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

(funded by RIPE NCC Community Projects)

Petros Gigis

(Joint work with: Dimitris Mavrommatis, Vasileios Kotronis, Pavlos Sermpezis, Xenofontas Dimitropoulos, Alberto Dainotti, Alistair King)

UKNOF 45, London, UK, 15 January, 2020

ARTEMIS

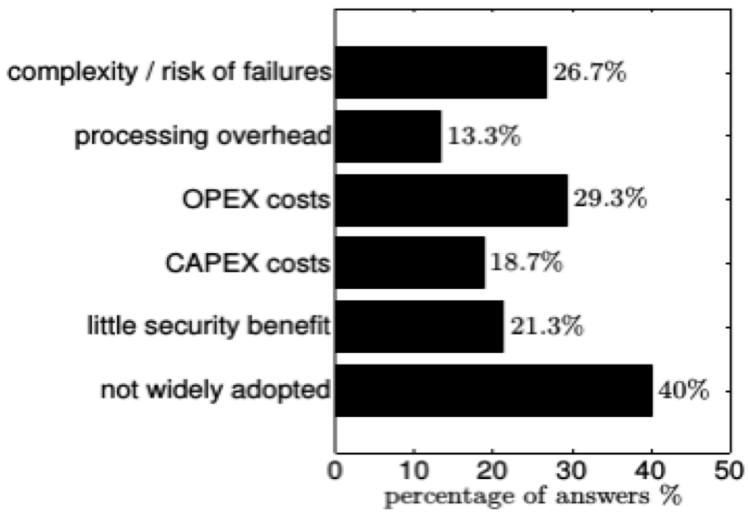
FORTH INSTITUTE OF COMPUTER SCIENCE

INternet Security & Privacy Intelligence REsearch Group

caida

How do people deal with hijacks today?→ **RPKI**

- X **< 20%** of prefixes covered by ROAs [1]
- X Why? → limited adoption & costs/complexity [2]
- X Does not protect the network against all attack types

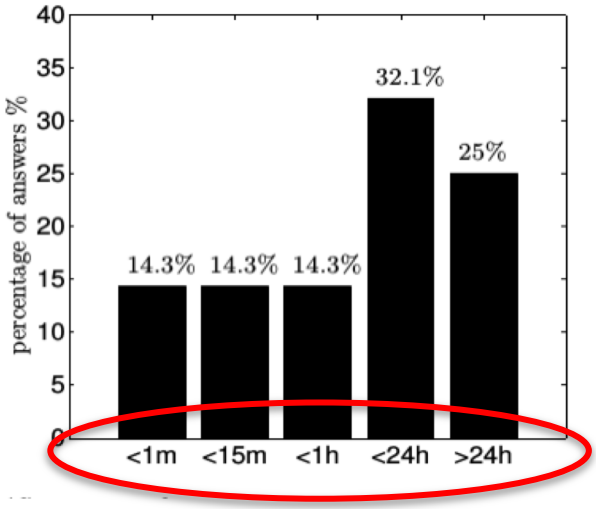


Reasons for not using RPKI [2]

[1] NIST. RPKI Monitor https://rpki-monitor.antd.nist.gov/, Jan. 2020.
[2] P. Sermpezis, 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**

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



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

[1] P. Sermpezis, et. al., "*A survey among Network Operators on BGP Prefix Hijacking*", in ACM SIGCOMM CCR, Jan. 2018.

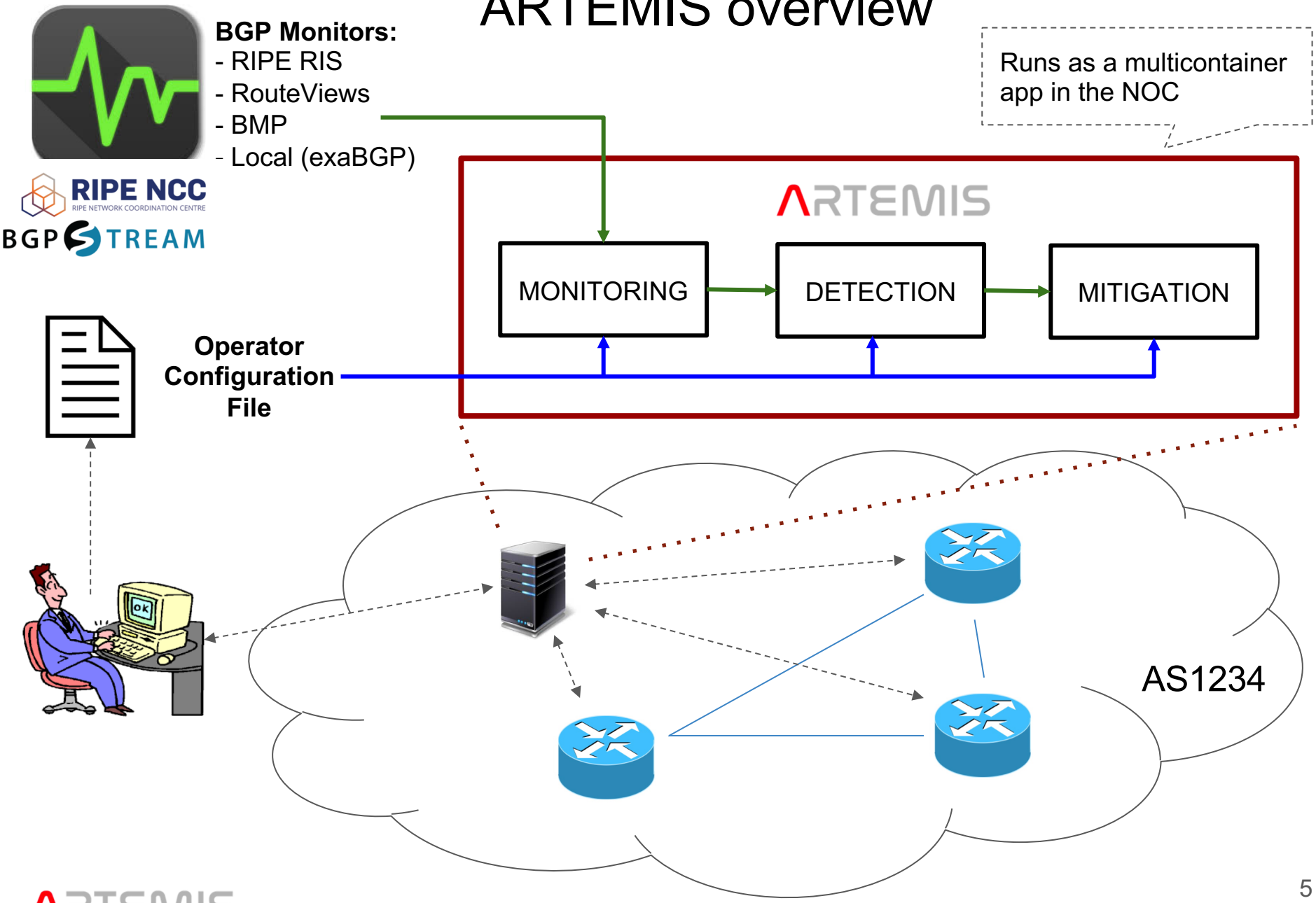
Our solution: ARTEMIS

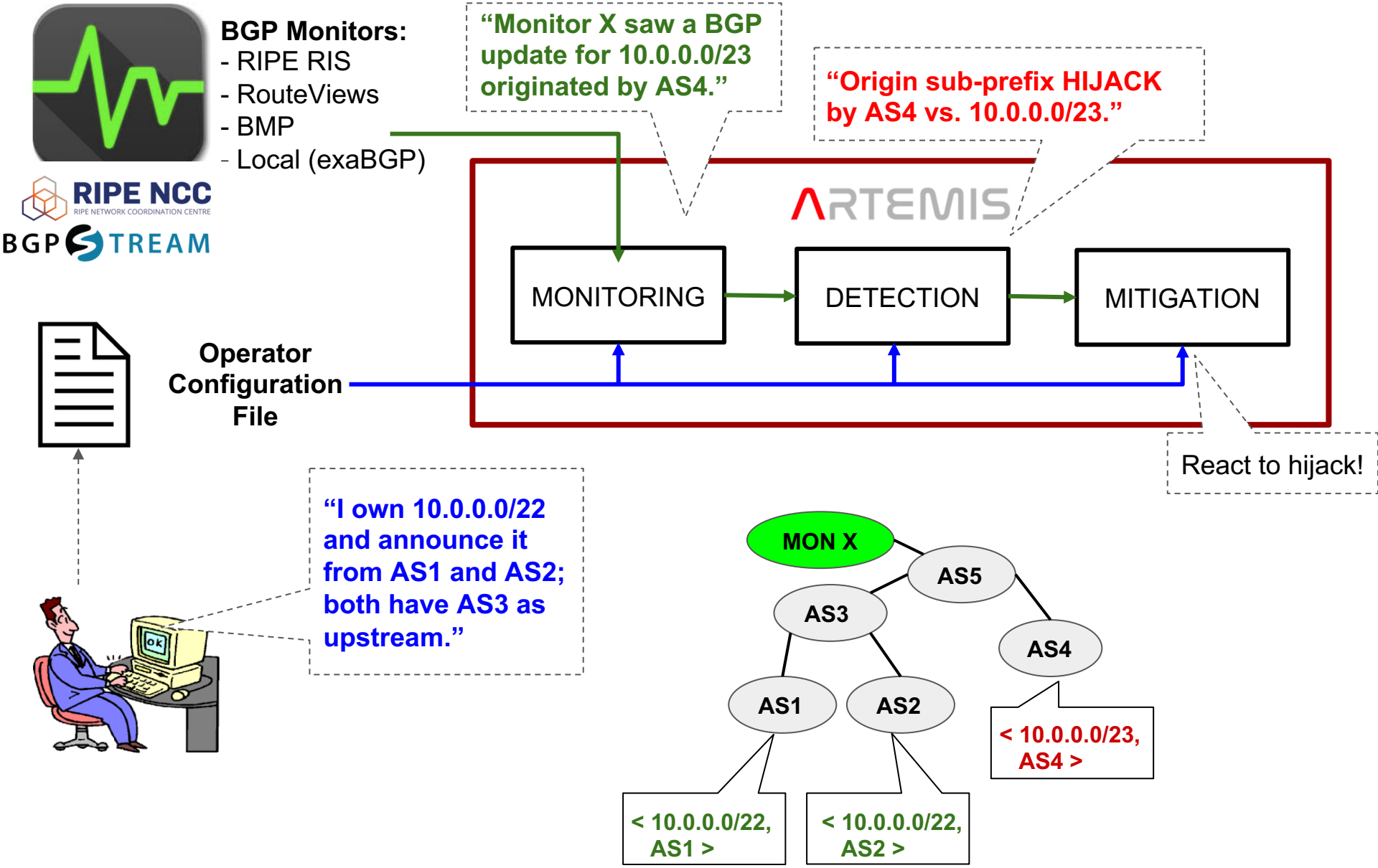
- Operated in-house: no third parties
- Real-time detection
- Flexible automated mitigation

✓ **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

[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.

ARTEMIS overview




BGP Monitors:
- RIPE RIS
- RouteViews
- BMP
- Local (exaBGP)
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
BGPSTREAM
"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."
ARTEMIS
MONITORING
DETECTION
MITIGATION
Operator Configuration File
React to hijack!
"I own 10.0.0.0/22 and announce it from AS1 and AS2; both have AS3 as upstream."
MON X
AS5
AS3
AS4
AS1
AS2
< 10.0.0.0/23, AS4 >
< 10.0.0.0/22, AS1 >
< 10.0.0.0/22, AS2 >

ARTEMIS: detection of **all** hijack types

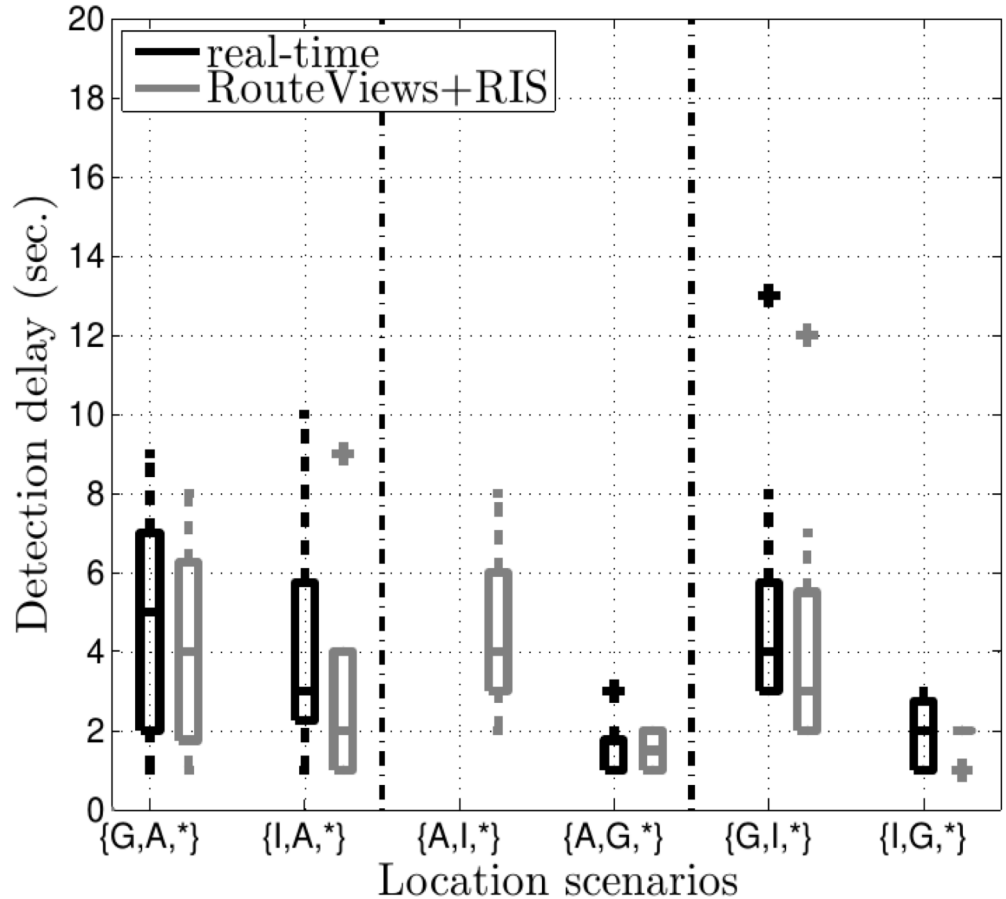
- Hijack types taxonomy - 4 dimensions:
  1. Affected prefixes:
     prefix or ***sub-prefix*** or ***squatting***
  2. Data-plane:
     blackholing or ***imposture*** or ***man-in-the-middle***
  3. AS-path manipulation: ***Type-0*** or ***Type-1*** or … or ***Type-N***

- Legit announcement: <my_prefix, **MY_AS**>
- Type-0 hijack: <my_prefix, **BAD_AS**, …>
- Type-1 hijack: <my_prefix, **MY_AS**, **BAD_AS**, …>
- Type-2 hijack: <my_prefix, **MY_AS**, MY_PEER, **BAD_AS**, …>
- …
- Type-N hijack: <my_prefix, **MY_AS**, ..., **BAD_AS**, …>
- Type-U hijack: <my_prefix, unaltered_path>

  4. Policy violation: ***No export route leak***

ARTEMIS: real-time monitoring, detection in *5 sec.*!

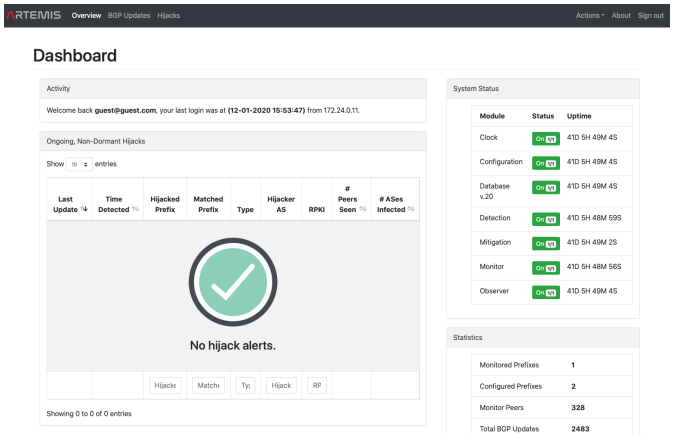
Real experiments in the Internet [1] (PEERING testbed)



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

ARTEMIS Open-source tool (1/2)
https://github.com/forth-ics-inspire/artemis

- Built as a multi-container Docker application
  - Easy to install and operate/maintain
- Can be used in 3 basic modes
  - Passive monitor (Collect only BGP Updates for your prefixes)
  - Passive detector (Collect BGP Updates and apply the detection algorithms)
  - Active joint detector and user-triggered mitigator (Collect, detect and mitigate hijack)
- Support for Kubernetes deployment
- Automatic tagging of hijack incidents
- Support for both IPv4/IPv6 prefixes

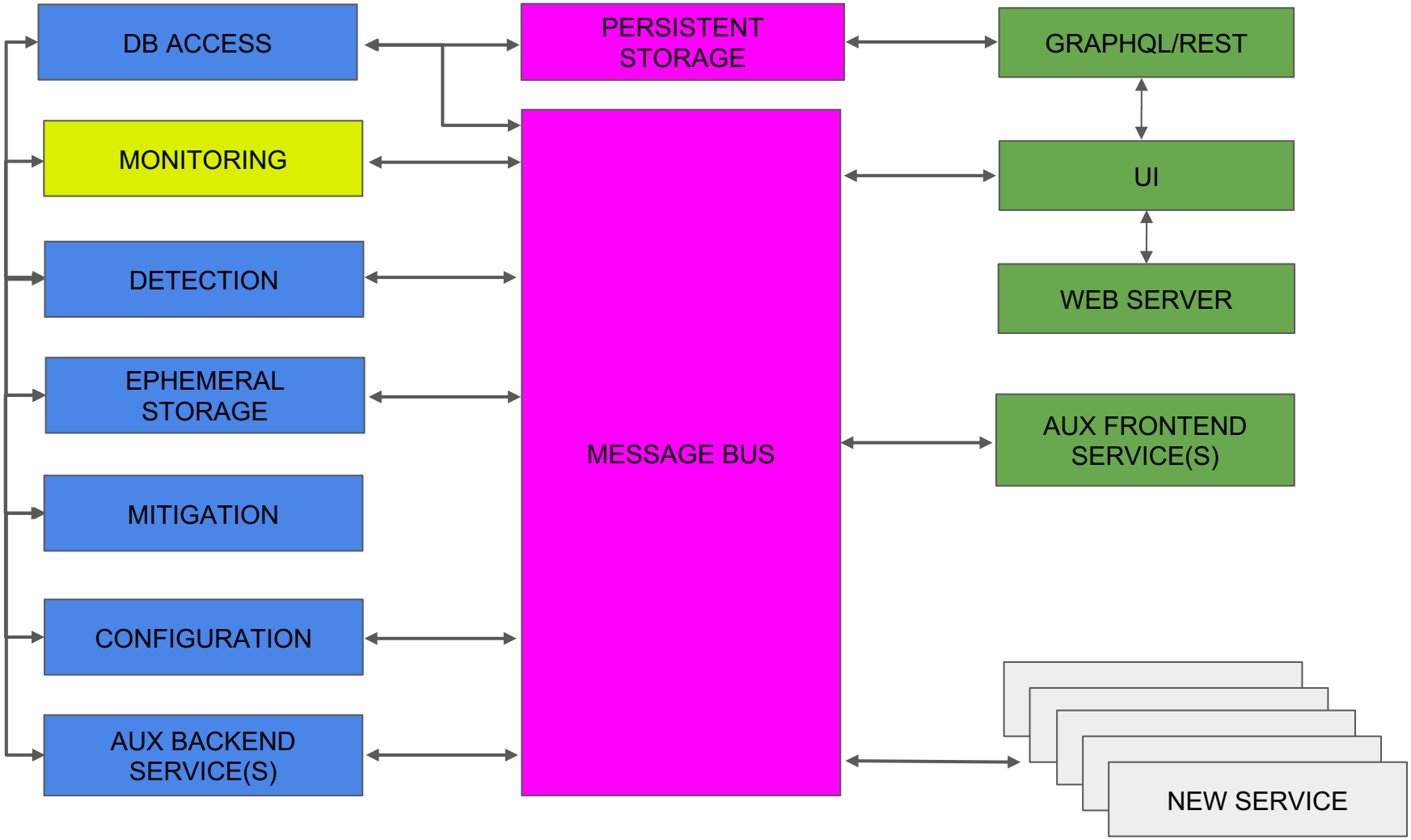


ARTEMIS

ARTEMIS Open-source tool (2/2)
https://github.com/forth-ics-inspire/artemis

- Manual or manually controlled mitigation of BGP prefix hijacking attacks
- Comprehensive web-based GUI
- Support for historical BGP update replaying
- Support for automated generation of the configuration file
- Support for RPKI validation of hijacked prefixes
- Compatibility with Grafana charts
- Modularity/extensibility by design

ARTEMIS Architecture



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|-|-

Example of Configuration file (1/4)

```
#
# 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
```

Example of Configuration file (2/4)

```
#
# ARTEMIS Configuration File
#

# Start of Monitor Definitions

monitors:
        riperis: ['']
        bgpstreamlive:
        - routeviews
        - ris
        - caida
        # exabgp:
        # - ip: 192.168.1.1
        #   port: 5000

# End of Monitor Definitions
```

Example of Configuration file (3/4)

```
#
# ARTEMIS Configuration File
#

# Start of ASN Definitions

asns:
     forth_asn: &forth_asn
     - 8522
     grnet_forth_upstream: &grnet_forth_upstream
     - 5408
     vodafone_forth_upstream: &vodafone_forth_upstream
     - 12361

# End of ASN Definitions
```

Example of Configuration file (4/4)

```
#
# ARTEMIS Configuration File
#

# Start of Rule Definitions

rules:
- prefixes:
  - *forth_prefix_main
  origin_asns:
  - *forth_asn
  neighbors:
  - *grnet_forth_upstream
  - *vodafone_forth_upstream
  mitigation: manual

# End of Rule Definitions
```

PEERING DEMO: Disclaimer

- In the following, I am using the PEERING BGP Testbed 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

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

Dashboard

Activity

Welcome back **admin@admin**, your last login was at **(03-09-2019 13:43:35)** from 172.18.0.8.

Ongoing, Non-Dormant Hijacks

Show 10 entries

Last Update	Time Detected	Hijacked Prefix	Matched Prefix	Type	Hijacker AS	RPKI	# Peers Seen	# ASes Infected	Ack	More
		Hijacl	Matcl	Tyl	Hijac	R				

No hijack alerts.

Showing 0 to 0 of 0 entries

*Times are shown in your local time zone **GMT-0 (Europe/London)**.*

System Status

Module	Status	Uptime
Clock	On 1/1	0D 0H 43M 38S
Configuration	On 1/1	0D 0H 43M 38S
Database v.20	On 1/1	0D 0H 43M 38S
Detection	On 1/1	0D 0H 6M 1S
Mitigation	On 0/1	
Monitor	On 1/1	0D 0H 6M 0S
Observer	On 1/1	0D 0H 4M 42S

Statistics

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

ARTEMIS

Deploy the demo configuration

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

System

Monitor Module

Active 1/1

Detection Module

Active 1/1

Mitigation Module

Active 0/1

Current Configuration

Load AS-SETs Edit

Configuration file updated.

```
  bgpstreamlive:
  - routeviews
  - ris
  - caida
    # bgpstreamkafka:
    #     host: bmp.bgpstream.caida.org
    #     port: 9092
    #     topic: '^openbmp\.router--.+\.peer-as--.+\.bmp_raw'
    # exabgp:
    #     - ip: exabgp
    #       port: 5000
    # bgpstreamhist:
    #     - <csv_dir_with_formatted_BGP_updates>
# End of Monitor Definitions
#
# Start of ASN Definitions
asns:
  peering_asn: &peering_asn
  - 47065
  los_nettos_upstream: &los_nettos_upstream
  - 226
# End of ASN Definitions
#
# Start of Rule Definitions
rules:
- prefixes:
  - *peering_prefix_main
  origin_asns:
  - *peering_asn
  neighbors:
  - *los_nettos_upstream
  mitigation: manual
# End of Rule Definitions
```

ARTEMIS

Make “legitimate” announcement from isi01 site

(Origin AS: 47065, Upstream AS: 226)

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

BGP Updates

Live Update:

All | Past 1h | Past 24h | Past 48h | Custom

Show 5 entries

Download Table

Timestamp	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	Type	Hijack	Status	More
2019-09-04 09:13:37	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 09:13:31	184.164.243.0/24	184.164.243.0/24	47065	50300 2914 226 47065	50300	ripe-ris -> rrc00	A			
2019-09-04 09:13:22	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 09:13:07	184.164.243.0/24	184.164.243.0/24	47065	395152 14007 6939 226 47065	395152	ripe-ris -> rrc00	A			
2019-09-04 09:12:47	184.164.243.0/24	184.164.243.0/24	47065	12307 57118 29691 13030 226 47065	12307	ripe-ris -> rrc20	A			
	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	A|W			

Showing 1 to 5 of 716 entries

1 2 3 4 5 ... 144

*Times are shown in your local time zone **GMT-0 (Europe/London)**.*

Additional actions

View distinct values

Select

ARTEMIS

Make “illegitimate” announcement from grnet01 site

(Origin AS: 47065, Upstream AS: 5408)

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

BGP Updates

Live Update:

All | Past 1h | Past 24h | Past 48h | Custom

Show 5 entries

Download Table

Timestamp	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	Type	Hijack	Status	More
2019-09-04 09:31:09	184.164.243.0/24	184.164.243.0/24	47065	328145 1299 21320 21320 21320 21320 5408 47065	328145	ripe-ris -> rrc01	A			
2019-09-04 09:30:56	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			
2019-09-04 09:30:55	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			
2019-09-04 09:30:55	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			
2019-09-04 09:30:42	184.164.243.0/24	184.164.243.0/24	47065	206499 34549 13101 2603 21320 5408 47065	206499	ripe-ris -> rrc00	A			
	Prefix	Matched Prefix	Origin AS	AS Path	Peer AS	Service	A|W			

Showing 1 to 5 of 913 entries

1 2 3 4 5 ... 183

*Times are shown in your local time zone **GMT-0 (Europe/London)**.*

ARTEMIS

ARTEMIS detects the Hijack in real time

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

Viewing Hijack Ongoing

Hijack Information

Not Acknowledged

Hijacker AS:	5408	**Time Started:**	2019-09-04 09:29:34
Type:	E|1|-|-	**Time Detected:**	2019-09-04 09:29:40
# Peers Seen:	109	**Last Update:**	2019-09-04 09:31:09
# 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 09:05:17	**RPKI Status:**	NA
Key:	426c0897c7cb3455e077fb369cb6d9d		

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 09:31:09	184.164.243.0/24	42807	328145 1299 21320 21320 21320 21320 5408 47065	328145	ripe-ris -> rrc01	A		

ARTEMIS

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

Next steps for the Open-source tool

- Verification and monitoring of BGP prefix hijacking incidents using RIPE Atlas probes
  - Selected as one of the Community Funded projects of RIPE NCC for 2019

- Auto-mitigation
  - Ansible + Python
  - Prefix deaggregation
  - GRE tunnelling using helper AS

- Further maintenance and testing of the tool

- Mobile notification App

- Integrate side project enabling auto-configuration and auto-mitigation using Ansible (https://github.com/georgeepta/artemis-ansible)

Thank you! Questions?

- Current ARTEMIS users:
  - ***Internet2***, the biggest R&E network in the US
  - ***AMS-IX***, one of the biggest European Internet eXchange Points
  - A major Greek ISP with hundreds of active peerings
  - ***FORTH***, a stub dual-homed academic network
  - Many others…

- What do we want from you?
  - Try demo at: http://inspire.edu.gr/artemis/demo/ (creds: guest / guest@artemis2018)
  - Visit the ARTEMIS website *http://www.inspire.edu.gr/artemis/*
  - **Download and deploy** ARTEMIS in your network ☺ https://github.com/FORTH-ICS-INSPIRE/artemis

- Stay in touch with us:
  - Mailing list: http://lists.ics.forth.gr/mailman/listinfo/artemis
  - Discord channel: https://discordapp.com/invite/8UerJvh

funded by: RIPE NCC RIPE NETWORK COORDINATION CENTRE NSF erc European Research Council Established by the European Commission

BACKUP

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

RIPE NCC
RIPE NETWORK COORDINATION CENTRE
BGPSTREAM

"2 monitors saw in last 5 minutes < 10.0.0.0/22, AS1, AS2, AS4, … >"

"Link AS2-AS4 not seen in last 10 months for any prefix or direction. Path manipulation exact -prefix HIJACK by AS4 vs. 10.0.0.0/22."

ARTEMIS

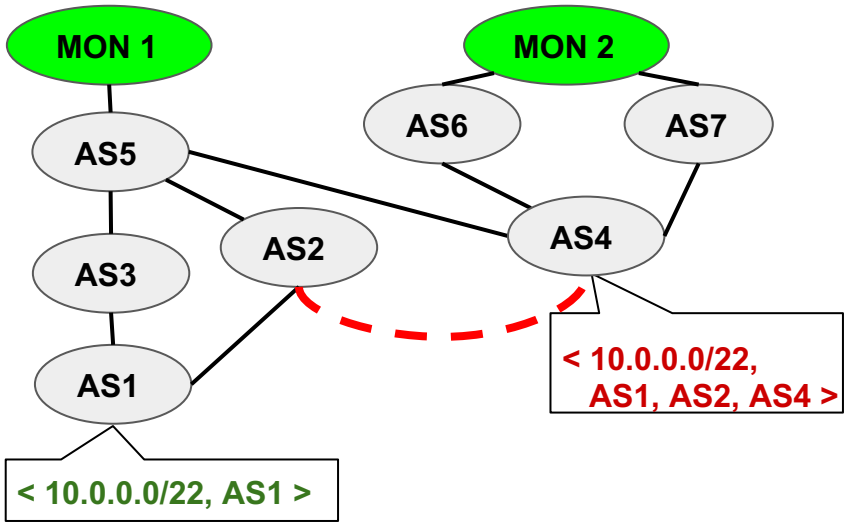
MONITORING → DETECTION → MITIGATION

BACKUP

Operator Configuration File

React to hijack!

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



ARTEMIS

ARTEMIS: mitigation methods (BACKUP)

- 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%

ARTEMIS: Hijacks Page

BACKUP

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

Hijacks

Live Update:

All | Past 1h | Past 24h | Past 48h | Custom

Type hijack key... View

Show 10 entries

Selected Hijacks Mark as Ignored Apply Clear

Download Table

Last Update	Time Detected	Status	Hijacked Prefix	Matched Prefix	Type	Hijacker AS	RPKI	# Peers Seen	# ASes Infected	Ack	More
2020-01-12 20:50:31	2020-01-12 20:50:35	Ongoing	139.185.5.0/24	139.0.0.0/8	S|0|-|-	793	NA	1	2		View
2020-01-12 20:50:31	2020-01-12 20:50:35	Resolved	139.185.0.0/17	139.0.0.0/8	S|0|-|-	793	NA	1	2		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Resolved	139.5.98.0/24	139.0.0.0/8	S|0|-|-	55879	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Ignored	139.5.97.0/24	139.0.0.0/8	S|0|-|-	55879	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Ignored	139.5.96.0/24	139.0.0.0/8	S|0|-|-	55879	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Resolved	139.190.237.0/24	139.0.0.0/8	S|0|-|-	55453	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Resolved	139.190.236.0/24	139.0.0.0/8	S|0|-|-	55453	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Resolved	139.5.116.0/24	139.0.0.0/8	S|0|-|-	17539	NA	1	2		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Ignored	139.5.145.0/24	139.0.0.0/8	S|0|-|-	45328	NA	1	3		View
2020-01-12 20:50:31	2020-01-12 20:50:34	Ignored	139.5.155.0/24	139.0.0.0/8	S|0|-|-	38320	NA	1	2		View
			Hijacked Prefix	Matched Prefix	Type	Hijack AS	RPKI				

Showing 1 to 10 of 450 entries

1 2 3 4 5 ... 45

Select Status: Ongoing / Dormant / Resolved / Ignored / Under Mitigation / Withdrawn / Outdated

*Times are shown in your local time zone **GMT-0 (Europe/London)**.*

ARTEMIS: User Management

BACKUP

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

User Management

Approve pending users

Select pending user to approve:

Approve user

Promote to Admin

Select user to give admin privileges:

Promote to Admin

Demote Admin

Select user to remove admin privileges:

Demote to User

Delete user

Select user to delete:

Delete User

User list

Show 10 entries Search:

ID	Username	Email	Role	Last Login
1	admin	admin@admin	admin	18-12-2019 17:43:35

Showing 1 to 1 of 1 entries 1

Times are shown in your local time zone.

ARTEMIS: Configuration Comparison

BACKUP

ARTEMIS Overview BGP Updates Hijacks Admin Actions About Sign out

Configuration Comparison

Select config:

Timestamp: 2019-12-11 15:56:11

```
1  #
2  # ARTEMIS Configuration File (default config, please change in your deployment)
3  #
4  # Defining a named variable:
5  #     named_variable: &named_variable
6  #         value_of_variable
7  # Use named variable:
8  #     *named_variable
9  # - denotes an entry
10 #
11 # Start of Prefix Definitions (IPv4 and IPv6 are supported)
12 prefixes:
13     super_prefix: &super_prefix
14         - 139.91.0.0/16
15     sub_prefix_1: &sub_prefix_1
16         139.91.250.0/24
17     sub_prefix_2: &sub_prefix_2
18         139.91.2.0/24
19 # End of Prefix Definitions
20 #
21 # Start of Monitor Definitions
22 monitors:
23     riperis: [''] # by default this uses all available monitors
24     bgpstreamlive:
25         - routeviews
26         - ris
27         - caida
28     # bgpstreamkafka:
29     #     host: bmp.bgpstream.caida.org
30     #     port: 9092
31     #     topic: '^openbmp\.router--.+\.peer-as--.+\.bmp_raw'
32     # exabgp:
33     #     - ip: exabgp
```

Select config:

Timestamp: 2019-12-18 17:45:36

```
1  #
2  # ARTEMIS Configuration File (default config, please change in your deployment)
3  #
4  # Defining a named variable:
5  #     named_variable: &named_variable
6  #         value_of_variable
7  # Use named variable:
8  #     *named_variable
9  # - denotes an entry
10 #
11 # Start of Prefix Definitions (IPv4 and IPv6 are supported)
12 prefixes:
13     super_prefix: &super_prefix
14         - 139.0.0.0/8
15     sub_prefix_1: &sub_prefix_1
16         139.91.250.0/24
17     sub_prefix_2: &sub_prefix_2
18         139.91.2.0/24
19 # End of Prefix Definitions
20 #
21 # Start of Monitor Definitions
22 monitors:
23     riperis: [''] # by default this uses all available monitors
24     bgpstreamlive:
25         - routeviews
26         - ris
27         - caida
28     # bgpstreamkafka:
29     #     host: bmp.bgpstream.caida.org
30     #     port: 9092
31     #     topic: '^openbmp\.router--.+\.peer-as--.+\.bmp_raw'
32     # exabgp:
33     #     - ip: exabgp
```

Configuration comments

ARTEMIS

BGP prefix hijacking is a critical threat

→ to your **organization** & **customers** & **peers**

BACKUP

- **Outages** in the Internet cause losses of millions of $$$
- **Interception** of bitcoins, credit card transactions, passwords, ...
- **Bad reputation** for hijacked networks: security, service reliability

...only in 2017: ***5,304*** hijacks, with ***3,106*** organizations as victims [1]

[1] "14,000 Incidents: A 2017 Routing Security Year in Review", www.internetsociety.org

Threat Model → the hijacker:

- controls a single AS and its edge routers
- has full control of the control plane and data plane within its own AS
- can arbitrarily manipulate the:
  - BGP messages that it sends to its neighboring ASes (control plane)
  - traffic that crosses its network (data plane)
- has otherwise no control over BGP messages and traffic exchanged between two other ASes.

BACKUP

→ Extensions (future work): multiple ASes controlled by a single hijacker

Note: What we do not cover as hijacks →route leaks

- Not actual hijacks in the classic threat model
  - All links involved in the announced paths are valid!
- Fall in the context of “policy violations”, e.g.,
  - What if Google decided to be a Tier-1 global transit network for one hour?
  - What if your friendly IXP peer decided to act as your upstream?
- Detecting them requires detailed knowledge of in-path policies
  - These are not publicly available
  - Existing datasets → would yield high numbers of FP
  - 30% of observed routes are not consistent with available routing policy data [1]
  - **Ongoing work! (beyond “good filtering”)**

BACKUP

ARTEMIS

[1] Ruwaifa Anwar et al. Investigating interdomain routing policies in the wild. In Proc. ACM IMC, 2015.