

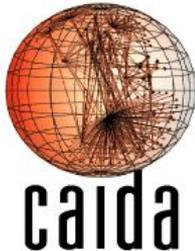
ARTEMIS: an Open-source Tool for Detecting BGP Prefix Hijacking in Real Time

(funded by  **RIPE NCC** Community Projects 2017)
RIPE NETWORK COORDINATION CENTRE

Vasileios Kotronis

Foundation for Research and Technology - Hellas (FORTH), Institute of Computer Science
(& grateful RIPE fellow!)

RIPE79 Plenary, Lightning Talk, Rotterdam, NL, 14 October 2019





BGP Monitors:

- RIPE RIS
- BGPStream
- Live
- Historical
- Beta BMP
- Local (exaBGP)

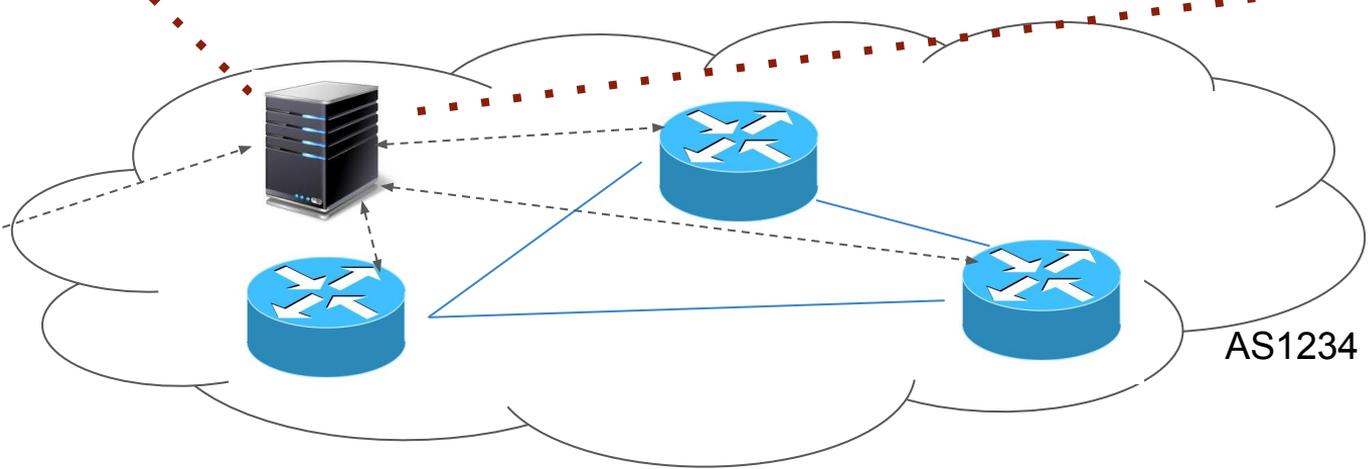
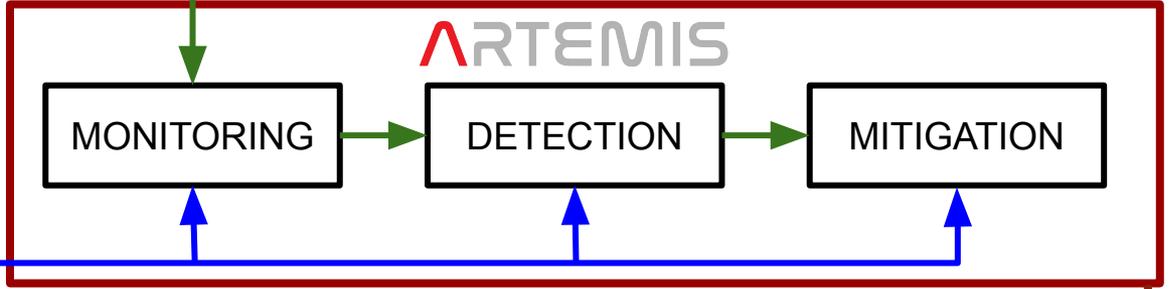


Operator Configuration File



ARTEMIS overview

Runs as a multi-container app in the NOC





BGP Monitors:

- RIPE RIS
- BGPStream
- Live
- Historical
- Beta BMP
- Local (exaBGP)



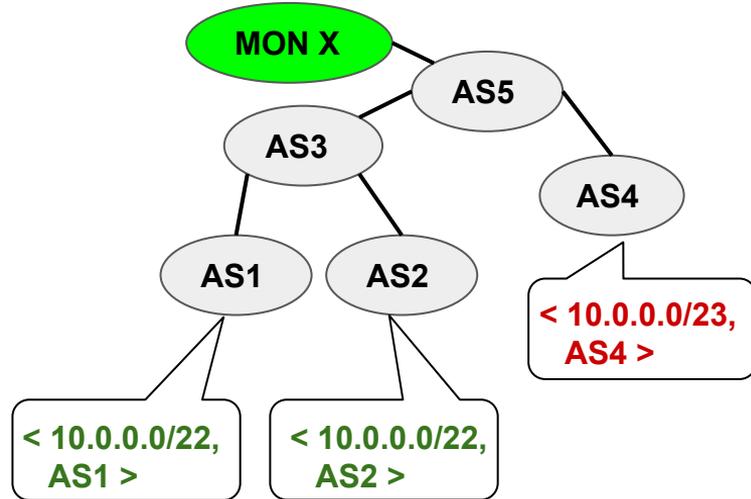
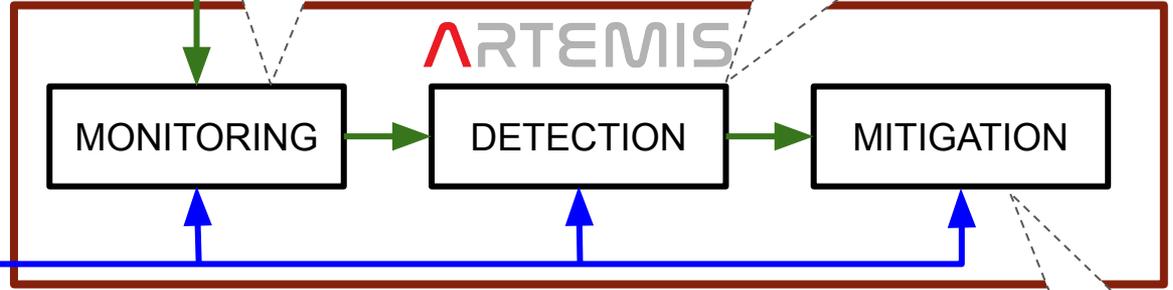
“Monitor X saw a BGP update for 10.0.0.0/23 originated by AS4.”

“Origin sub-prefix HIJACK by AS4 vs. 10.0.0.0/23.”

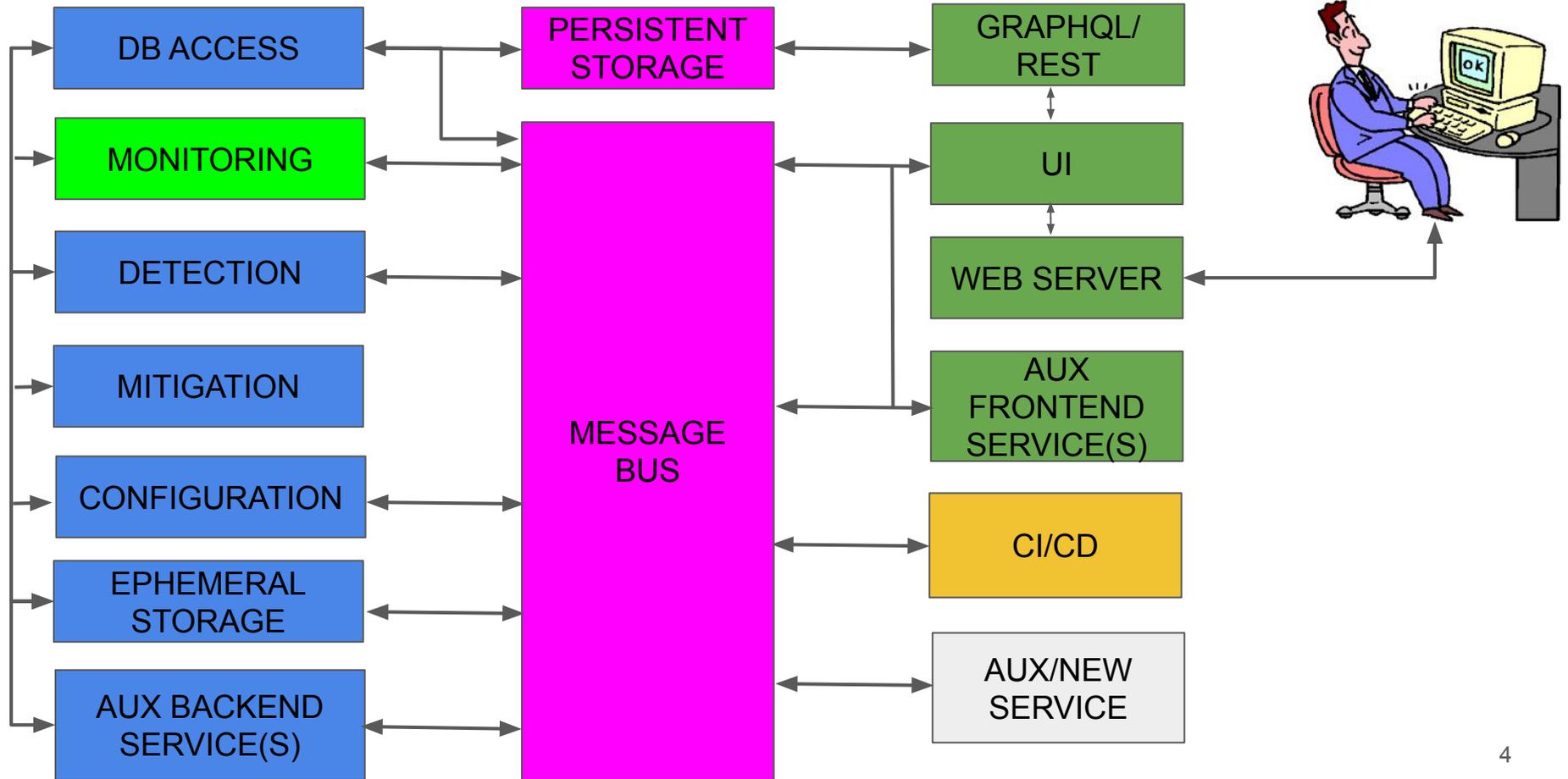
Operator Configuration File



“I own 10.0.0.0/22 and announce it from AS1 and AS2; both have AS3 as upstream.”



ARTEMIS architecture



Features of open-source tool @

<https://github.com/FORTH-ICS-INSPIRE/artemis>

- Real-time BGP monitoring
- Real-time BGP detection + notifications
- Support for multiple modes of operation
 - Passive monitor
 - Passive detector
 - Active joint detector and user-triggered mitigator
- Support for Kubernetes deployment
- Automatic tagging of hijack incidents
- Comprehensive web-based GUI
- Support for both IPv4/IPv6 prefixes

Hijacks: dimensions

Type	Examples	ARTEMIS-Supported
Prefix	Sub(S)-/Exact(E)-prefix, squatting (Q)	S, E, Q
AS-Path	Type-0/1/... (depending on hijacker AS-hop)	0, 1
Data plane	Blackholing, Imposture, MitM	- (control-plane tool)
Policy	No-export route leak (L), ...	L (based on AS-path length)

Example 1: Invalid origin, advertising a configured prefix:

E|0|-|-

Example 2: Valid origin, fake neighbor, leaking a sub-prefix of a configured prefix: **S|1|-|L**

Hijacks: states

Type	Description	Auto/user
Ongoing	Hijack is currently active.	Auto
Dormant	Ongoing hijack, no updates in X hours.	Auto
Under mitigation	User has initiated mitigation.	User
Ignored	Implicit false positive, needs conf update.	User
Resolved	Incident resolved by user (implicit true positive).	User
Withdrawn	Hijacked route withdrawn from monitors.	Auto
Outdated	Hijack deprecated according to new configuration.	Auto

ARTEMIS configuration file

- Define prefix, ASN, monitor groups
- Declare ARTEMIS rules:
 - “My ASes ASX and ASY originate prefix P”
 - “And they advertise it to ASZ”
 - “When a hijack occurs → mitigate manually”

Sample Rule	Sample Incoming BGP update	Hijack
prefixes: - *my_prefix origin_asns: - *my_origin neighbors: - *my_neighbor mitigation: manual	[..., <subprefix_of_my_prefix>]	S - -
	[..., <not_my_origin>, <my_prefix>]	E 0 -
	[..., <not_my_neighbor>, <my_origin>, <my_prefix>]	E 1 -
prefixes: - *my_prefix mitigation: manual	[..., <my_prefix>]	Q 0 -

```
#
# ARTEMIS Configuration File
#
# Start of Prefix Definitions
prefixes:
    forth_prefix_main: &forth_prefix_main
        - 139.91.0.0/16
    forth_prefix_lamda: &forth_prefix_lamda
        - 139.91.250.0/24
    forth_prefix_vod: &forth_prefix_vod
        - 139.91.2.0/24
# End of Prefix Definitions
# Start of Monitor Definitions
monitors:
    ripervis: ['']
    bgpstreamlive:
        - routeviews
        - ris
    betabmp:
        - betabmp
    # exabgp:
    # - ip: 192.168.1.1
    #   port: 5000
# End of Monitor Definitions
# Start of ASN Definitions
asns:
    forth_asn: &forth_asn
        8522
    grnet_forth_upstream: &grnet_forth_upstream
        5408
    lamda_forth_upstream_back: &lamda_forth_upstream_back
        56910
    vodafone_forth_upstream_back:
&vodafone_forth_upstream_back
        12361
# End of ASN Definitions
# Start of Rule Definitions
rules:
```

PEERING DEMO: Disclaimer

- In the following, I am using the PEERING BGP testbest to demonstrate an emulated “hijack”.
- Only the resource 184.164.243.0/24 which is allocated in the context of the experiment is “affected”.
- The two PEERING sites I am using (isi01 and grnet01) are used for demonstration purposes (one site in the US, one in Europe), to show how an emulated hijack attempt from a well-connected location can affect a remote network.
- The experiment complies with the PEERING terms of use.

Demo: Start and configure ARTEMIS

Dashboard

Activity

Welcome back **admin@admin**, your last login was at (03-09-2019 13:23:57) from 172.18.0.10.

Ongoing, Non-Dormant Hijacks

Show entries

Last Update	Time Detected	Hijacked Prefix	Matched Prefix	Type	Hijacker AS	# Peers Seen	# ASes Infected	Ack	More
 No hijack alerts.									

Showing 0 to 0 of 0 entries

Times are shown in your local time zone **GMT+3 (Europe/Athens)**.

System Status

Module	Status	Uptime
Clock	On 1/1	0D 0H 4M 0S
Configuration	On 1/1	0D 0H 4M 0S
Database v.17	On 1/1	0D 0H 4M 0S
Detection	On 10/10	View instances
Mitigation	On 0/1	
Monitor	On 1/1	0D 0H 0M 48S
Observer	On 1/1	0D 0H 4M 0S

Statistics

Monitored Prefixes	1
Configured Prefixes	1
Monitor Peers	0
Total BGP Updates	0
Total Unhandled Updates	0
Total Hijacks	0

Demo: Start and configure ARTEMIS

System

Monitor Module

Active 1/1

Detection Module

Active 10/10

Mitigation Module

Active 0/1

Current Configuration

Load AS-SETS Edit

Configuration file updated.

```
12 riperis: []
13 bgpstreamlive:
14   - routeviews
15   - ris
16 betabmp: betabmp
17 # End of Monitor Definitions
18
19 # Start of ASN Definitions
20 asns:
21   peering_asn: &peering_asn
22   - 47065
23   los_nettos_upstream: &los_nettos_upstream
24   - 226
25 # End of ASN Definitions
26
27 # Start of Rule Definitions
28 rules:
29 - prefixes:
30   - *peering_prefix_main
31 origin_asns:
32   - *peering_asn
33 neighbors:
34   - *los_nettos_upstream
35 mitigation:
36   manual
37 # End of Rule Definitions
```

Demo: Make “legitimate” announcement from isi01 site (origin: AS47065, upstream: AS226)

BGP Updates

Live Update:

All Past 1h Past 24h Past 48h Custom

Show 10 entries

Download Table

Timestamp	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	Type	Hijack	Status	More
2019-09-04 11:13:37	184.164.243.0/24	184.164.243.0/24	47065	262757 4230 6453 2914 226 47065	262757	ripe-ris -> rrc15	A			
2019-09-04 11:13:31	184.164.243.0/24	184.164.243.0/24	47065	50300 2914 226 47065	50300	ripe-ris -> rrc00	A			
2019-09-04 11:13:22	184.164.243.0/24	184.164.243.0/24	47065	12307 39540 57118 29691 13030 226 47065	12307	ripe-ris -> rrc20	A			
2019-09-04 11:13:07	184.164.243.0/24	184.164.243.0/24	47065	395152 14007 6939 226 47065	395152	ripe-ris -> rrc00	A			
2019-09-04 11:12:47	184.164.243.0/24	184.164.243.0/24	47065	12307 57118 29691 13030 226 47065	12307	ripe-ris -> rrc20	A			
2019-09-04 11:12:40	184.164.243.0/24	184.164.243.0/24	47065	37239 37468 1299 2914 226 47065	37239	ripe-ris -> rrc19	A			
2019-09-04 11:12:34	184.164.243.0/24	184.164.243.0/24	47065	328145 1299 2914 226 47065	328145	ripe-ris -> rrc01	A			
2019-09-04 11:12:19	184.164.243.0/24	184.164.243.0/24	47065	58299 13030 226 47065	58299	ripe-ris -> rrc20	A			
2019-09-04 11:12:17	184.164.243.0/24	184.164.243.0/24	47065	132825 3491 2914 226 47065	132825	ripe-ris -> rrc00	A			
2019-09-04 11:12:15	184.164.243.0/24	184.164.243.0/24	47065	204092 57199 200780 3257 2914 226 47065	204092	ripe-ris -> rrc00	A			
	<input type="text" value="Prefix"/>	<input type="text" value="Matched Prefix"/>	<input type="text" value="Origin AS"/>	<input type="text" value="AS Path"/>	<input type="text" value="Peer AS"/>	<input type="text" value="Service"/>	<input type="text" value="A W"/>			

Showing 1 to 10 of 409 entries

Demo: Make “illegitimate” announcement from grnet01 site (origin: AS47065, upstream: AS5408)

BGP Updates

Live Update:

All Past 1h Past 24h Past 48h Custom

Show 10 entries

[Download Table](#)

Timestamp	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	Type	Hijack	Status	More
2019-09-04 11:31:09	184.164.243.0/24	184.164.243.0/24	47065	328145 1299 21320 21320 21320 21320 5408 47065	328145	ripe-ris -> rrc01	A	View		
2019-09-04 11:30:56	184.164.243.0/24	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	ripe-ris -> rrc03	A	View		
2019-09-04 11:30:55	184.164.243.0/24	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	ripe-ris -> rrc13	A	View		
2019-09-04 11:30:55	184.164.243.0/24	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	ripe-ris -> rrc12	A	View		
2019-09-04 11:30:42	184.164.243.0/24	184.164.243.0/24	47065	206499 34549 13101 2603 21320 5408 47065	206499	ripe-ris -> rrc00	A	View		
2019-09-04 11:30:41	184.164.243.0/24	184.164.243.0/24	47065	58057 34549 13101 2603 21320 5408 47065	58057	ripe-ris -> rrc00	A	View		
2019-09-04 11:30:41	184.164.243.0/24	184.164.243.0/24	47065	58057 34549 33891 21320 5408 47065	58057	ripe-ris -> rrc00	A	View		
2019-09-04 11:30:41	184.164.243.0/24	184.164.243.0/24	47065	34549 13101 2603 21320 5408 47065	34549	ripe-ris -> rrc00	A	View		
2019-09-04 11:30:38	184.164.243.0/24	184.164.243.0/24	47065	57264 174 21320 21320 21320 21320 5408 47065	57264	ripe-ris -> rrc00	A	View		
2019-09-04 11:30:31	184.164.243.0/24	184.164.243.0/24	47065	174 21320 21320 21320 21320 5408 47065	174	ripe-ris -> rrc00	A	View		
	<input type="text" value="Prefix"/>	<input type="text" value="Matched Prefix"/>	<input type="text" value="Origin AS"/>	<input type="text" value="AS Path"/>	<input type="text" value="Peer AS"/>	<input type="text" value="Service"/>	<input type="text" value="AIW"/>			

Demo: Check that ARTEMIS detects the illegitimate announcement in real time

Viewing Hijack Ongoing

Hijack Information Not Acknowledged

Hijacker AS:	5408	Time Started:	2019-09-04 11:29:34
Type:	E 1 +	Time Detected:	2019-09-04 11:29:40
# Peers Seen:	109	Last Update:	2019-09-04 11:31:09
# ASes Infected:	133	Time Ended:	Never
Prefix:	184.164.243.0/24	Mitigation Started:	Never
Matched:	184.164.243.0/24	Community Annotation:	NA
Config:	2019-09-04 11:05:17		
Key:	426c0897c7cb3455e077fb3696cb6d9d	Display Peers Seen Hijack:	

BGP Announcement BGP Withdrawal

Hijack Actions

Mark as Resolved Apply

Comments Edit

1

Related BGP Updates

Show 10 entries Download Table

Timestamp	Prefix	Origin AS	AS Path	Peer AS	Service	Type	Status	More
2019-09-04 11:31:09	184.164.243.0/24	47065	328145 1299 21320 21320 21320 5408 47065	328145	riperis -> rrc01	A		
2019-09-04 11:30:56	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	riperis -> rrc03	A		
2019-09-04 11:30:55	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	riperis -> rrc13	A		
2019-09-04 11:30:55	184.164.243.0/24	47065	47441 31133 174 21320 21320 21320 21320 5408 47065	47441	riperis -> rrc12	A		

Demo: Withdraw “illegitimate” announcement

ARTEMIS
Overview
BGP Updates
Hijacks
Admin ▾ Actions ▾ About Sign out

Hijacker AS:	5408
Type:	E I H-
# Peers Seen:	118
# ASes Infected:	148
Prefix:	184.164.243.0/24
Matched:	184.164.243.0/24
Config:	2019-09-04 11:05:17
Key:	426c0897c7cb3455e077fb3696cb6d9d

Time Started:	2019-09-04 11:29:34
Time Detected:	2019-09-04 11:29:40
Last Update:	2019-09-04 11:58:23
Time Ended:	Never
Mitigation Started:	Never
Community Annotation:	NA

Display Peers Seen Hijack:

BGP Announcement
BGP Withdrawal

Mark as Resolved ▾
Apply

Comments Edit

1

(118) Peers Seen Hijack BGP Announcement:

174	553	680	1103
1140	1299	1916	2603
2613	2895	3267	3277
3333	3741	5413	6423
6667	6720	6881	6894
8218	8220	8426	8455
8492	8607	8758	8896
9002	9304	12350	12779
12859	13237	14537	14907
15435	15547	20514	20562
20764	20811	20932	20953
21320	24482	24875	25091
25160	25220	25227	28917
29140	29479	29504	29680
30132	31019	34177	34224
34224	34224	34224	34224

(117) Peers Seen Hijack BGP Withdrawal:

174	553	680	1103
1140	1299	1916	2603
2613	2895	3267	3277
3333	3741	5413	6423
6667	6720	6881	6894
8218	8220	8426	8455
8492	8607	8758	8896
9002	9304	12350	12779
12859	13237	14537	14907
15435	15547	20514	20764
20811	20932	20953	21320
24482	24875	25091	25160
25220	25227	28917	29140
29479	29504	29680	30132
31019	34177	34224	34288
34224	34224	34224	34288

Next steps for the open-source tool

- Auto-configuration (generation of ARTEMIS conf file)
 - Ansible + Python
 - RPKI ROAs → (allowed) prefixes, origin ASNs, rules
- Auto-mitigation
 - Ansible + Python
 - Prefix deaggregation
 - GRE tunneling using helper AS
- Data-plane extensions
 - RIPE Atlas traceroutes
 - Evaluation and monitoring of data-plane impact
- Further maintenance and testing
 - Already tested ARTEMIS in a major Greek ISP, AMS-IX, Internet2 and FORTH.
 - Join discord (<https://discordapp.com/invite/8UerJvh>) and let's deploy!

Do not miss our live demo on Wed/Thu!

- **Side-room, during 10.30 - 11.00 coffee break**
- Show more about the configuration file
- Trigger different hijack types
- Show “ignore” (learn), “resolve”, “mitigate”, “ack”, “delete” actions
- Show auto-withdrawn, auto-outdated characterization
- Answer questions regarding the open-source tool

Thank you very much for your attention!

Online Resources

1. GitHub repository: <https://github.com/FORTH-ICS-INSPIRE/artemis>
2. Discord channel: <https://discordapp.com/invite/8UerJvh>
3. Mailing list: <http://lists.ics.forth.gr/mailman/listinfo/artemis>
4. Wiki: <https://github.com/FORTH-ICS-INSPIRE/artemis/wiki>
5. Webpage: <https://www.inspire.edu.gr/artemis/>
6. Publications:
 - a. Pavlos Sermpezis, et al. **"ARTEMIS: Neutralizing BGP Hijacking within a Minute."** *In ACM/IEEE Transactions on Networking (ToN)*, vol. 26, iss. 6, 2018.
 - b. Pavlos Sermpezis, et al. **"A survey among Network Operators on BGP Prefix Hijacking."** *In ACM SIGCOMM Computer Communications Review (CCR)*, vol. 48, no. 1, January 2018.
 - c. Gavriil Chaviaras, et al. **"ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking (demo)."** *Proc. of the ACM SIGCOMM 2016*, 625-626. (demo/poster) Florianopolis, Brazil, 2016.
7. Blogs/articles:
 - a. https://labs.ripe.net/Members/vasileios_kotronis/artemis-an-open-source-tool-for-detecting-bgp-hijacking-in-real-time
 - b. https://labs.ripe.net/Members/vasileios_kotronis/artemis-neutralising-bgp-hijacking-within-a-minute
 - c. <https://blog.apnic.net/2018/07/19/artemis-neutralizing-bgp-hijacking-within-a-minute/>

BACKUP

What is this presentation about?

1. Quick recap of ARTEMIS anti-hijacking solution
2. Updates on ARTEMIS open-source tool
3. Short demo using PEERING BGP testbed (slides)
4. Next steps

BACKUP

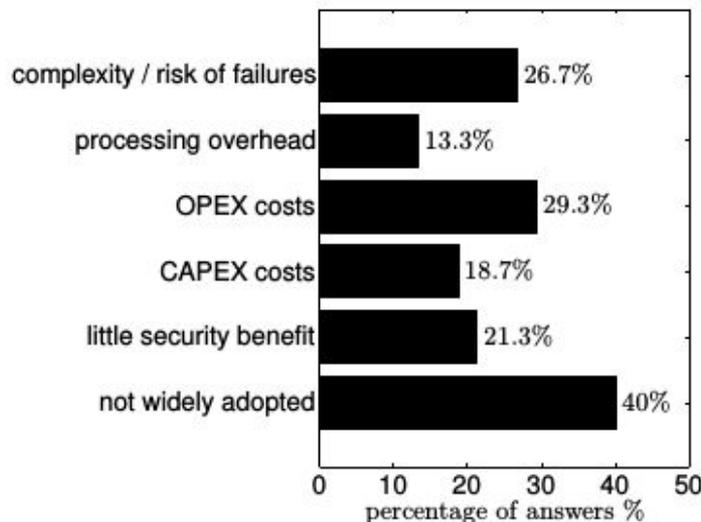
DEMO with crafted BGP updates

1. Show configuration file
 - a. 2-homed network (1 origin, 2 upstreams)
 - b. 1 main prefix
 - c. 1 prefix with no-export tag
 - d. 1 prefix that should not be announced
2. Send crafted BGP updates (benign/hijack)
3. Trigger the following hijack types:
 - a. Exact-prefix: E|0|-|-, E|1|-|-, E|-|L
 - b. Sub-prefix: S|0|-|-, S|1|-|-, S|-|-
 - c. Squatting: Q|0|-|-
4. Show “ignore” (learn), “resolve”, “mitigate”, “ack”, “delete” actions
5. Show auto-withdrawn, auto-outdated characterization
6. Withdraw everything (optional)

BACKUP

How do people deal with hijacks today? → RPKI

- ✗ ~16% of prefixes covered by ROAs [1]
- ✗ Why? → limited adoption & costs/complexity [2]
- ✗ Does not protect the network against all attack types



Reasons for not using RPKI [2]

BACKUP

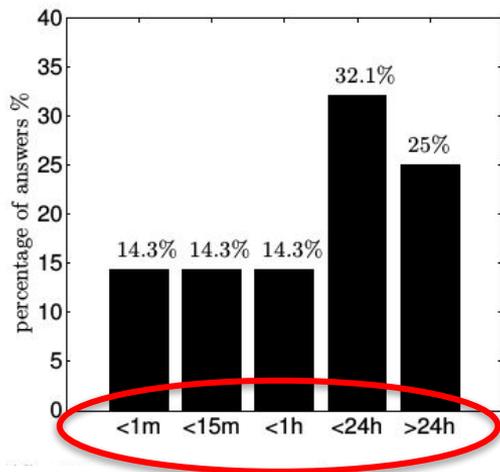
[1] NIST. RPKI Monitor <https://rpki-monitor.antd.nist.gov/>, Sep. 2019.

[2] P. Sempetzis, et. al., "[A survey among Network Operators on BGP Prefix Hijacking](#)", in ACM SIGCOMM CCR, Jan. 2018.

How do people deal with hijacks today? → 3rd parties

- ✗ **Comprehensiveness:** detect only simple attacks
- ✗ **Accuracy:** lots of false positives (FP) & false negatives (FN)
- ✗ **Speed:** manual verification & then manual mitigation
- ✗ **Privacy:** need to share private info, routing policies, etc.

BACKUP



How much time an operational network was affected by a hijack [1]

Our solution: ARTEMIS

- Operated in-house: no third parties
- Real-time detection
- Flexible automated mitigation

✓ **Comprehensive:** covers *all* hijack types

✓ **Accurate:** *0% FP, 0% FN* for basic types;
low tunable FP-FN trade-off for remaining types

Fast: neutralizes (detect & mitigate) attacks in *< 1 minute*

Privacy preserving: no sensitive info shared

Flexible: configurable mitigation per-prefix + per-hijack type

BACKUP

[1] ARTEMIS website www.inspire.edu.gr/artemis/

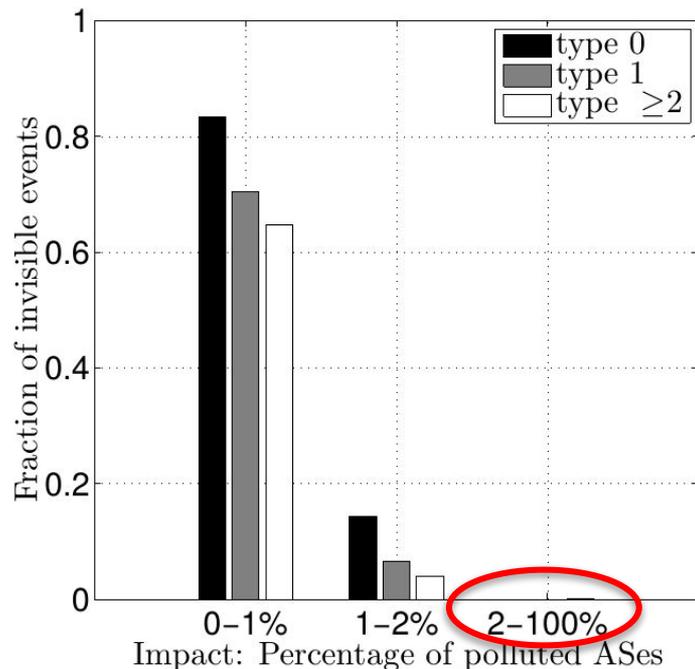
[2] P. Sermpezis et al., "[ARTEMIS: Neutralizing BGP Hijacking within a Minute](#)", in ACM/IEEE ToN, vol. 26, iss. 6, 2018.

[3] G. Chaviaras et al., "[ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking](#)", ACM SIGCOMM '16 demo.

Question 1: Which hijacks are visible?

- Public BGP monitor infrastructure
 - RIPE RIS, RouteViews
 - ~100s vantage points worldwide (BGP routers)

Simulation results on
the AS-level graph [1]

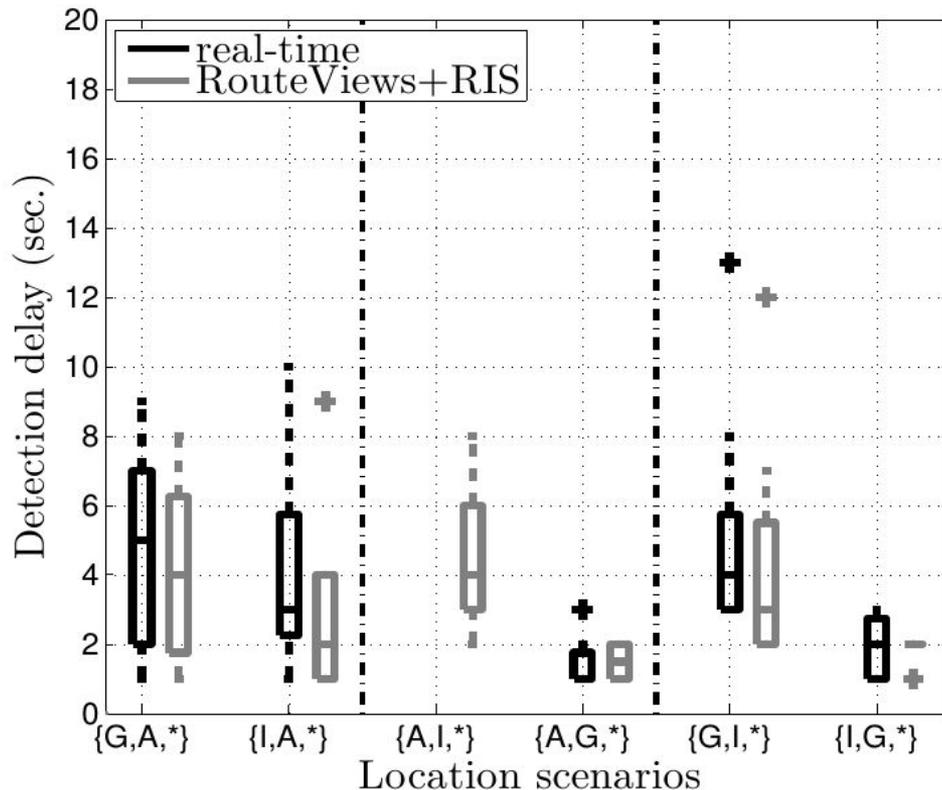


BACKUP

Question 2: How fast can ARTEMIS detect them?

BACKUP

Real experiments in
the Internet [1]
(PEERING testbed)



[1] P. Sermpezis et al., "[ARTEMIS: Neutralizing BGP Hijacking within a Minute](#)", in IEEE/ACM ToN, vol. 26, iss. 6, 2018.

Question 3: How accurate is the detection?

Hijacking Attack			ARTEMIS Detection				
Prefix	AS-PATH (Type)	Data Plane	False Positives (FP)	False Negatives (FN)	Detection Rule	Needed Local Information	Detection Approach
Sub-prefix	*	*	None	None	Config. vs BGP updates	Pfx.	Sec. 5.2
Squatting	*	*	None	None	Config. vs BGP updates	Pfx.	Sec. 5.2
Exact	0/1	*	None	None	Config. vs BGP updates	Pfx. + ASN (+ neighbor ASN)	Sec. 5.3
Exact	≥ 2	*	$< 0.3/\text{day}$ for $> 73\%$ of ASes	None	Past Data vs BGP updates (bidirectional link)	Pfx.+ Past AS links	Sec. 5.4 Stage 1
Exact	≥ 2	*	None for 63% of ASes ($T_{s2} = 5min,$ $th_{s2} > 1$ monitors)	$< 4\%$	BGP updates (waiting interval, bidirectional link)	Pfx.	Sec. 5.4 Stage 2

BACKUP

Question 4: How can hijacks be mitigated?

- DIY: react by **de-aggregating** if you can
- Otherwise (e.g., /24 prefixes) **get help** from other ASes
→ *announcement (MOAS) and tunneling from siblings or helper AS(es)*

TABLE 7: Mean percentage of polluted ASes, when outsourcing BGP announcements to organizations providing DDoS protection services; these organizations can provide highly effective outsourced mitigation of BGP hijacking.

	without outsourcing	top ISPs	AK	CF	VE	IN	NE
Type0	50.0%	12.4%	2.4%	4.8%	5.0%	7.3%	11.0%
Type1	28.6%	8.2%	0.3%	0.8%	0.9%	2.3%	3.3%
Type2	16.9%	6.2%	0.2%	0.4%	0.4%	1.3%	1.1%
Type3	11.6%	4.5%	0.1%	0.4%	0.3%	1.1%	0.5%

BACKUP

Automated & flexible mitigation

- Automated: triggered immediately upon detection
- Flexible: configure per prefix / hijack type / impact / etc.

BACKUP

detection + mitigation:

NOW

ARTEMIS

hours/days **→** **1 min.**

