BGP Link Reputation Evaluator

An Algorithm based tool to identify *legitimate* or *malicious/hijack* BGP link

Alfred Arouna[1] Lionel Metongnon[2] Pr. Marc Lobelle[3]

[12]Université d'Abomey-Calavi,[23]Université Catholique de Louvain
[1]alfred@arouna.net,[2]lionel.metongnon@uclouvain.be,[3]marc.lobelle@uclouvain.be

AfPIF 2017 - 22,23,24 August 2017 - Abidjan, Côte D'Ivoire

Disclamer

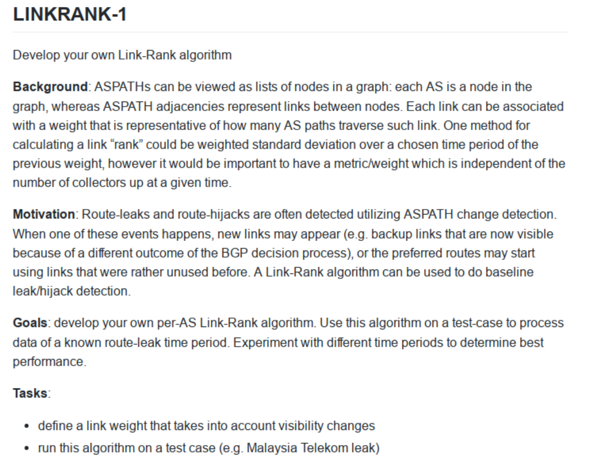
- Ongoing study...
- Community input to improve current result.
- Code not yet ready for production (alpha release).
- Code available at: `https://bitbucket.org/alfredarouna/bgplink`

Outline

1. Base Idea
2. Tools
3. Our proposal
4. Hypothesis & verification
5. Malaysia Telecom test cases results
6. Other tests cases results
7. Improvement (proposals)

Base Idea

Linkrank Challenge from CAIDA BGP Hackathon



LINKRANK-1

Develop your own Link-Rank algorithm

Background: ASPATHs can be viewed as lists of nodes in a graph: each AS is a node in the graph, whereas ASPATH adjacencies represent links between nodes. Each link can be associated with a weight that is representative of how many AS paths traverse such link. One method for calculating a link "rank" could be weighted standard deviation over a chosen time period of the previous weight, however it would be important to have a metric/weight which is independent of the number of collectors up at a given time.

Motivation: Route-leaks and route-hijacks are often detected utilizing ASPATH change detection. When one of these events happens, new links may appear (e.g. backup links that are now visible because of a different outcome of the BGP decision process), or the preferred routes may start using links that were rather unused before. A Link-Rank algorithm can be used to do baseline leak/hijack detection.

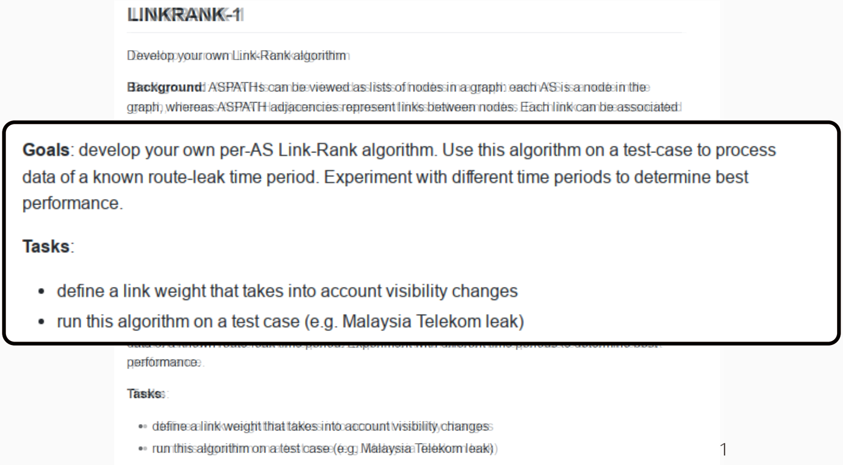
Goals: develop your own per-AS Link-Rank algorithm. Use this algorithm on a test-case to process data of a known route-leak time period. Experiment with different time periods to determine best performance.

Tasks:

- define a link weight that takes into account visibility changes
- run this algorithm on a test case (e.g. Malaysia Telekom leak)

1

Linkrank Challenge from CAIDA BGP Hackathon



LINKRANK-1

Develop your own Link-Rank algorithm

Background: ASPATHs can be viewed as lists of nodes in a graph: each AS is a node in the graph, whereas ASPATH adjacencies represent links between nodes. Each link can be associated

Goals: develop your own per-AS Link-Rank algorithm. Use this algorithm on a test-case to process data of a known route-leak time period. Experiment with different time periods to determine best performance.

Tasks:

- define a link weight that takes into account visibility changes
- run this algorithm on a test case (e.g. Malaysia Telekom leak)

data of a known route-leak time period. Experiment with different time periods to determine best performance.

Tasks:

- define a link weight that takes into account visibility changes
- run this algorithm on a test case (e.g. Malaysia Telekom leak)

[1]

[1] https://github.com/CAIDA/bgp-hackathon/wiki/List-of-Challenges#linkrank-1

Tools

Tools available and missing components

Tools available:

[2] https://bgpstream.caida.org/

[3] https://bgplayjs.com/?section=bgplay

[4] https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

Tools available and missing components

Tools available:

- BGPStream[2] (from CAIDA) framework to easily collect BGP records.

[2] https://bgpstream.caida.org/

[3] https://bgplayjs.com/?section=bgplay

[4] https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

Tools available and missing components

Tools available:

- BGPStream[2] (from CAIDA) framework to easily collect BGP records.
- BGPlayJs[3] (from RIPE NCC) as user-friendly view and event animation.

[2] https://bgpstream.caida.org/
[3] https://bgplayjs.com/?section=bgplay
[4] https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

Tools available and missing components

Tools available:

- BGPStream[2] (from CAIDA) framework to easily collect BGP records.
- BGPlayJs[3] (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available[4] (Team Cymru).

[2] https://bgpstream.caida.org/

[3] https://bgplayjs.com/?section=bgplay

[4] https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

Tools available and missing components

Tools available:

- BGPStream[2] (from CAIDA) framework to easily collect BGP records.
- BGPlayJs[3] (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available[4] (Team Cymru).

Missing components:

[2] https://bgpstream.caida.org/
[3] https://bgplayjs.com/?section=bgplay
[4] https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

Tools available and missing components

Tools available:

- **BGPStream**[2] (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**[3] (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available[4] (Team Cymru).

Missing components:

An *acceptable* algorithm for link *reputation* evaluation.

[2] `https://bgpstream.caida.org/`
[3] `https://bgplayjs.com/?section=bgplay`
[4] `https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt`

Tools available and missing components

Tools available:

- **BGPStream**[2] (from CAIDA) framework to easily collect BGP records.
- **BGPlayJs**[3] (from RIPE NCC) as user-friendly view and event animation.
- Updated list of bogon freely available[4] (Team Cymru).

Missing components:

An *acceptable* **algorithm** for link *reputation* evaluation.

[2] `https://bgpstream.caida.org/`

[3] `https://bgplayjs.com/?section=bgplay`

[4] `https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt`

algorithm

noun

Word used by programmers when they do not want to explain what they did.

algorithm

noun

Word used by programmers when they do not want to explain what they did.

Our proposal

Our proposal

Before going further, what do we have:

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
-

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.
- New Objective:

Our proposal

Before going further, what do we have:

- Test case: Telekom Malaysia leak.
- Metric: link weight.

Will be interesting to have:

- New metrics: link bogon degree and link stability.
- Rename: link weight to link rank.
- New Objective:
    - Algorithm to easily identify link with good/bad reputation.
    - Graphical view with intuitive color code: green to red.

Hypothesis & verification

Our approach (1/2)

Hypothesis

Our approach (1/2)

Hypothesis

Links with *good reputation*:

Our approach (1/2)

Hypothesis

Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Our approach (1/2)

Hypothesis

Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)

Our approach (1/2)

Hypothesis

Links with *good reputation*:

- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)

Developed an algorithm based on the hypothesis metrics:

Our approach (1/2)

Hypothesis

Links with *good reputation*:

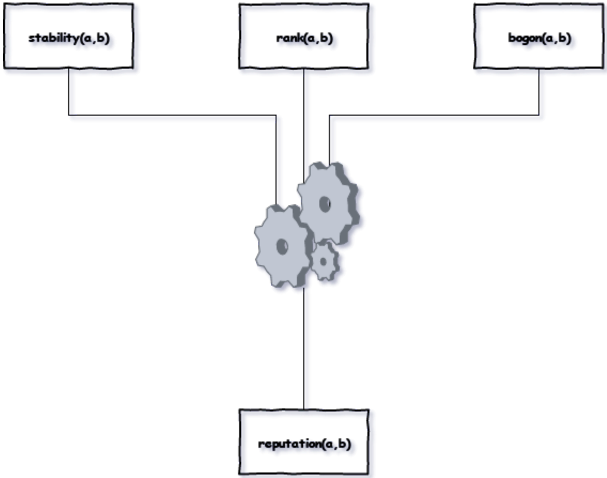
- does not carry bogon,
- have positive stability,
- are used by many AS.

Verification (1/2)

Developed an algorithm based on the hypothesis metrics:

- bogon degree - $bogons_t(\langle A, B \rangle)$,
- link stability - $stability_t(\langle A, B \rangle)$,
- link rank - $rank_t(\langle A, B \rangle)$.

Our algorithm...



Our approach (2/2)

Verification (2/2)

[5] https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

[6] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[7] http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

[5] https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

[6] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[7] http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

- Draw each link instead of AS_PATH.
- Use specific color (from green to red) based on link *reputation* cost.

[5] https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

[6] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[7] http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

- Draw each link instead of AS_PATH.
- Use specific color (from green to red) based on link *reputation* cost.

Tested on three cases:

[5] https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

[6] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[7] http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

Our approach (2/2)

Verification (2/2)

Modified BGPlayJS to:

- Draw each link instead of AS_PATH.
- Use specific color (from green to red) based on link *reputation* cost.

Tested on three cases:

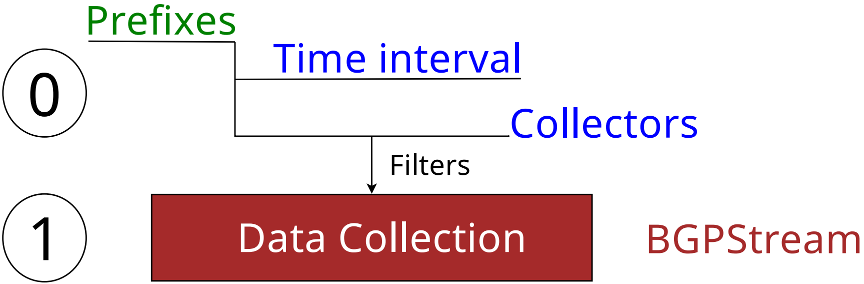
- Routes leak with Telekom Malaysia [5].
- Censorship with Youtube hijack by Pakistan Telecom [6].
- Malicious activities with Link Telecom incident[7].

[5] https://bgpmon.net/massive-route-leak-cause-internet-slowdown/

[6] https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[7] http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

Three phases (1/3)



0

Prefixes

Time interval

Collectors

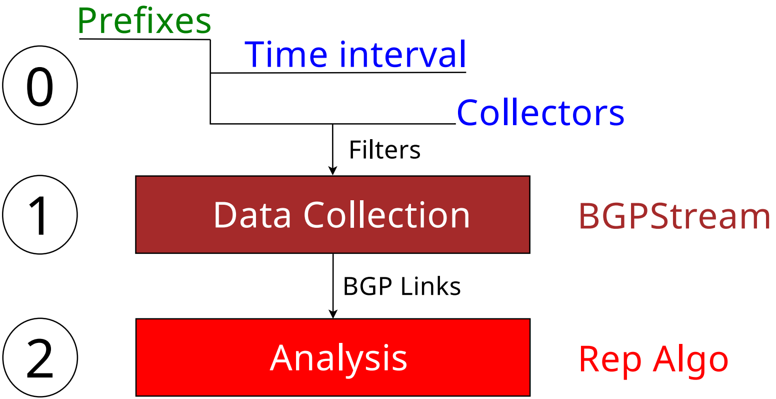
Filters

1

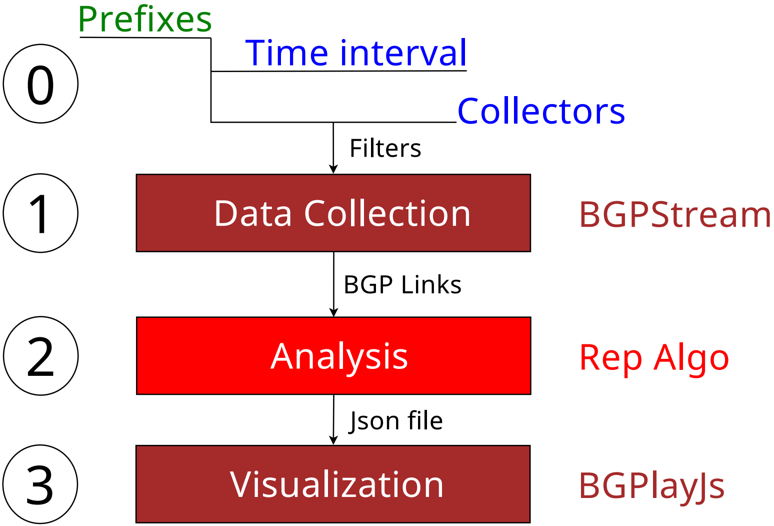
Data Collection

BGPStream

Three phases (2/3)



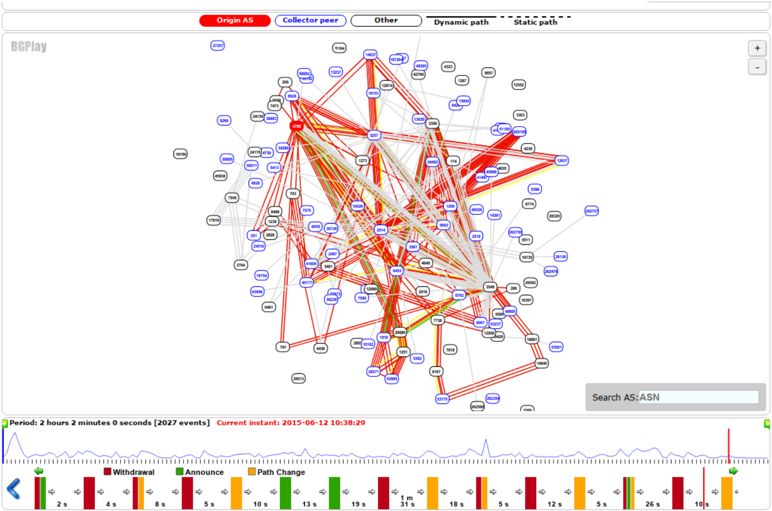
Three phases (3/3)



Malaysia Telecom test cases results

Test: Leak case (Telekom Malaysia)

Test: Leak case (Telekom Malaysia)

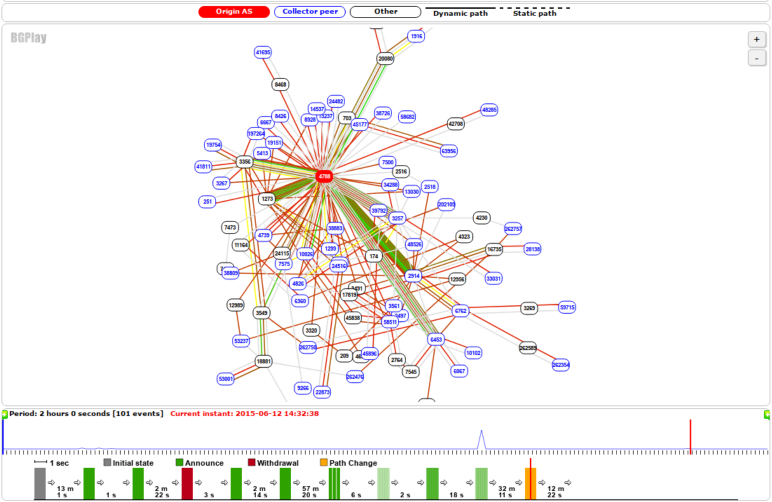


Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Search AS: ASN

Test: Control case (Telekom Malaysia)

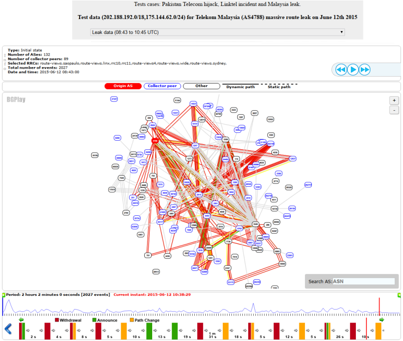
Test: Control case (Telekom Malaysia)



Period: 2 hours 0 seconds [101 events] Current instant: 2015-06-12 14:32:38

Leak and Control cases (Telekom Malaysia)

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Leak data (08:43 to 10:45 UTC) ▾

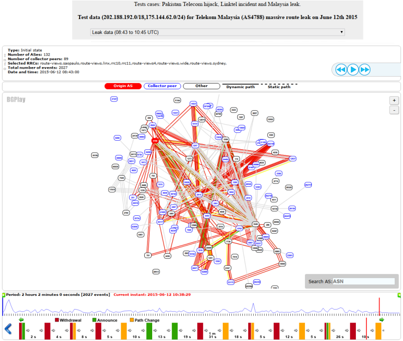
Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Search AS: ASN

Figure 1: Leak case reputation

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Leak data (08:43 to 10:45 UTC) ▾

Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

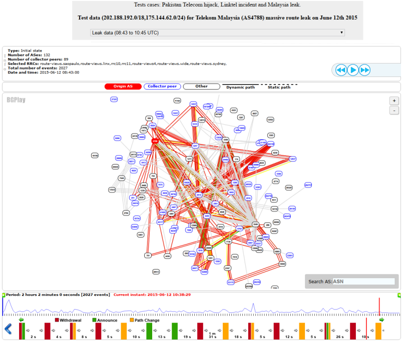
Period: 2 hours 2 minutes 0 seconds [2027 events] **Current instant: 2015-06-12 10:38:29**

Search AS: ASN

Figure 1: Leak case reputation

- 08:43 to 10:45 UTC.
-

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Leak data (08:43 to 10:45 UTC)

Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

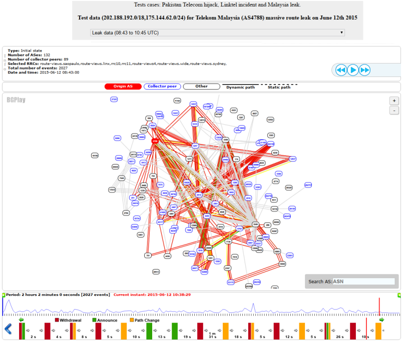
Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Search AS: ASN

Figure 1: Leak case reputation

- 08:43 to 10:45 UTC.
- Most links have *bad reputation*.

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

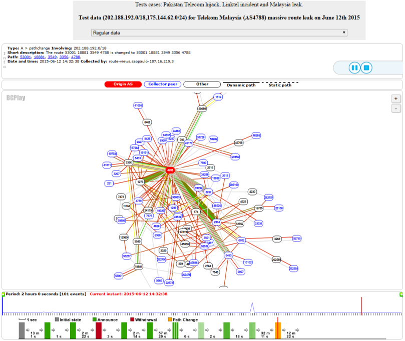
Leak data (08:43 to 10:45 UTC) ▾

Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Search AS: ASN

Figure 1: Leak case reputation



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Regular data ▾

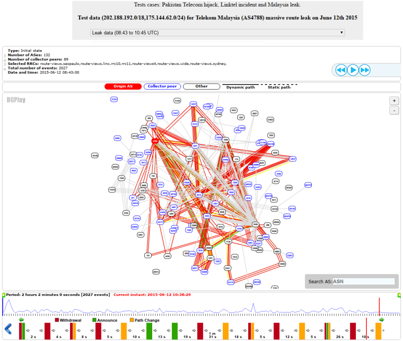
Type: A > pathchange **Involving:** 202.188.192.0/18
Short description: The route 53001 18881 3549 4788 is changed to 53001 18881 3549 3356 4788
Path: 53001, 18881, 3549, 3356, 4788,
Date and time: 2015-06-12 14:32:38 **Collected by:** route-views.saopaulo-187.16.219.3

Period: 2 hours 0 seconds [101 events] Current instant: 2015-06-12 14:32:38

Figure 2: Control case reputation

- 08:43 to 10:45 UTC.
- Most links have *bad reputation*.

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

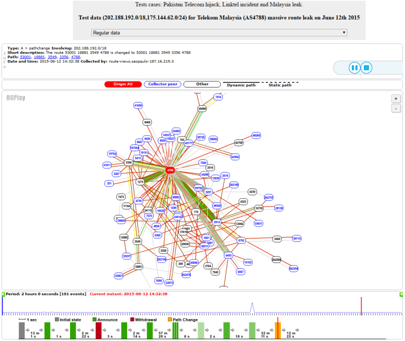
Leak data (08:43 to 10:45 UTC)

Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Search AS: ASN

Figure 1: Leak case reputation



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Regular data

Type: A > pathchange **Involving:** 202.188.192.0/18
Short description: The route 53001 18881 3549 4788 is changed to 53001 18881 3549 3356 4788
Path: 53001, 18881, 3549, 3356, 4788,
Date and time: 2015-06-12 14:32:38 **Collected by:** route-views.saopaulo-187.16.219.3

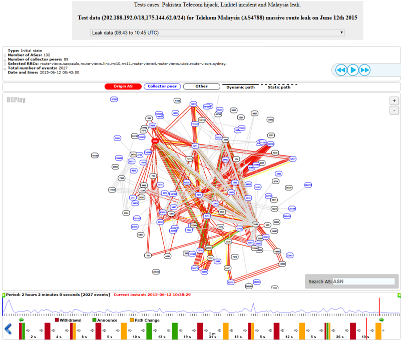
Period: 2 hours 0 seconds [101 events] Current instant: 2015-06-12 14:32:38

Figure 2: Control case reputation

- 08:43 to 10:45 UTC.
- Most links have *bad reputation*.

- 12:45 to 14:45 UTC.
-

Leak and Control cases (Telekom Malaysia)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

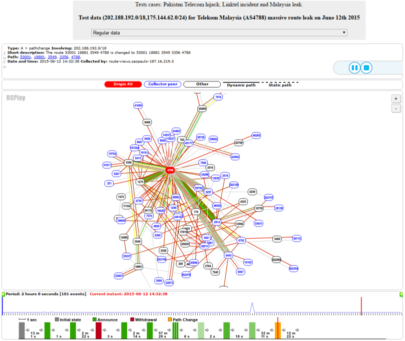
Leak data (08:43 to 10:45 UTC)

Type: Initial state
Number of ASes: 132
Number of collector peers: 89
Selected RRCs: route-views.saopaulo,route-views.linx,rrc10,rrc11,route-views4,route-views.wide,route-views.sydney,
Total number of events: 2027
Date and time: 2015-06-12 08:43:00

Search AS: ASN

Period: 2 hours 2 minutes 0 seconds [2027 events] Current instant: 2015-06-12 10:38:29

Figure 1: Leak case reputation



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (202.188.192.0/18,175.144.62.0/24) for Telekom Malaysia (AS4788) massive route leak on June 12th 2015

Regular data

Type: A > pathchange **Involving:** 202.188.192.0/18
Short description: The route 53001 18881 3549 4788 is changed to 53001 18881 3549 3356 4788
Path: 53001, 18881, 3549, 3356, 4788,
Date and time: 2015-06-12 14:32:38 **Collected by:** route-views.saopaulo-187.16.219.3

Period: 2 hours 0 seconds [101 events] Current instant: 2015-06-12 14:32:38

Figure 2: Control case reputation

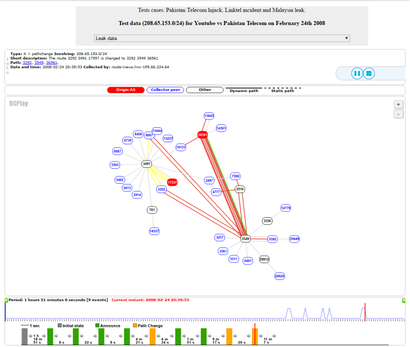
- 08:43 to 10:45 UTC.
- Most links have *bad reputation*.

- 12:45 to 14:45 UTC.
- Mix of *good* and *bad reputation*.

Other tests cases results

Censorship test case (YouTube Hijack)

Censorship test case (YouTube Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

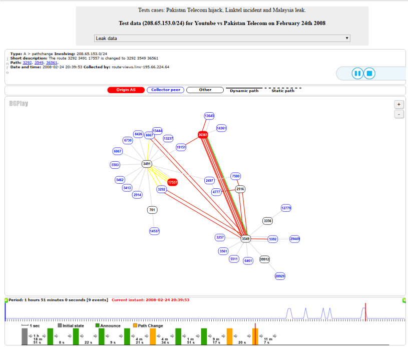
Leak data ▾

Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] **Current instant: 2008-02-24 20:39:53**

Figure 3: Hijack case reputation

Censorship test case (YouTube Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Leak data ▾

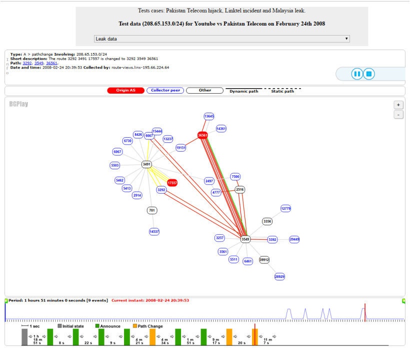
Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] **Current instant: 2008-02-24 20:39:53**

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
-

Censorship test case (YouTube Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Leak data ▾

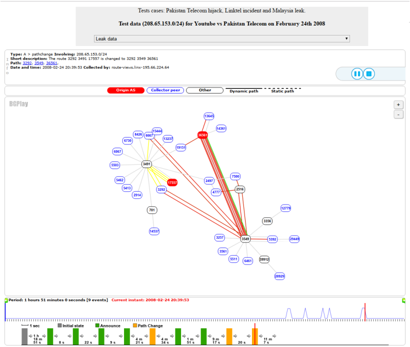
Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] Current instant: 2008-02-24 20:39:53

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have *bad reputation*.

Censorship test case (YouTube Hijack)


Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

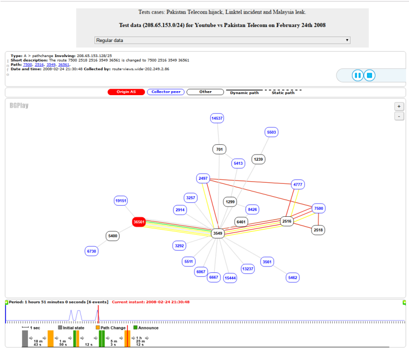
Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Leak data

Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] Current instant: 2008-02-24 20:39:53

Figure 3: Hijack case reputation


Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Regular data

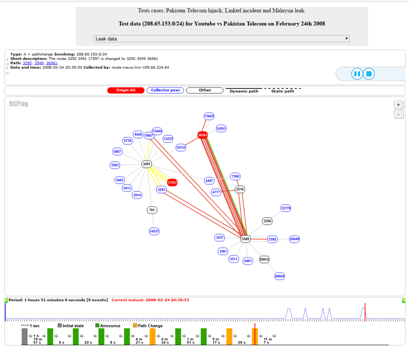
Type: A > pathchange **Involving:** 208.65.153.128/25
Short description: The route 7500 2518 2516 3549 36561 is changed to 7500 2516 3549 36561
Path: 7500, 2516, 3549, 36561,
Date and time: 2008-02-24 21:30:48 **Collected by:** route-views.wide-202.249.2.86

Period: 1 hours 51 minutes 0 seconds [6 events] Current instant: 2008-02-24 21:30:48

Figure 4: Control case reputation

- 19:00 to 20:51 UTC.
- Youtube links have *bad reputation*.

Censorship test case (YouTube Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

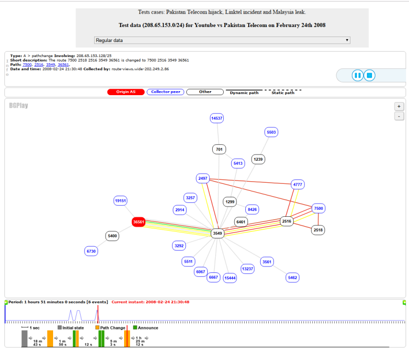
Leak data ▾

Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] Current instant: 2008-02-24 20:39:53

Figure 3: Hijack case reputation

- 19:00 to 20:51 UTC.
- Youtube links have *bad reputation*.



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Regular data ▾

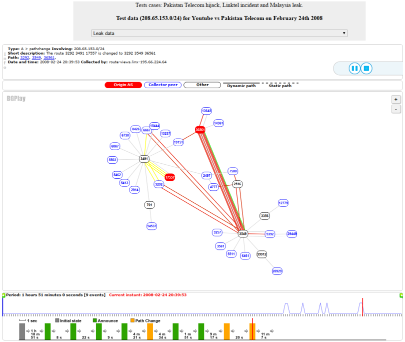
Type: A > pathchange **Involving:** 208.65.153.128/25
Short description: The route 7500 2518 2516 3549 36561 is changed to 7500 2516 3549 36561
Path: 7500, 2516, 3549, 36561,
Date and time: 2008-02-24 21:30:48 **Collected by:** route-views.wide-202.249.2.86

Period: 1 hours 51 minutes 0 seconds [6 events] Current instant: 2008-02-24 21:30:48

Figure 4: Control case reputation

- 21:05 to 22:56 UTC.
-

Censorship test case (YouTube Hijack)



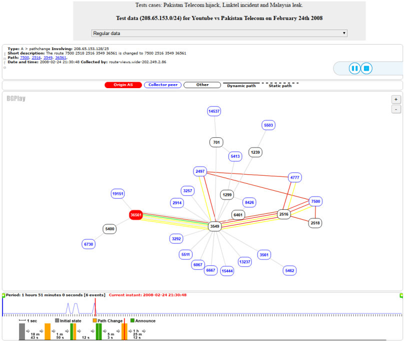
Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Leak data

Type: A > pathchange **Involving:** 208.65.153.0/24
Short description: The route 3292 3491 17557 is changed to 3292 3549 36561
Path: 3292, 3549, 36561,
Date and time: 2008-02-24 20:39:53 **Collected by:** route-views.linx-195.66.224.64

Period: 1 hours 51 minutes 0 seconds [9 events] Current instant: 2008-02-24 20:39:53



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (208.65.153.0/24) for Youtube vs Pakistan Telecom on February 24th 2008

Regular data

Type: A > pathchange **Involving:** 208.65.153.128/25
Short description: The route 7500 2518 2516 3549 36561 is changed to 7500 2516 3549 36561
Path: 7500, 2516, 3549, 36561,
Date and time: 2008-02-24 21:30:48 **Collected by:** route-views.wide-202.249.2.86

Period: 1 hours 51 minutes 0 seconds [6 events] Current instant: 2008-02-24 21:30:48

Figure 3: Hijack case reputation

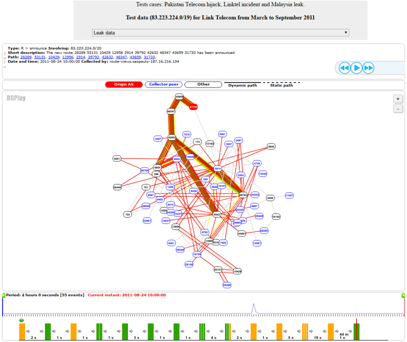
Figure 4: Control case reputation

- 19:00 to 20:51 UTC.
- Youtube links have *bad reputation*.

- 21:05 to 22:56 UTC.
- Mix of *good reputation* and *bad reputation*.

Malicious activities test case (Link Telecom Hijack)

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

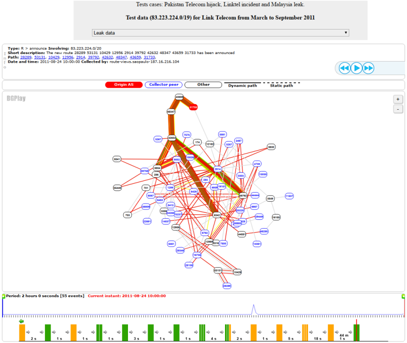
Leak data ▾

Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] Current instant: 2011-08-24 10:00:00

Figure 5: Leak case reputation

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Leak data ▾

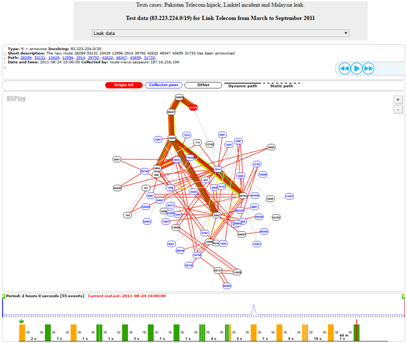
Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] Current instant: 2011-08-24 10:00:00

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
-

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Leak data ▾

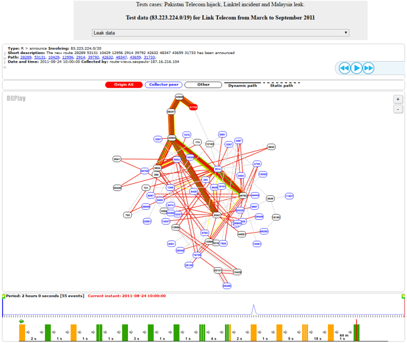
Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] Current instant: 2011-08-24 10:00:00

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad reputation*.

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

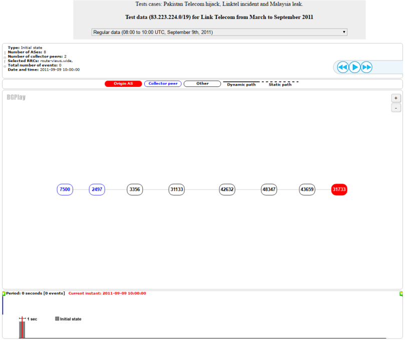
Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Leak data ▾

Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] Current instant: 2011-08-24 10:00:00

Figure 5: Leak case reputation



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Regular data (08:00 to 10:00 UTC, September 9th, 2011) ▾

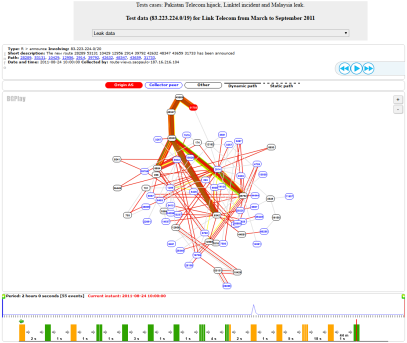
Type: Initial state
Number of ASes: 8
Number of collector peers: 2
Selected RRCs: route-views.wide,
Total number of events: 0
Date and time: 2011-09-09 10:00:00

Period: 0 seconds [0 events] Current instant: 2011-09-09 10:00:00

Figure 6: Control case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad reputation*.

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

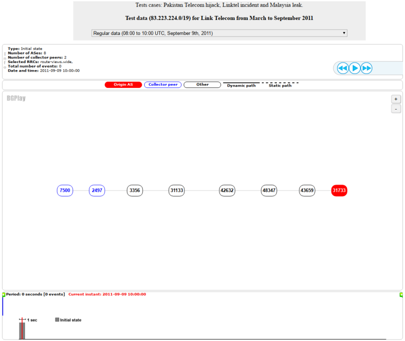
Leak data

Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] Current instant: 2011-08-24 10:00:00

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad reputation*.



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Regular data (08:00 to 10:00 UTC, September 9th, 2011)

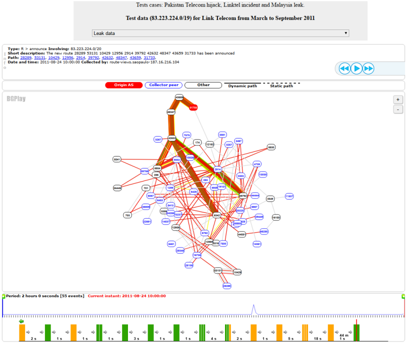
Type: Initial state
Number of ASes: 8
Number of collector peers: 2
Selected RRCs: route-views.wide,
Total number of events: 0
Date and time: 2011-09-09 10:00:00

Period: 0 seconds [0 events] Current instant: 2011-09-09 10:00:00

Figure 6: Control case reputation

- 08:00 to 10:00 UTC (September 9, 2011).
-

Malicious activities test case (Link Telecom Hijack)



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

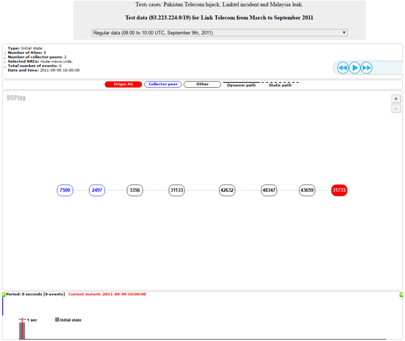
Leak data

Type: R > announce **Involving:** 83.223.224.0/20
Short description: The new route 28289 53131 10429 12956 2914 39792 42632 48347 43659 31733 has been announced
Path: 28289, 53131, 10429, 12956, 2914, 39792, 42632, 48347, 43659, 31733,
Date and time: 2011-08-24 10:00:00 **Collected by:** route-views.saopaulo-187.16.216.104

Period: 2 hours 0 seconds [55 events] **Current instant: 2011-08-24 10:00:00**

Figure 5: Leak case reputation

- 08:00 to 10:00 UTC (August 24, 2011).
- Most links have *bad reputation*.



Tests cases: Pakistan Telecom hijack, Linktel incident and Malaysia leak.

Test data (83.223.224.0/19) for Link Telecom from March to September 2011

Regular data (08:00 to 10:00 UTC, September 9th, 2011)

Type: Initial state
Number of ASes: 8
Number of collector peers: 2
Selected RRCs: route-views.wide,
Total number of events: 0
Date and time: 2011-09-09 10:00:00

Period: 0 seconds [0 events] **Current instant: 2011-09-09 10:00:00**

Figure 6: Control case reputation

- 08:00 to 10:00 UTC (September 9, 2011).
- No event.

Improvement (proposals)

Improvement (proposals)

Improvement (proposals)

- Better view

Improvement (proposals)

- Better view
    - [Problem] Unclear view with BGPlayJS.
    -

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).

Improvement (proposals)

- Better view
    - [Problem] Unclear view with BGPlayJS.
    - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  -

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
  -
  -

Improvement (proposals)

- Better view
    - [Problem] Unclear view with BGPlayJS.
    - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
    - [Problem] Collectors and time interval are hard coded.
    - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
    - [Problem] Only three test cases.
    -

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.
- Large scale algorithm

Improvement (proposals)

- Better view
    - [Problem] Unclear view with BGPlayJS.
    - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
    - [Problem] Collectors and time interval are hard coded.
    - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
    - [Problem] Only three test cases.
    - [Proposal] Add more (well-known) BGP incidents.
- Large scale algorithm
    -
    -

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.
- Large scale algorithm
  - [Problem] BGP is large scale protocol vs limited resources.
  -

Improvement (proposals)

- Better view
  - [Problem] Unclear view with BGPlayJS.
  - [Proposal] Draw **One** line between links (using netJSON ?).
- Inputs flexibility
  - [Problem] Collectors and time interval are hard coded.
  - [Proposal] Allow user to select collectors and time interval for analysis.
- More testing
  - [Problem] Only three test cases.
  - [Proposal] Add more (well-known) BGP incidents.
- Large scale algorithm
  - [Problem] BGP is large scale protocol vs limited resources.
  - [Proposal] Use Massive Data/AI tools for link classification.

Thanks

Thanks

Corrections / updates / comments

would be appreciated