BGP ATTACK ANALYSIS

Research project supported by the Security Lab of EPITA (LSE).

BOKOWY Théo
LAMARCHE Dorian
PAURON Nathan
ROCHAT Coline

HYPOTHESIS :

Can we support data analysts in their interpretation by creating an automatic detection process relying on the state-of-the-art tool Tabi ?

OUR GOAL :

- Gather data in real time
- Detect BGP hijacks
- Build pretty graph :)
- Implement alerting bot
- Automate the process

COLLECTING DATA : RIPE

Collect BGP announcements as MRT files (routing data export format).
Dataset is updated every 5min.

Source : **rrc21.ripe.net** at Paris, France

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

PARSING MRT FILES : MABO

Transpose MRT data into usable input for Tabi.

Output :
- update_xxx.json

ANSSI

HIJACK DETECTION : TABI

Compute data and highlights routing anomalies, aka hijacks.

Output :
- all.default.json
- all.hijacks.json
- all.routes.json

ANSSI

BUILD THE GRAPH : IGRAPH

Transpose hijacks and routes into a drawable graph.
iGraph is a python library.

Output :
- routes.graphML

DISPLAY THE GRAPH : GEPHI

Implements Leiden algorithm for community computation.
Graphical tool for metrics managment.

Output :
- export.svg

RESULT AND ALERTING :

A WRAPPING TOOL TO AUTOMATE THE DETECTION PROCESS.

All results are stored as log files containing all alerts for each 5min frame.

For each hijack, we export :
- the legit AS ID
- the current AS ID (corrupted)
- more network data

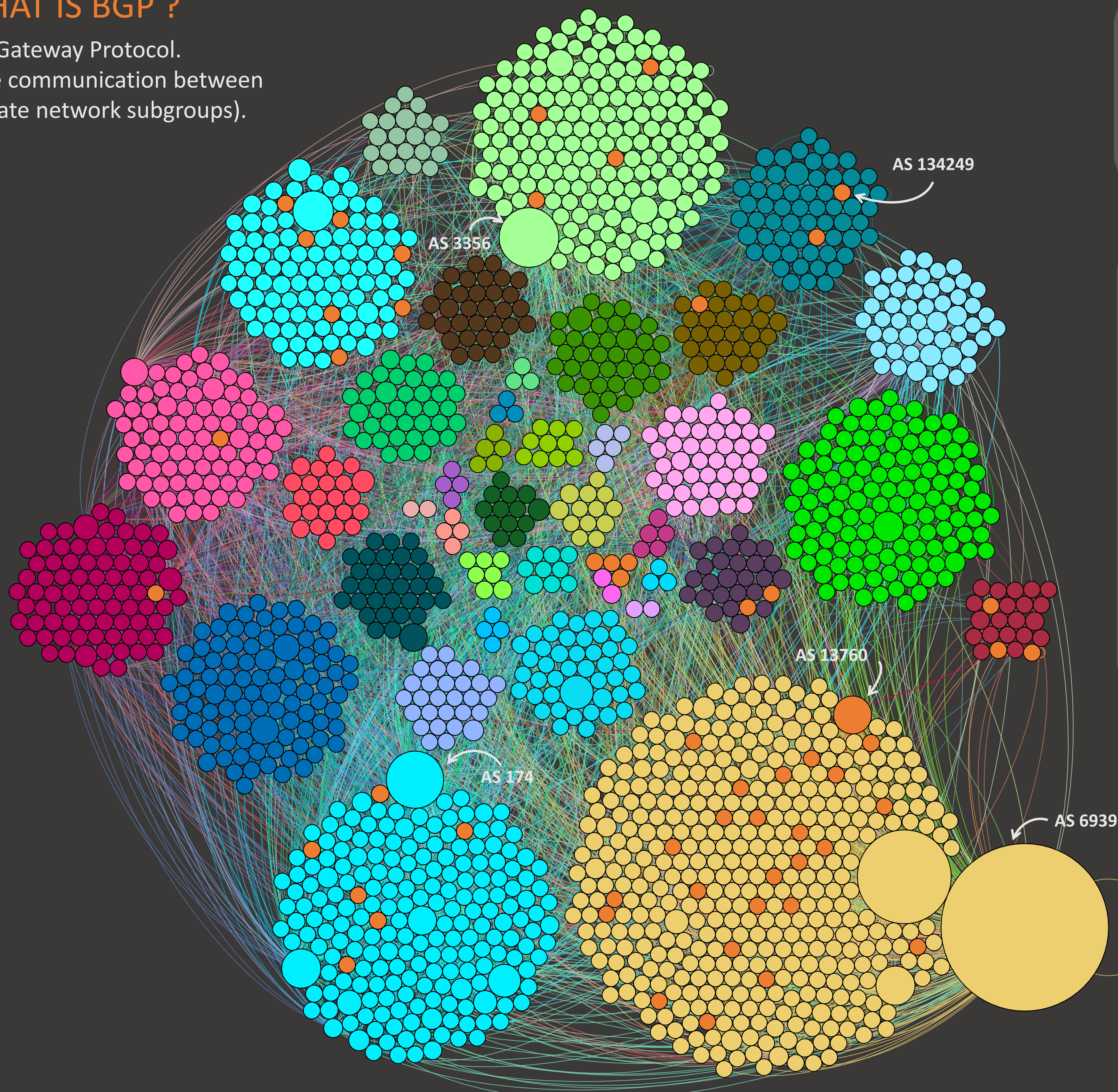
DISCORD BOT :
Display informations for one or all hijacks

MAIL ALERTING :
Send informations for all hijacks

WHAT IS BGP ?

Border Gateway Protocol.
Manage communication between AS (private network subgroups).

HIJACKED BGP NETWORK GRAPH



● HIJACKS
● LEGIT AS
⌒ ROUTES

AS 6939 :
Hurricane Electric LLC

AS 174 :
Cogent Communications

AS 3356 :
Level 3 Parent, LLC

AS 13760 : hijacked
Unity Fiber Holdings Inc.

AS 134249 : hijacked
Margo Networks Pvt Ltd.

We'd like to give our warmest thanks to **Sébastien Larinier** and **Badis Hammi** for guiding us through all the steps of this project.

THANK YOU

SEE OUR GITHUB

bgpaa.epita2021@gmail.com