type` : type of the event
- `view_ts` : event time in unix time format
- `finished_ts` : event finished time, null if still ongoing
- `external` : data extracted from external sources (e.g. ASRank, and IIJ Hegemony Score)
- `summary` : information summarized from the prefix events of this event
  - `ases` : ASes involved in the event
  - `prefixes` : prefixes involved in the event
  - `tr_worthy` : whether the event is traceroute worthy
  - `tags` : list of tags from all prefix events
  - `attackers` and `victims` : inferred potential attackers and victims of the event
  - `inference_result` : inference result for the event
    - `inferences` list of all inferences extracted from the prefix events
      - `inference_id` : name of the inference
      - `suspicion_level` : suspicion level of the prefix event from this inference
      - `confidence` : confidence level
      - `explanation` : explanation of this inference
      - `labels` : extra labels of the inference for grouping and searching
    - `primary_inference` : the main inference from the list of all inferences, highest confidence and highest suspicion level
- `pfx_events` : list of prefix events objects (**as-paths excluded if `full` parameter is not true**)

Pulling Data using Curl Queries

Curl URL Queries are constructed with the follow:

- **HTTP hosting API**
- **Number of Events Queried**
- **Start Date**
- **End Date**
- **Minimum Suspicious and Maximum Suspicion**
- **Event Type**

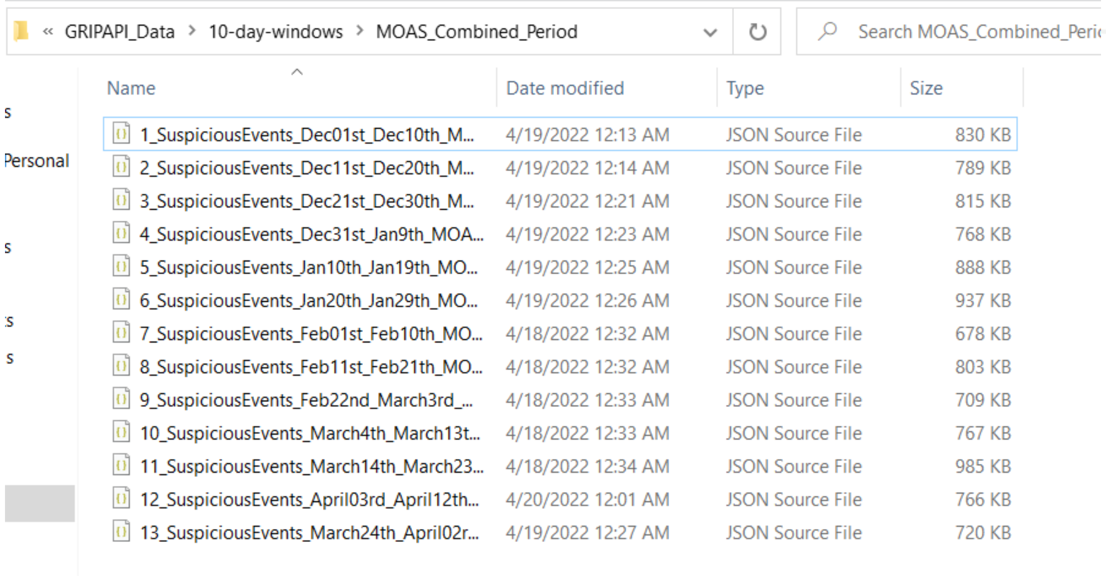
Example: MOAS EVENTS 2.01.22 -> 2.10.22

```
curl https://api.grip.inetintel.cc.gatech.edu/dev/json/events?length=100&start=0&ts_start=2022-02-01T19%3A03&ts_end=2022-02-10T19%3A03&min_susp=80&max_susp=100&event_type=moas
```

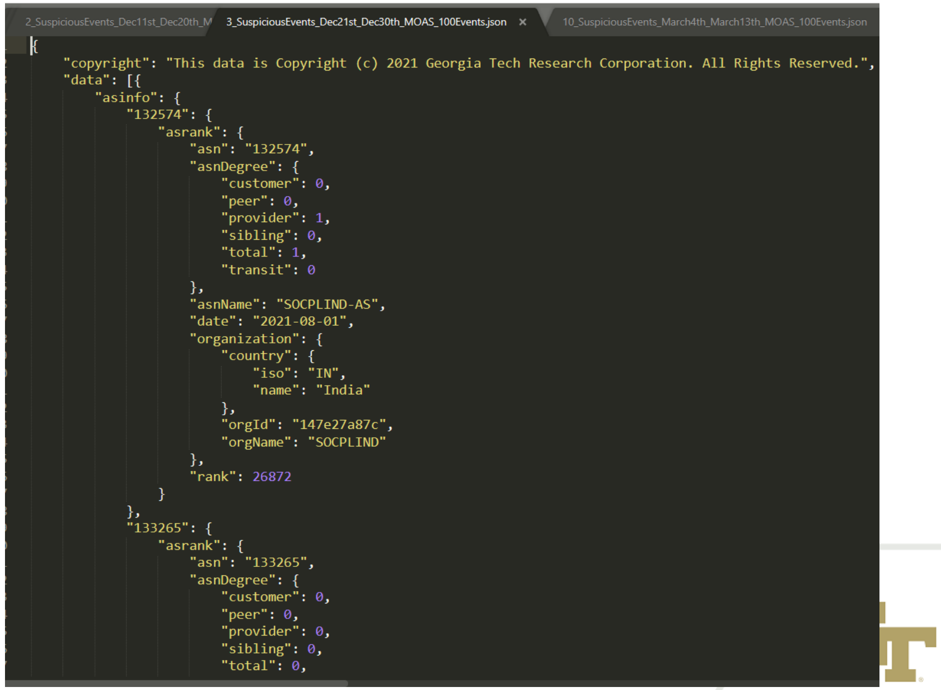
APIs for Running Curl Query with Good Formatting:
https://reqbin.com/req/c-g95rmxs0/curl-for-windows

Parsing API Data

- File Parsing
  - Saved .json files locally
  - Accessed files from Notebook
  - Accessed data according to metadata descriptions provided on API documentation
- Brief Walkthrough of notebook
- Challenges
  - A LOT of data available -> took time to parse through
  - Gaps in available information for even entry -> code optimized to handle this case
  - Investigating UI and API
  - What data is relevant to Ukraine-Russian conflict?

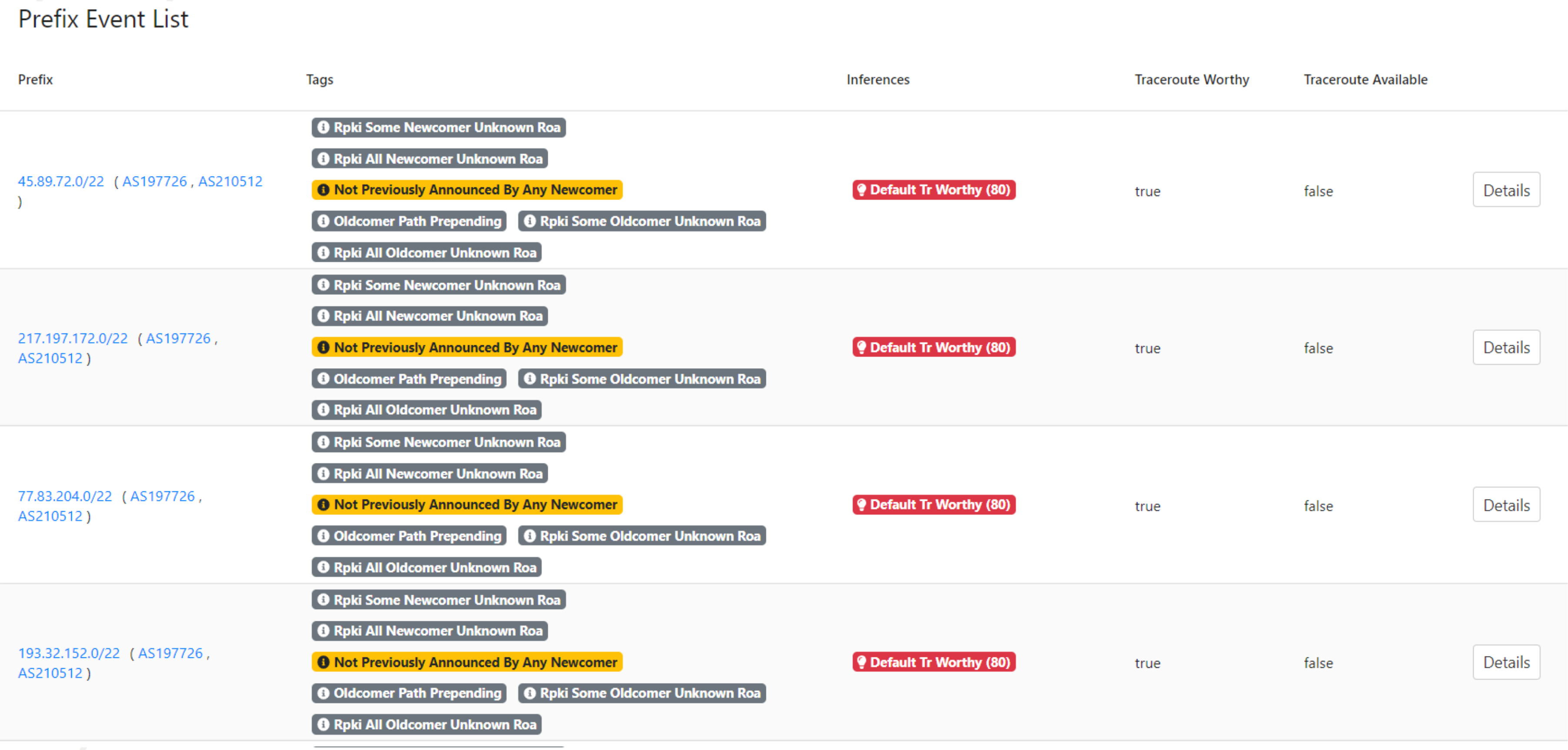

« GRIPAPI_Data › 10-day-windows › MOAS_Combined_Period
Search MOAS_Combined_Peri
s
Personal
s
s
s

Name	Date modified	Type	Size
1_SuspiciousEvents_Dec01st_Dec10th_M...	4/19/2022 12:13 AM	JSON Source File	830 KB
2_SuspiciousEvents_Dec11st_Dec20th_M...	4/19/2022 12:14 AM	JSON Source File	789 KB
3_SuspiciousEvents_Dec21st_Dec30th_M...	4/19/2022 12:21 AM	JSON Source File	815 KB
4_SuspiciousEvents_Dec31st_Jan9th_MOA...	4/19/2022 12:23 AM	JSON Source File	768 KB
5_SuspiciousEvents_Jan10th_Jan19th_MO...	4/19/2022 12:25 AM	JSON Source File	888 KB
6_SuspiciousEvents_Jan20th_Jan29th_MO...	4/19/2022 12:26 AM	JSON Source File	937 KB
7_SuspiciousEvents_Feb01st_Feb10th_MO...	4/18/2022 12:32 AM	JSON Source File	678 KB
8_SuspiciousEvents_Feb11st_Feb21th_MO...	4/18/2022 12:32 AM	JSON Source File	803 KB
9_SuspiciousEvents_Feb22nd_March3rd_...	4/18/2022 12:33 AM	JSON Source File	709 KB
10_SuspiciousEvents_March4th_March13t...	4/18/2022 12:33 AM	JSON Source File	767 KB
11_SuspiciousEvents_March14th_March23...	4/18/2022 12:34 AM	JSON Source File	985 KB
12_SuspiciousEvents_April03rd_April12th...	4/20/2022 12:01 AM	JSON Source File	766 KB
13_SuspiciousEvents_March24th_April02r...	4/19/2022 12:27 AM	JSON Source File	720 KB


2_SuspiciousEvents_Dec11st_Dec20th_M
3_SuspiciousEvents_Dec21st_Dec30th_MOAS_100Events.json ×
10_SuspiciousEvents_March4th_March13th_MOAS_100Events.json

```
{
    "copyright": "This data is Copyright (c) 2021 Georgia Tech Research Corporation. All Rights Reserved.",
    "data": [{
        "asinfo": {
            "132574": {
                "asrank": {
                    "asn": "132574",
                    "asnDegree": {
                        "customer": 0,
                        "peer": 0,
                        "provider": 1,
                        "sibling": 0,
                        "total": 1,
                        "transit": 0
                    },
                    "asnName": "SOCPLIND-AS",
                    "date": "2021-08-01",
                    "organization": {
                        "country": {
                            "iso": "IN",
                            "name": "India"
                        },
                        "orgId": "147e27a87c",
                        "orgName": "SOCPLIND"
                    },
                    "rank": 26872
                }
            },
            "133265": {
                "asrank": {
                    "asn": "133265",
                    "asnDegree": {
                        "customer": 0,
                        "peer": 0,
                        "provider": 0,
                        "sibling": 0,
                        "total": 0,
```

Tags



Prefix Event List

Prefix	Tags	Inferences	Traceroute Worthy	Traceroute Available	
45.89.72.0/22 (AS197726 , AS210512)	Rpki Some Newcomer Unknown Roa Rpki All Newcomer Unknown Roa Not Previously Announced By Any Newcomer Oldcomer Path Prepending Rpki Some Oldcomer Unknown Roa Rpki All Oldcomer Unknown Roa	Default Tr Worthy (80)	true	false	Details
217.197.172.0/22 (AS197726 , AS210512)	Rpki Some Newcomer Unknown Roa Rpki All Newcomer Unknown Roa Not Previously Announced By Any Newcomer Oldcomer Path Prepending Rpki Some Oldcomer Unknown Roa Rpki All Oldcomer Unknown Roa	Default Tr Worthy (80)	true	false	Details
77.83.204.0/22 (AS197726 , AS210512)	Rpki Some Newcomer Unknown Roa Rpki All Newcomer Unknown Roa Not Previously Announced By Any Newcomer Oldcomer Path Prepending Rpki Some Oldcomer Unknown Roa Rpki All Oldcomer Unknown Roa	Default Tr Worthy (80)	true	false	Details
193.32.152.0/22 (AS197726 , AS210512)	Rpki Some Newcomer Unknown Roa Rpki All Newcomer Unknown Roa Not Previously Announced By Any Newcomer Oldcomer Path Prepending Rpki Some Oldcomer Unknown Roa Rpki All Oldcomer Unknown Roa	Default Tr Worthy (80)	true	false	Details

Tags are useful for investigating an event more closely. For example, a prefix with the tag “Not Previously Announced by Any Newcomer” could indicate that some new prefix yet to be explored is being advertised.

Review of Notebooks

- MOAS_Ukraine_Russia_Exploration - Jupyter Notebook
- SUBMOAS_Ukraine_Russia_Exploration - Jupyter Notebook

Project Takeaways

- Based on although an increase in activity, no malicious activity launched by Russia or any other country against Ukraine has definitively detected -> Closer inspection required
- More subMOAS activity than MOAS activity recorded in region
- Super_pfx and Sub_prefix do not indicate especially malicious activity
- Notable frequently occurring tags:
  - 'some-newcomers-stub-ases’
  - 'some-newcomer-announced-no-pfxs’
  - 'all-origins-same-country’
  - 'all-newcomer-announced-no-pfxs’
  - 'not-previously-announced-by-any-newcomer’

Remaining Work

- Finish pulling data for December and January for subMOAS events
- Take a closer look at the available tags, especially on subMOAS events to determine if malicious behavior is detected.
- Investigate activity other countries in regions (Beleru, Romania, Poland, Moldova, Slovakia)
- Investigate if especially suspicious prefixes were advertised in subMOAS data
- Investigate relationship between organizations hosting ASes

Sweden
Estonia
Latvia
Russian Federation
Baltic Sea
Lithuania
Belarus
Germany
Poland
Czech Republic
Ukraine
Slovakia
Austria
Moldova
Hungary
Slovenia
Romania
Croatia
Bosnia and Herzegovina
Serbia
Black Sea
Bulgaria
Kosovo
Italy
Monte-negro
Macedonia
Turkey
Albania
Greece