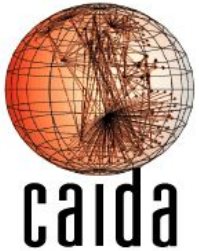
ARTEMIS: Neutralizing BGP Hijacking within a Minute

(funded by 

Community Projects 2017)

Foundation for Research and Technology - Hellas (FORTH), Greece
&
Center for Applied Internet Data Analysis (CAIDA) UCSD, US

RIPE76, Marseille, France, 14-18 May, 2018



Hijacks: Human Errors

Today's BGP leak in Brazil

Posted by Andree Toonk - October 21, 2017 - News and Updates - No Comme

Earlier today several people noticed network reachability prob
Twitter, Google and others. The root cause turned out to be another BGP mishap.

```
mtr -4rwc10 172.217.16.106
Start: 2017-10-21T13:26:55+0200
HOST: linux-0lcz                                   Loss%  Drop   Rcv   Snt   Last   Best   Avg  Wrst StDev Gmean Jttr Javg Jmax Jint
  1. AS???    10.235.224.157                        0.0%     0    10    10   71.9   37.6  56.7  71.9   9.3  56.0  15.8   9.1  16.2  72.4
  2. AS62292  217.112.143.217                       0.0%     0    10    10   58.8   47.0  54.8  65.2   6.2  54.5   1.3   7.1  16.7  53.2
  3. AS???    bix.he.net (193.188.137.175)          0.0%     0    10    10   45.8   45.1  55.9  69.3   7.4  55.4  16.2   7.7  16.2  62.6
  4. AS6939   100ge11-1.core1.vie1.he.net (184.105.213.249)  10.0%     1     9    10   60.0   44.7  54.0  73.4   8.8  54.0   3.7   8.2  20.0  57.5
  5. AS6939   100ge13-1.core1.par2.he.net (184.105.65.5)    0.0%     0    10    10  125.0   62.0  86.8  120.0  21.7  84.4  52.5  23.3  52.5  193.0
  6. AS6939   100ge10-2.core1.ash1.he.net (184.105.213.173)  0.0%     0    10    10  160.6  144.0  152.1  161.4   6.2  152.0  16.0   6.1  16.0  52.6
  7. AS6939   100ge8-2.core1.atl1.he.net (184.105.213.69)   0.0%     0    10    10  157.5  148.1  164.4  185.9  12.5  164.0  11.1  14.1  37.8  100.2
  8. AS6939   100ge4-1.core1.mia1.he.net (184.105.213.26)   0.0%     0    10    10  174.5  160.1  172.2  181.7   7.9  172.1   0.7   8.1  21.5  59.1
  9. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 10. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 11. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 12. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 13. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 14. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 15. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 16. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 17. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 18. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 19. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 20. AS???    ???                                     100.0    10     0    10    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
 21. AS52320  200.16.70.209                            80.0%     8     2    10  496.2  496.2  498.3  500.5   2.9  498.2   4.1   2.1   4.1   4.1
 22. AS???    45.6.52.32                               88.9%     8     1     9  530.5  530.5  530.5  530.5   0.0  530.5   0.0   0.0   0.0   0.0
 23. AS???    ???                                     100.0     4     0     4    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
```

Fusl
@OhNoItsFusl

VANTAGEPOINT
IN: RESEARCH

Large BGP Leak by Google Disrupts Internet in Japan

Research // Aug 28, 2017 // Doug Madory

情報種別	故障情報
ステータス	
発生日時	2017年08月25日12時22分頃
復旧日時	2017年08月25日12時45分

Hijacks: Malicious Attacks

ANDY GREENBERG SECURITY 08.07.14 01:00 PM

HACKER REDIRECTS TRAFFIC FROM 19 INTERNET PROVIDERS TO STEAL BITCOINS

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT

"Suspicious" event routes traffic for big-name sites through Russia

Google, Facebook, Apple, and Microsoft all affected by "intentional" BGP mishap.

DAN GOODIN - 12/14/2017, 12:43 AM

FORTH INSTITUTE OF COMPUTER SCIENCE caida

BGP prefix hijacking is a critical threat

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

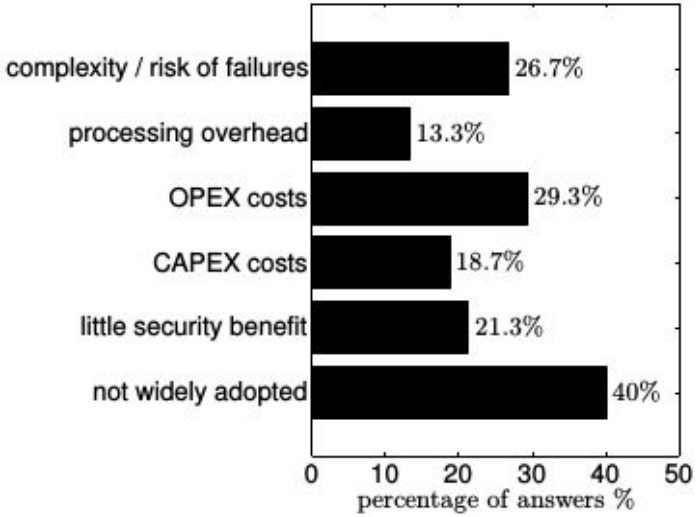
- **Outages** in the Internet cause losses of millions of $$$
- **Interception** of bitcoins, credit card transactions, passwords, ...
- **Bad reputation** for hijacked networks: security, service reliability

...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

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

- ✗ Only **8%** of prefixes covered by ROAs [1]
- ✗ Why? → limited adoption & costs/complexity [2]
- ✗ Does not protect the network against all attack types



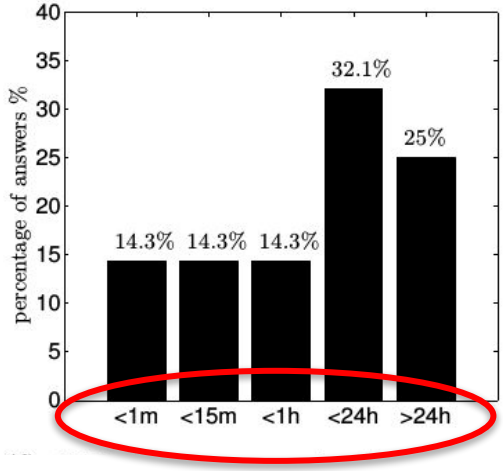
Reasons for not using RPKI [2]

[1] NIST. RPKI Monitor https://rpki-monitor.antd.nist.gov/. May 2018

[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 this today? → **Third parties**

- X **Comprehensiveness**: detect only route leaks or 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]

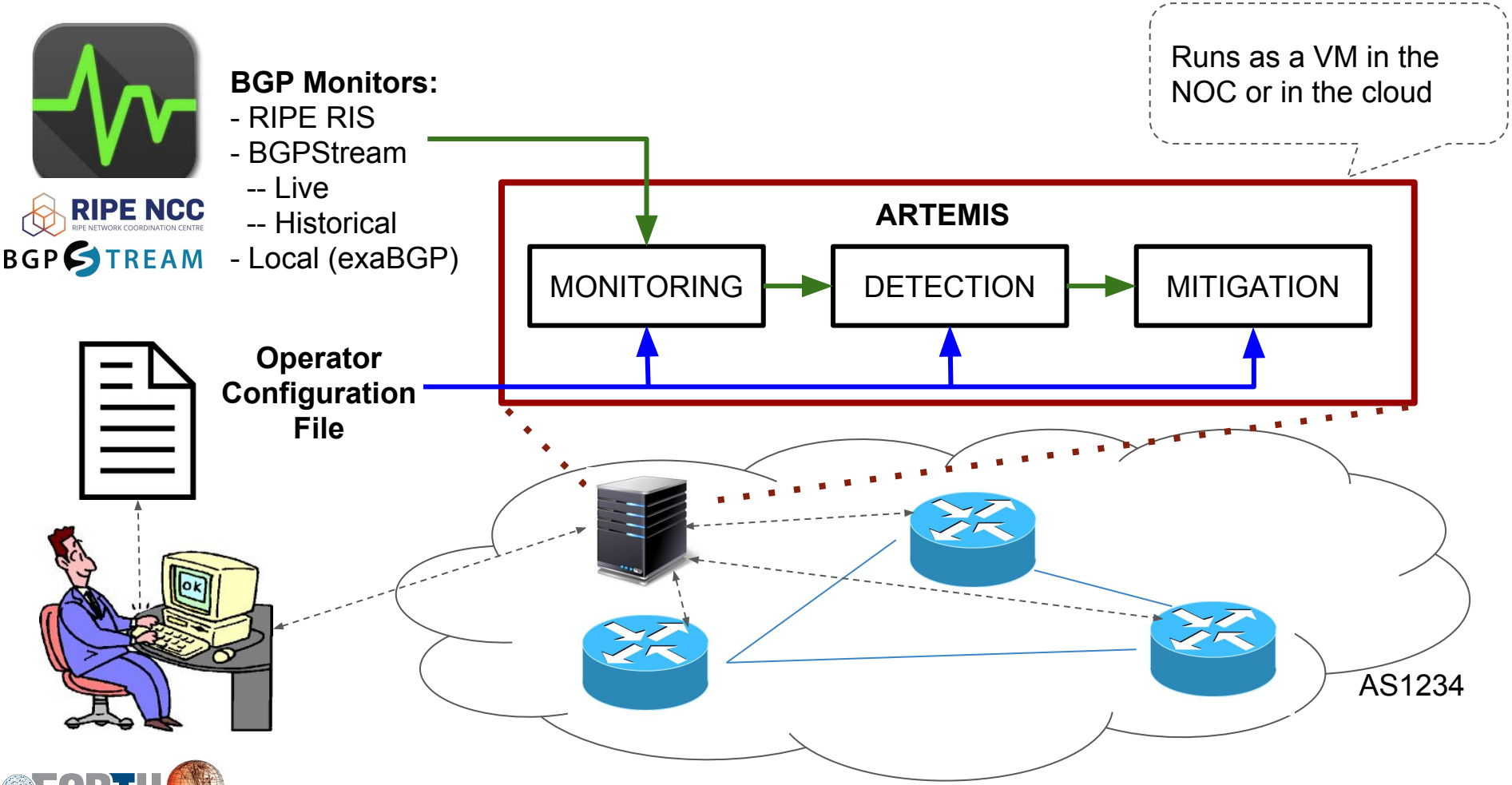
[1] P. Sermpezis, et. al., "*A survey among Network Operators on BGP Prefix Hijacking*", in ACM SIGCOMM CCR, Jan 2018.

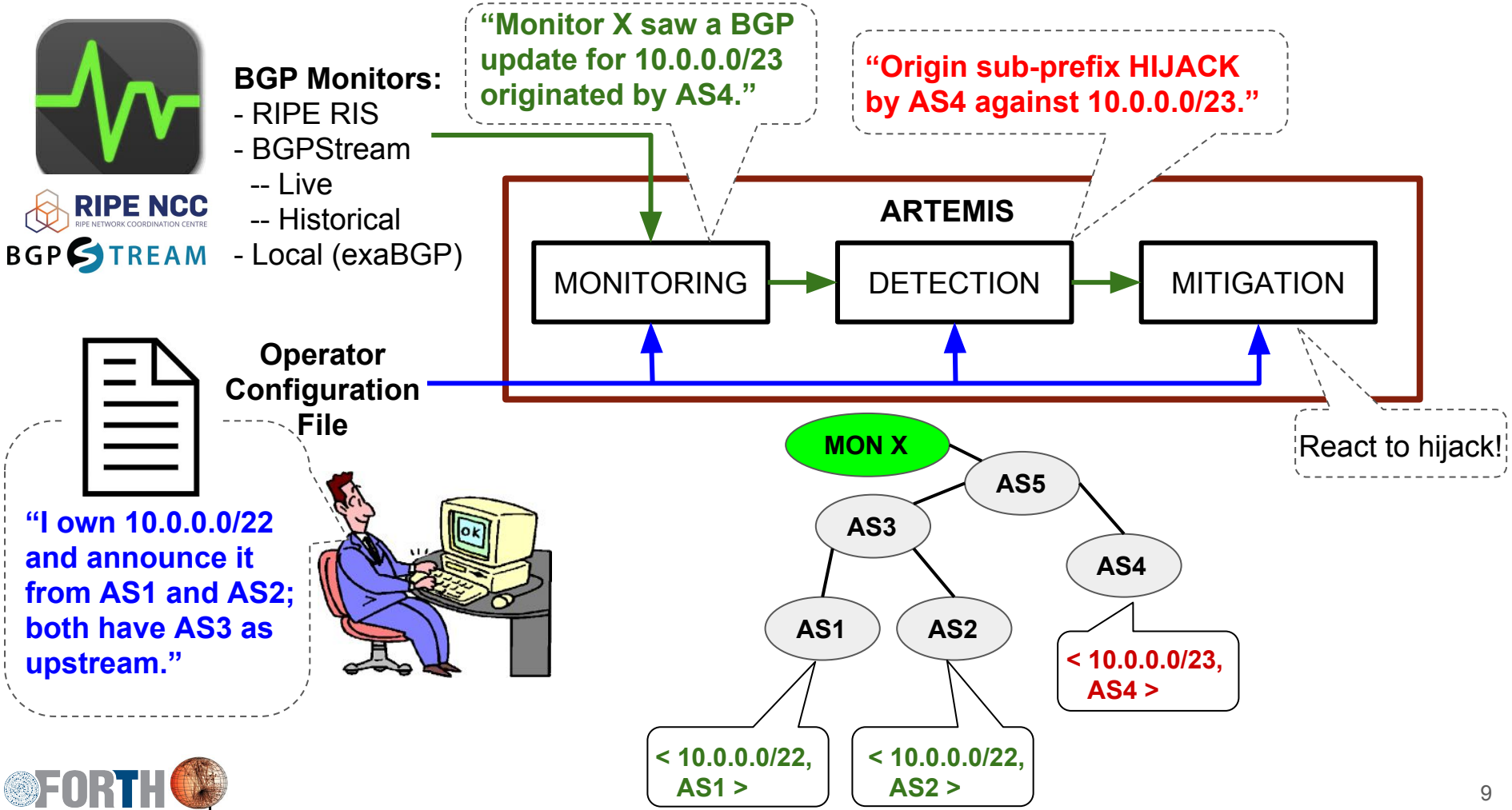
Our solution: ARTEMIS

- Operated in-house: no third parties
- Real-time Detection
- Automatic 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", under revision ACM/IEEE ToN, arXiv 1801.01085.
[3] G. Chaviaras et al., "ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking", ACM SIGCOMM'16 demo.


BGP Monitors:
- RIPE RIS
- BGPStream
-- Live
-- Historical
- Local (exaBGP)
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
BGPSTREAM
Runs as a VM in the NOC or in the cloud
ARTEMIS
MONITORING
DETECTION
MITIGATION
Operator Configuration File
ok
AS1234


BGP Monitors:
- RIPE RIS
- BGPStream
-- Live
-- Historical
- 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 against 10.0.0.0/23."
ARTEMIS
MONITORING
DETECTION
MITIGATION
Operator Configuration File
"I own 10.0.0.0/22 and announce it from AS1 and AS2; both have AS3 as upstream."
ok
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 >
React to hijack!
FORTH
INSTITUTE OF COMPUTER SCIENCE
caida

RIPE NCC
RIPE NETWORK COORDINATION CENTRE
BGPSTREAM

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

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

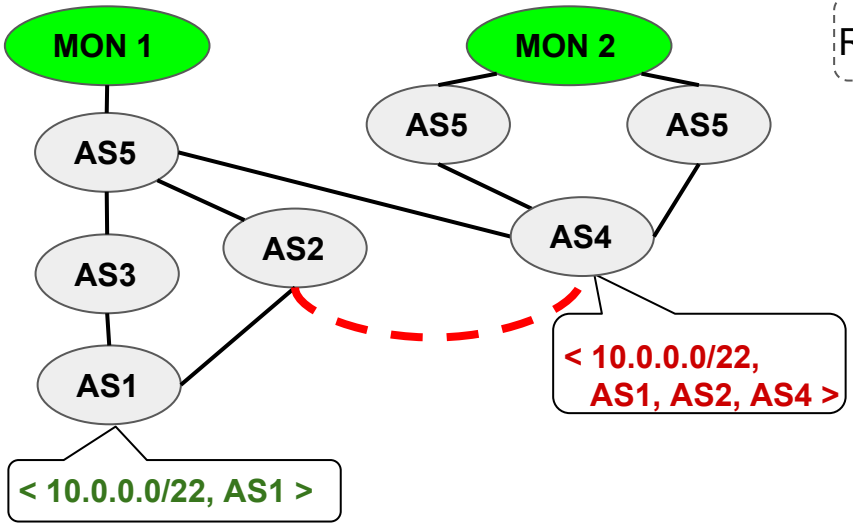
"Link AS2-AS4 not seen in last 10 months for any prefix, in any direction. Path manipulation HIJACK by AS4 against 10.0.0.0/22."

ARTEMIS

MONITORING → DETECTION → MITIGATION

Operator Configuration File

"I own 10.0.0.0/22 and announce it from AS1 with AS2 and AS3 as upstreams."



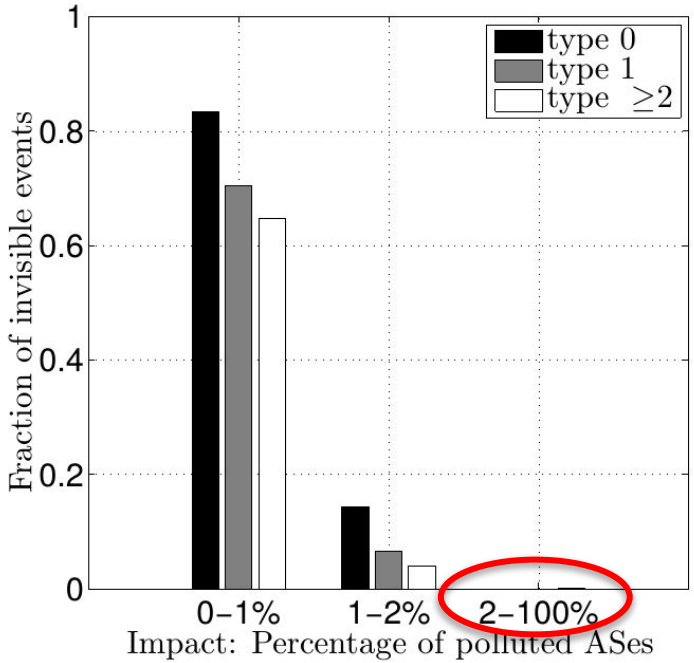
React to hijack!

FORTH INSTITUTE OF COMPUTER SCIENCE
caida

ARTEMIS: Visibility of *all* impactful hijacks

- Public BGP monitor infrastructure
  - RIPE RIS, RouteViews, BGPmon
  - ~500 vantage points worldwide (BGP routers)

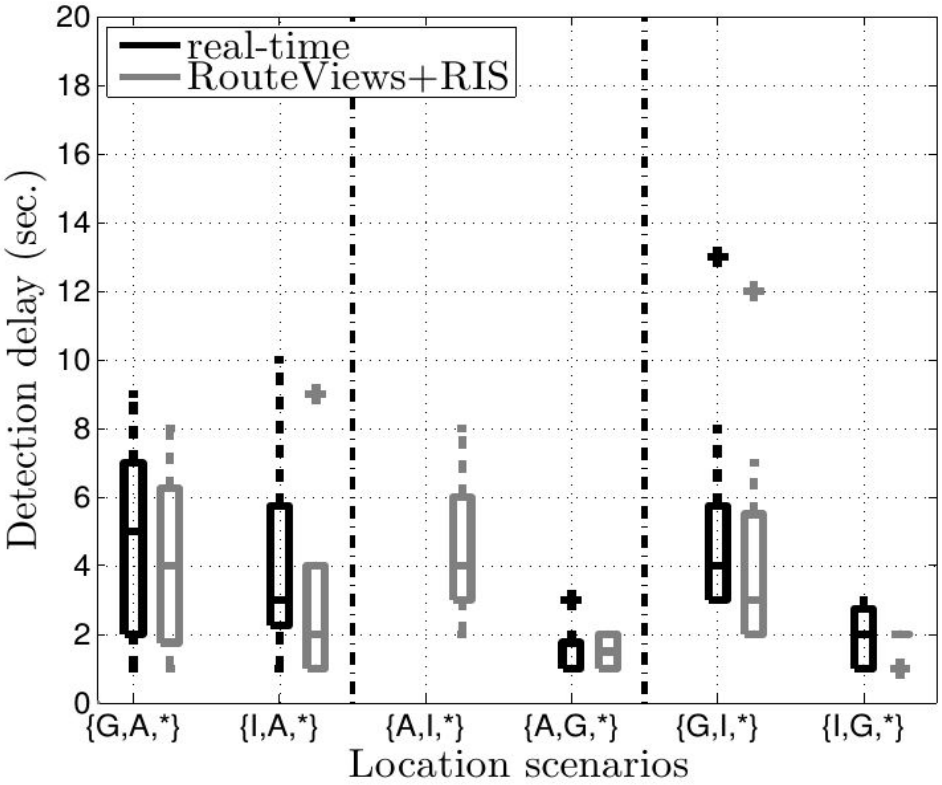
Simulation results on the AS-level graph [1]



[1] P. Sermpezis et al., "*ARTEMIS: Neutralizing BGP Hijacking within a Minute*", under revision IEEE/ACM ToN, arXiv 1801.01085.

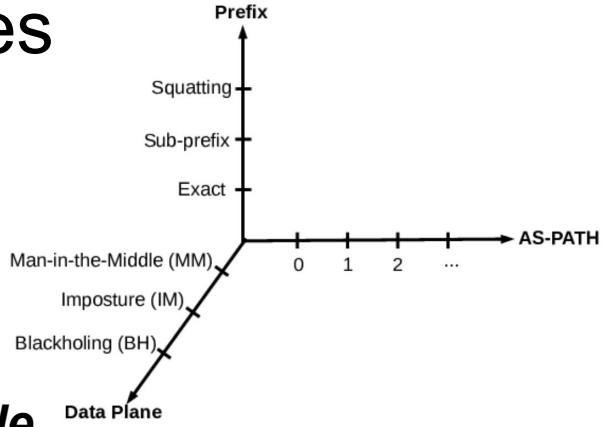
ARTEMIS: real-time monitoring, detection in *5 sec.*!

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



[1] P. Sermpezis et al., "*ARTEMIS: Neutralizing BGP Hijacking within a Minute*", under revision IEEE/ACM ToN, arXiv 1801.01085.

ARTEMIS: detection of *all* hijack types

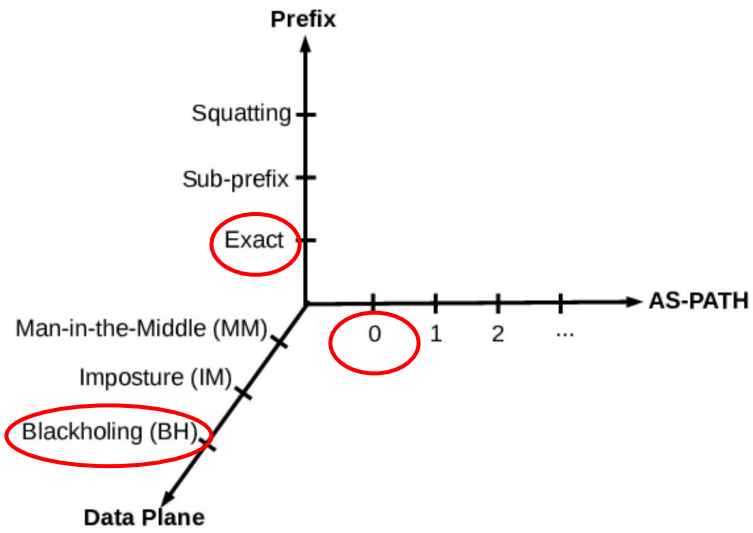


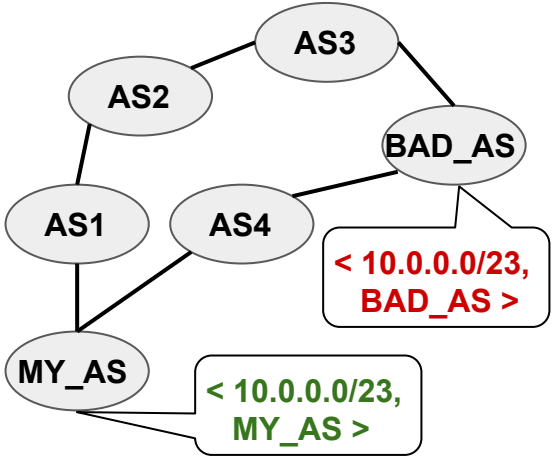
- Hijack types taxonomy - 3 dimensions:
  1. Affected prefixes:
     prefix or ***sub-prefix*** or ***squatting***
  2. Data-plane:
     blackholing or ***imposture*** or ***man-in-the-middle***
  3. AS-path manipulation: ***Type-0*** or ***Type-1*** or … or ***Type-N***
     - Legit announcement: <my_prefix,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

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: detection of *all* hijack types

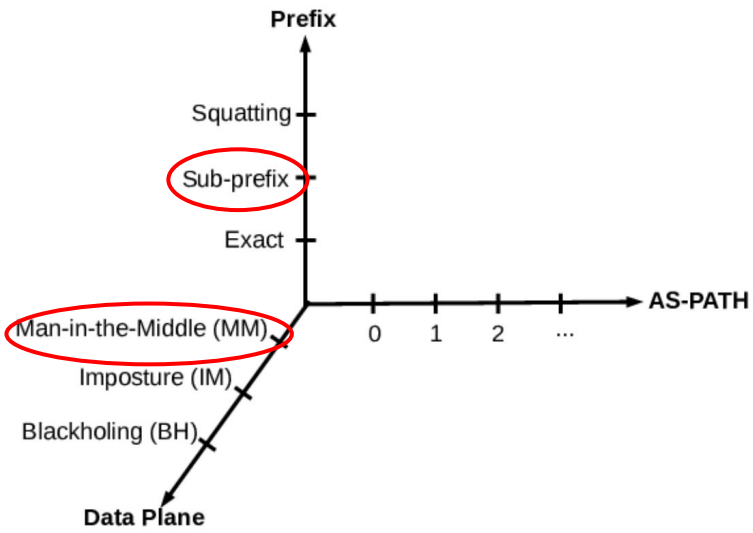
- Taxonomy - Example 1: **prefix** + **Type-0** + **blackholing**

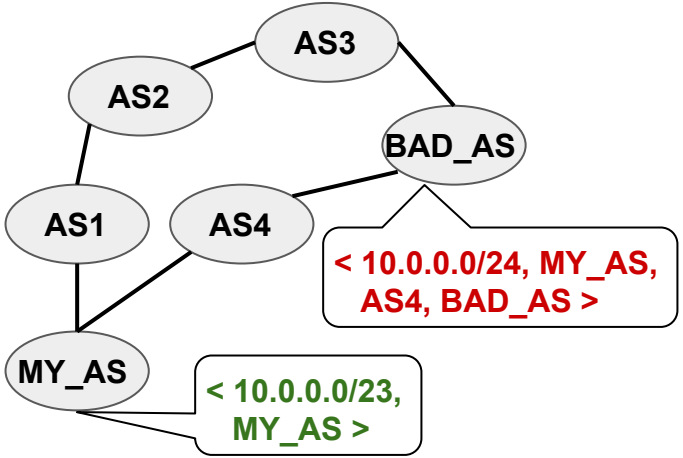




ARTEMIS: detection of *all* hijack types

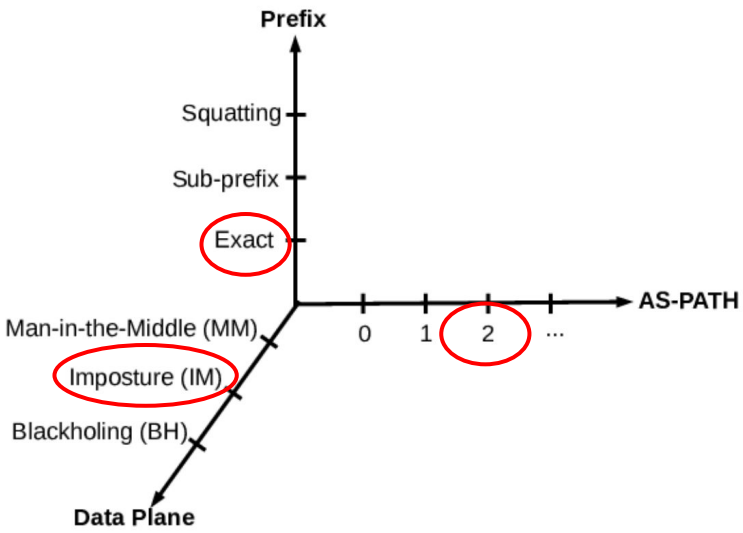
- Taxonomy - Example 2: **sub-prefix** + **Type-U** + **man-in-the-middle**

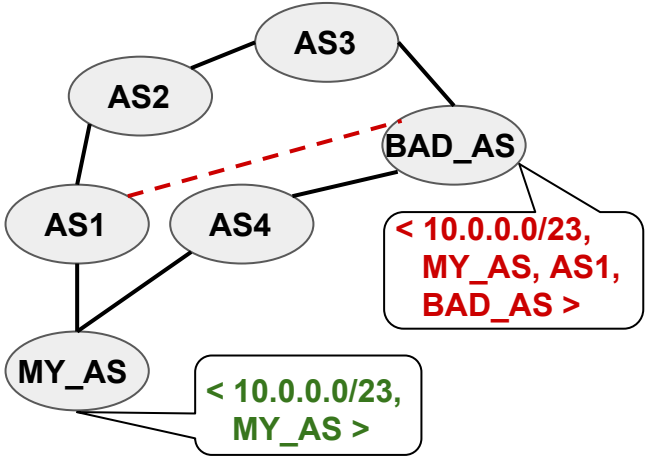




ARTEMIS: detection of *all* hijack types

- Taxonomy - Example 3: **prefix** + **Type-2** + **imposture**





ARTEMIS: detection of *all* hijack types

TABLE 1: Comparison of BGP prefix hijacking detection systems/services w.r.t. ability to detect different classes of attacks.

Class of Hijacking Attack			Control-plane System/Service			Data-plane System/Service		Hybrid System/Service		
Affected prefix	AS-PATH (Type)	Data plane	ARTEMIS	Cyclops (2008) [21]	PHAS (2006) [36]	iSpy (2008) [68]	Zheng *et al.* (2007) [70]	HEAP (2016) [57]	Argus (2012) [60]	Hu *et al.* (2007) [32]
Sub	U	*	✓	×	×	×	×	×	×	×
Sub	0/1	BH	✓	×	✓	×	×	✓	✓	✓
Sub	0/1	IM	✓	×	✓	×	×	✓	×	✓
Sub	0/1	MM	✓	×	✓	×	×	×	×	×
Sub	≥ 2	BH	✓	×	×	×	×	✓	✓	✓
Sub	≥ 2	IM	✓	×	×	×	×	✓	×	✓
Sub	≥ 2	MM	✓	×	×	×	×	×	×	×
Exact	0/1	BH	✓	✓	✓	✓	×	×	✓	✓
Exact	0/1	IM	✓	✓	✓	×	✓	×	×	✓
Exact	0/1	MM	✓	✓	✓	×	✓	×	×	×
Exact	≥ 2	BH	✓	×	×	✓	×	×	✓	✓
Exact	≥ 2	IM	✓	×	×	×	✓	×	×	✓
Exact	≥ 2	MM	✓	×	×	×	✓	×	×	×

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: *accurate* 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/day for $> 80\%$ of ASes	None	Past Data vs BGP updates (bidirectional link)	Pfx.+ Past AS links	Sec. 5.4 *Stage 1*
Exact	≥ 2	*	None for 89% of ASes ($T_{s2} = 5min$, $th_{s2} > 1$ monitors)	$< 4\%$	BGP updates (waiting interval, bidirectional link)	Pfx.	Sec. 5.4 *Stage 2*

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: mitigation methods

- 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%

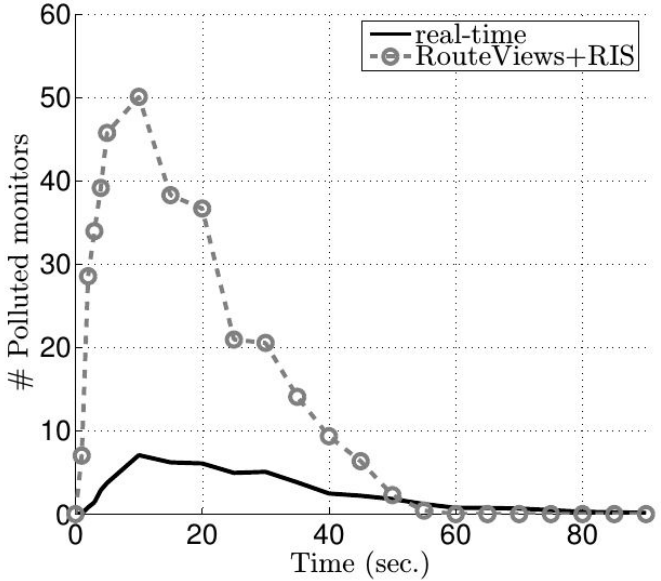
FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: automated & flexible mitigation

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

detection + mitigation:

NOW	ARTEMIS
hours/days →	**1 min.**



(b) # polluted monitors

The ARTEMIS tool: status

- Development funded by RIPE NCC Community Projects 2017
- Alpha version soon available
- Modules:
  - Minimal GUI (web application)
  - Configuration (list of prefixes, ASNs, rules, etc.)
  - Monitoring: log BGP updates for all owned (sub-)prefixes
  - Detection
    - Working
    - Under development
  - Mitigation
    - Under development: automated mitigation

Affected prefix	AS-PATH (Type)	Data plane	ARTEMIS
Sub	U	*	✓
Sub	0/1	BH	✓
Sub	0/1	IM	✓
Sub	0/1	MM	✓
Sub	≥ 2	BH	✓
Sub	≥ 2	IM	✓
Sub	≥ 2	MM	✓
Exact	0/1	BH	✓
Exact	0/1	IM	✓
Exact	0/1	MM	✓
Exact	≥ 2	BH	✓
Exact	≥ 2	IM	✓
Exact	≥ 2	MM	✓

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS configuration file

- Configure manually, react automatically
  - Define prefix, ASN, monitor groups
  - Declare ARTEMIS rules:

```
[group1]
prefixes:       my_prefixes
origin_asns:    my_asn, moas_asn
neighbors:      peer_65003,upstream_65002
mitigation:     manual
```

  - (Optionally) define mitigation parameters
- Future work: configuration automation
  - Extract from routers/RR
  - Extract from RADB/RIR

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
#                    ARTEMIS Config File                            #
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #


#   #   #   #   #   #   #   #   #   #   #   #   #   #   #   #   #
# - - - - - # Start of Prefix Definition Groups # - - - - - #

[prefixes_group]

my_prefixes: X.Y.Z.W/N, ...
...: ...

# - - - - - # End of Prefix Definition Groups # - - - - - - #
# - - - - - # Start of Monitor Definition Groups # - -- - - #

[monitors_group]

riperis: rrc15, ...
exabgp: (<IP1> : <PORT_1>), ...
bgpstreamhist: <path_to_dir_with_hist_csv_files>
bgpstreamlive: routeviews, ris
...: ...

# - - - - - # End of Monitor Definition Groups #  - - - - - #
# - - - - - # Start of ASN  Definition Groups # - - - - - - #

[asns_group]

my_asn: 65001
my_upstream_asn: 65002
moas_asn: 65005
moas_upstream_asn: 65003
...: ...

# - - - - - # End of Monitor Definition Groups #  - - - - - #
# - - - - - # Start of Rule Declaration Groups  # - - - - - #

[group1]
prefixes: my_prefixes
origin_asns: my_asn, moas_asn
neighbors: my_upstream_asn, moas_upstream_asn
mitigation: manual

# - - - - - # End of Rule Declaration Groups  # - - - - - - #
```

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS UI

Monitor Logs

↑ID	Prefix	Origin AS	Peer AS	AS Path	Service	Type	Timestamp	Hijack ID	Handled
107	139.91.0.0/16	8522	52888	52888 1916 27750 20965 5408 8522	RIPEris rrc15	A	5/7/18, 3:35 PM		Yes
106	139.91.0.0/16	8522	36236	36236 16397 26615 6762 2603 21320 5408 8522	bgpstream|routeviews|route-views4	A	5/7/18, 2:47 PM		Yes
105	139.91.0.0/16	8522	24482	24482 174 21320 21320 21320 21320 5408 8522	bgpstream|routeviews|route-views4	A	5/7/18, 2:47 PM		Yes
104	139.91.0.0/16	8522	24482	24482 174 21320 21320 21320 21320 5408 8522	bgpstream|routeviews|route-views.sg	A	5/7/18, 2:46 PM		Yes
103	139.91.0.0/16	8522	24482	24482 2603 21320 5408 8522	bgpstream|routeviews|route-views.sg	A	5/7/18, 2:46 PM		Yes

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS UI

DISCLAIMER: The data used on this slide for hijacks are fake/random and serve only to show how the tool looks.

Hijack Logs

↑ID	Type	Prefix	Hijack AS	CNum Peers Seen	CNum ASNs Infected	Time Started	Time Last Updated	Time Ended	Mit Pending	Mit Started	Mitigate	Resolved
6	1	139.91.250.0/24	56910	1	3	5/7/18, 2:33 PM	5/7/18, 2:33 PM	5/7/18, 5:26 PM	False	5/7/18, 5:26 PM	Mitigate	Resolved
5	1	139.91.250.0/24	56910	1	2	5/7/18, 2:20 PM	5/7/18, 2:20 PM		False		Mitigate	Resolved
4	1	139.91.250.0/24	56910	1	2	5/7/18, 2:00 PM	5/7/18, 2:00 PM		False		Mitigate	Resolved
3	1	139.91.250.0/24	56910	1	2	5/7/18, 2:00 PM	5/7/18, 2:00 PM		False		Mitigate	Resolved

FORTH INSTITUTE OF COMPUTER SCIENCE caida

What do we need from you?

- Feedback
  - E.g., try current test version at: http://inspire.edu.gr/artemis/demo/ (credentials: test / ripe76_artemis)
- Design requirements
- Advice on integrating ARTEMIS in operational environments
- Collaboration for testing ARTEMIS (e.g., configuration)
- Contact us at:
  - Come and talk to us during RIPE76 (*Vassilis, Pavlos, Lefteris, George, Fontas*)
  - Mail us at: *{vkotronis, sermpezis, leftman, gnomikos, fontas}@ics.forth.gr, {alberto, alistair}@caida.org*
  - Visit the ARTEMIS website http://www.inspire.edu.gr/artemis/

FORTH INSTITUTE OF COMPUTER SCIENCE caida

Thank you! Questions?

www.inspire.edu.gr/artemis

- ***Toy version for testing:*** *http://inspire.edu.gr/artemis/demo/* (creds: test/ripe76_artemis)
- ***ARTEMIS: Neutralizing BGP Hijacking within a Minute*** under revision in ACM/IEEE ToN, *https://arxiv.org/abs/1801.01085*
- ***A survey among Network Operators on BGP Prefix Hijacking*** in ACM SIGCOMM CCR, Jan'18, *https://arxiv.org/abs/1801.02918*

FORTH INSTITUTE OF COMPUTER SCIENCE

caida

INternet Security & Privacy Intelligence REsearch Group

funded by: NSF, U.S. DEPARTMENT OF HOMELAND SECURITY, RIPE NCC RIPE NETWORK COORDINATION CENTRE, erc European Research Council Established by the European Commission EU338402