

BGP-Monitor

TLP:CLEAR



CIRCL

Computer Incident
Response Center
Luxembourg

Jean-Louis Huynen

LUNOG5 16/11/2022

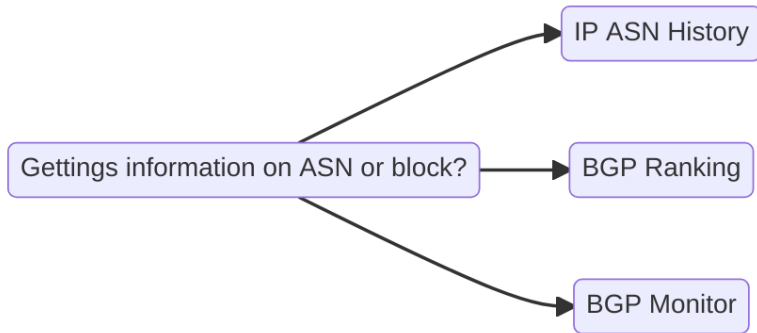
Agenda

- A tour of BGP-related tools at CIRCL
- Introducing BGP-Monitor
- Pushing to AIL
- Pushing to MISP
- Future works

About CIRCL

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.
- As such CIRCL has interest in network monitoring for threat detection and incident response purposes.
- For our constituencies as well as international partners.

About CIRCL - BGP related projects



IPASN history

- Find the ASN announcing a IP and the closest prefix in a specific time range.
- Uses CAIDA and RIPE dumps
- Open source project¹
- Public instance²
- Python API³
- Python API reference⁴

¹<https://github.com/D4-project/IPASN-History/>

²https://bgpranking-ng.circl.lu/ipasn_history/

³<https://github.com/D4-project/pyipasnhistory>

⁴https://pyipasnhistory.readthedocs.io/en/latest/api_reference.html

BGP Ranking

- Compute a ASN trust score based on existing datasets of compromised systems:
 - known malware C&C, botnets, SSL scanning,
 - from abuse.ch, malc0de, dshield, shadowserver, etc.

$\text{sum}(\text{IP} * \text{weight of the list})$

$\text{sum}(\text{IP announced by the ASN})$

Figure 1: formula

- Open Source project⁵
- Public Instance⁶

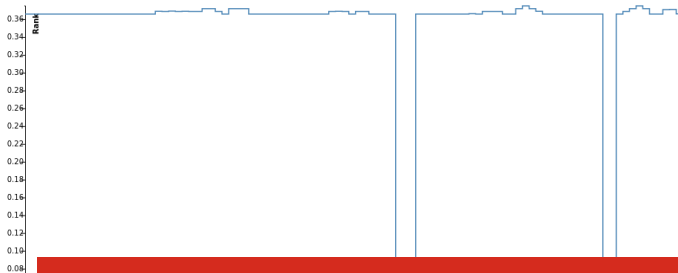
⁵<https://github.com/D4-project/BGP-Ranking>

⁶<http://bgpranking.circl.lu/>

BGP Ranking

Timestamp	ASN Description
2018-04-13T15:15:40+00:00	ROSTBANK-NET, RU
2019-10-10T14:17:20+00:00	-Reserved AS-, ZZ
2020-09-02T07:14:59+00:00	FASTLINES, IT

Prefix	Rank
185.156.232.0/22	0.3662109375



BGP Monitor

- A new tool to react to suspicious network changes.
- Work on streams of BGP announces with some must-haves:
 - Being able to monitor by country
 - Work on streams of data
 - Close to real time
 - Keep (our own) history
- Constituency challenge:
 - Monitoring a list of .LU AS is not enough as a CERT
 - Some constituencies have pool of addresses in remote AS
 - We don't know how Geolocation services like maxmind⁷ work

⁷<https://www.maxmind.com/en/home>

Enter Geo Open

- Home-grown geolocation database (AS announces, whois, some other ideas ^-^)
- Available in open data⁸
- Compatible with maxmind MMDB format⁹ and libraries¹⁰
- We provide mmdb-server¹¹ to build web services around Geo Open..
- Geo open Public instance¹²
- Current ip lookup ¹³

⁸<https://data.public.lu/fr/datasets/geo-open-ip-address-geolocation-per-country-in-mmdb-format/>

⁹<https://maxmind.github.io/MaxMind-DB/>

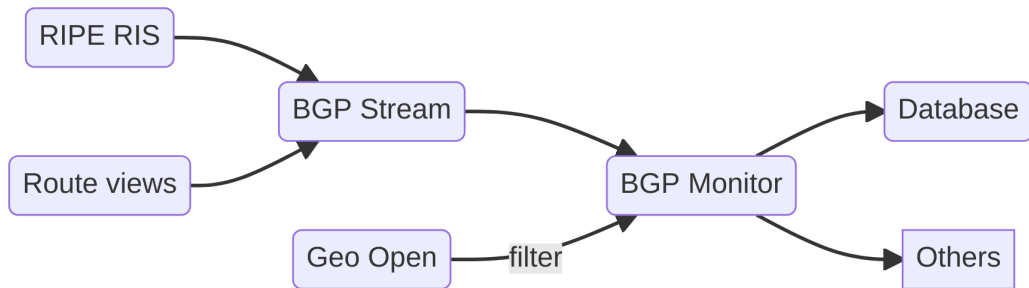
¹⁰<https://github.com/maxmind/MaxMind-DB-Reader-python>

¹¹<https://github.com/adulau/mmdb-server>

¹²<https://ip.circl.lu/geolookup/8.8.8.8>

¹³<https://ipv4.circl.lu/>

BGP-monitor



- Leverage BGP stream for stream collection¹⁴

¹⁴<https://bgpstream.caida.org>
10 of 26

BGP-monitor

- A simple CLI that:
 - Filter broker streams roughly as BGPreader¹⁵ does
 - Filter by countries according to Geo open
 - Outputs to files and column-based RDBM
 - Clickhouse¹⁶, and QuestDB¹⁷ are supported
- Available on github¹⁸

¹⁵<https://bgpstream.caida.org/docs/tools/bgpreader>

¹⁶<https://github.com/ClickHouse/ClickHouse>

¹⁷<https://github.com/questdb/questdb>

¹⁸<https://github.com/D4-project/bgp-monitor/>

BGP-monitor

And now what?

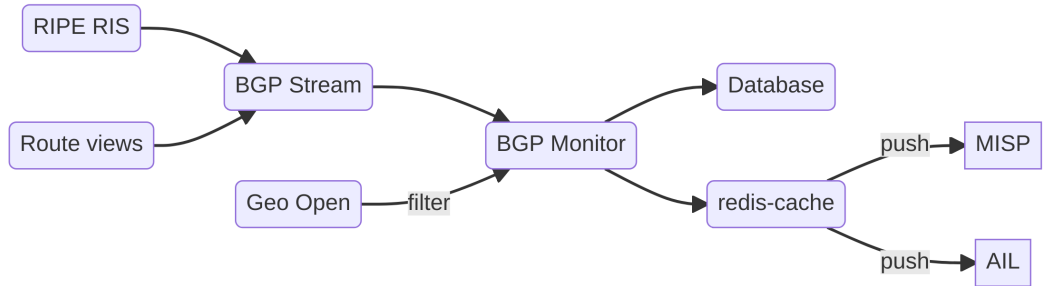
- It would be nice to have visualisation.

BGP-monitor

And now what?

- It would be nice to **react** to route changes.
 - Check reachability
 - Check for the announcer's reputation
 - Scan the subnet to check for changes

BGP-monitor

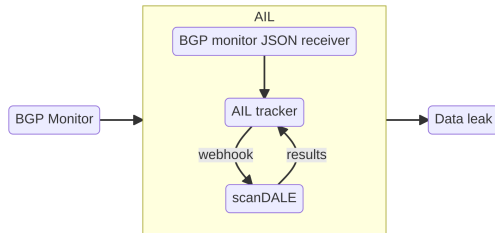


BGP-monitor in AIL



ail project

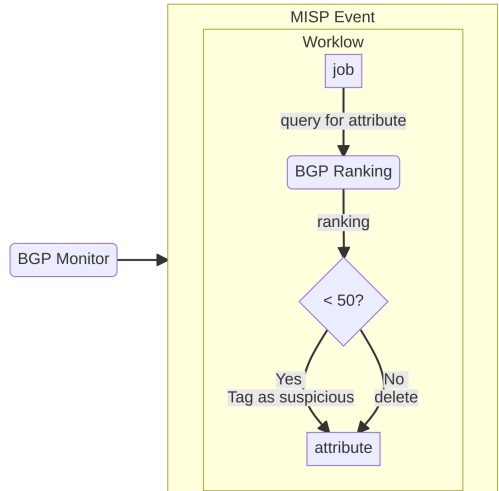
- Data Leak Prevention
- Scan network:
 - search for interesting bits (newly announced networks)
 - spot attacker's infrastructure
 - vulnerable hosts (Exchange servers ^-^).
- opt-in service for constituencies and international partners.



BGP-monitor in MISP



- Why MISP?
 - **Correlate**
 - Investigate changes,
 - Tag announces that come from suspicious AS (via BGP Ranking)
 - Share activities that are deemed suspicious



BGP-monitor in MISP - Workflows ?

- A mini SOAR in MISP
- Alleviate the need to use:
 - PyMISP¹⁹ and MISP API
 - cron jobs
 - PubSub Channels?
- Enable users to create and share automations tasks
- Allow for preventing a behavior
- Enable callbacks
- Visual dataflow programming with a drag and drop editor!

¹⁹<https://pymisp.readthedocs.io>

BGP-monitor in MISP - Triggers ?

Triggers



















































List the available triggers that can be listened to by workflows.

Missing a trigger? Feel free to open a [Github issue!](#)

[Documentation and concepts](#)

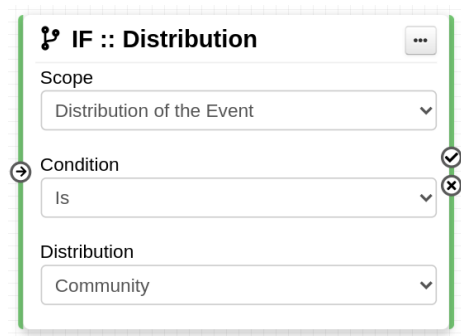
« previous

next »

Trigger name	Scope	Trigger overhead	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions
 Attribute After Save	attribute	high ?	83	×	✓	160	2022-08-03 09:00:41	<input type="checkbox"/>	×	   
 Enrichment Before Query	others	low	1154	✓	✓	162	2022-10-17 12:35:57	<input type="checkbox"/>	✓	   
 Event After Save	event	high ?	49	×	✓	175	2022-10-14 13:32:01	<input type="checkbox"/>	✓	   
 Event After Save New	event	low	5	×	✓	182	2022-10-17 09:12:14	<input checked="" type="checkbox"/>	✓	   
 Event After Save New From Pull	event	low	6	×	✓	183	2022-10-17 09:01:36	<input checked="" type="checkbox"/>	✓	   
 Event Publish	event	low	126	✓	✓	180	2022-10-13 10:42:53	<input checked="" type="checkbox"/>	✓	   
 Object After Save	object	high ?	35	×	✓	161	2022-08-05 07:12:52	<input type="checkbox"/>	×	   
 Post After Save	post	low	36	×	×	176	2022-07-28 13:59:51	<input type="checkbox"/>	×	   
 User After Save	user	low	0	×	×	181	2022-08-05 07:19:46	<input type="checkbox"/>	×	   
 User Before Save	user	low	42	✓	×	158	2022-07-28 14:00:32	<input type="checkbox"/>	×	   

BGP-monitor in MISP - Conditions ?


- If:
 - An MISP Event is tagged with tlp:red
 - The distribution an Attribute is a sharing group
 - The creator organisation is circl.lu
 - Or any other generic conditions



The screenshot shows a configuration window titled "IF :: Distribution" with a menu icon on the left and a close icon on the right. The window contains three sections, each with a dropdown menu:


- Scope:** A dropdown menu showing "Distribution of the Event".
- Condition:** A dropdown menu showing "Is". To the right of this section are two circular icons: a checkmark and an 'X'.
- Distribution:** A dropdown menu showing "Community".

BGP-monitor in MISP - Actions ?

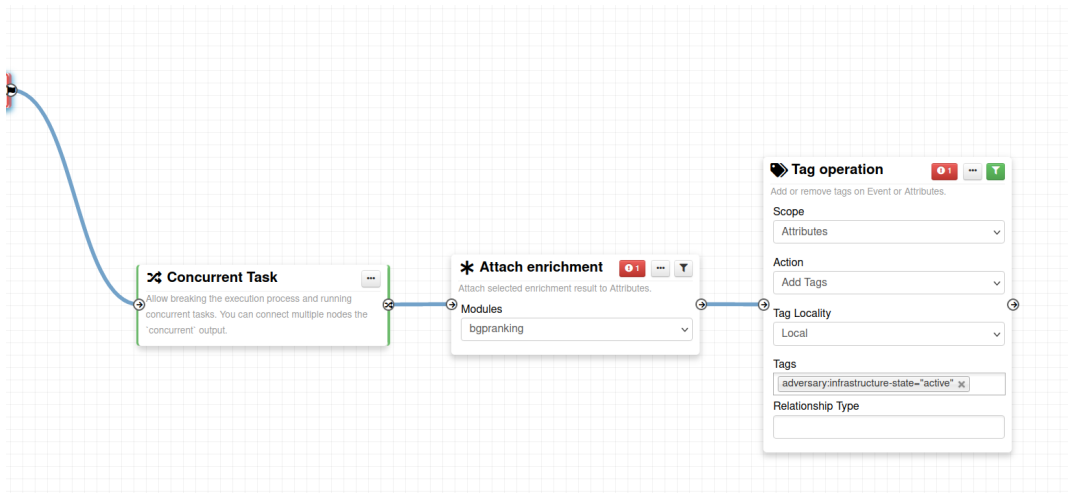
<div>All Action Logic misp-module Custom Blocking Enabled Disabled</div>								<div>Enter value to search Filter X</div>	
<input type="checkbox"/>	Module name	Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions	
<input type="checkbox"/>	 Blueprint action module	action	x	x	x	✓	✓	 	
<input type="checkbox"/>	 Enrich Event	action	x	✓	x	x	✓	 	
<input type="checkbox"/>	 mattermost	action	x	x	✓	x	✓	 	
<input type="checkbox"/>	 MS Teams Webhook	action	x	x	x	x	✓	 	
<input type="checkbox"/>	 Push to ZMQ	action	x	x	x	x	✓	 	
<input type="checkbox"/>	 Send Mail	action	x	x	x	x	✓	 	
<input type="checkbox"/>	 Stop execution	action	✓	x	x	x	✓	 	
<input type="checkbox"/>	 Tag operation	action	x	✓	x	x	✓	 	
<input type="checkbox"/>	 testaction	action	x	x	✓	x	✓	 	
<input type="checkbox"/>	 Webhook	action	x	x	x	x	✓	 	

BGP-monitor in MISP

Workflow blueprint view

Name	Set tag based on BGP Ranking maliciousness level
ID	17
UUID	4d426fce-26da-4c5d-a4f5-0d99377ba43a
Timestamp	1668498644
Description	[event-publish] Set tag based on BGP Ranking maliciousness level. A threshold of 50 is set by default but can be modified.
Preview	 <pre>graph LR; A[Event Publish] --> B[Concurrent Task]; B --> C[Attach enrichment]; C --> D[Tag operation]</pre>
Data	<pre>[{ "id": 1, "name": "Event Publish", "data": { "id": "event-publish", "scope": "event", "name": "Event Publish", "description": "This trigger is called just before a MISP Event starts the publishing process", "icon": "upload",</pre>

BGP-monitor in MISP



BGP-monitor in MISP

Node Filtering



Element selector

Event._AttributeFlattened.{n}

Value

float

Operator

Equals



Hash Path

.Object.{n}[name=bgp-ranking].Attribute.{n}[object_relation=position][value<50].type

Save

Close

Roadmap of what is to come

- Better exploitation of the collected data:
 - BGPlay²⁰ compatible web socket server to replay announces
- Actual infrastructure scanning on suspicious changes (scanDALE²¹)
- Create Announces baseline and smarter alerts
- Create MISP warning list from BGP rankings

²⁰<https://bgplay.massimocandela.com/>

²¹<https://github.com/scandale-project>

Credits and References

- Raphaël Vinot - BGP Ranking / IP ASN History
- Alexandre Dulaunoy - Geo Open
- Enes Usta - BGP-Monitor
- David Cruciani - BGP-Monitor
- Sami Mokaddem - BGP Ranking MISP workflow
- Luciano Righetti - Grafana dashboard
- <https://d4-project.org>
- <https://misp-project.org>
- <https://ail-project.org>



**Co-financed by the Connecting Europe
Facility of the European Union**