# **ARTEMIS**: Neutralizing BGP Hijacking within a Minute

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

Vasileios Kotronis & Xenofontas Dimitropoulos

*RIPE76, Routing WG, Marseille, France, 17 May, 2018*

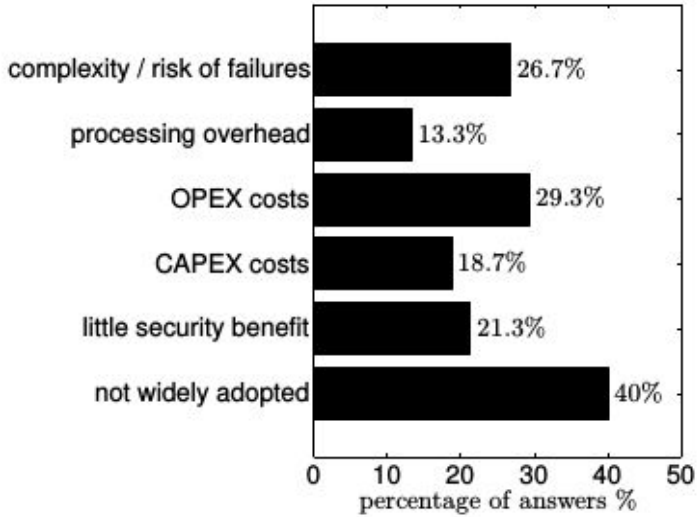
FORTH INSTITUTE OF COMPUTER SCIENCE

INternet Security & Privacy Intelligence REsearch Group

caida

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

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



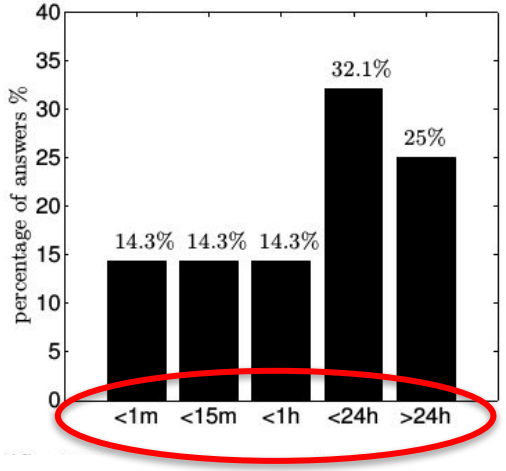

*Reasons for not using RPKI [2]*


[1] NIST. RPKI Monitor https://rpki-monitor.antd.nist.gov/. 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 hijacks today? → **3rd 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.

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

BGP STREAM

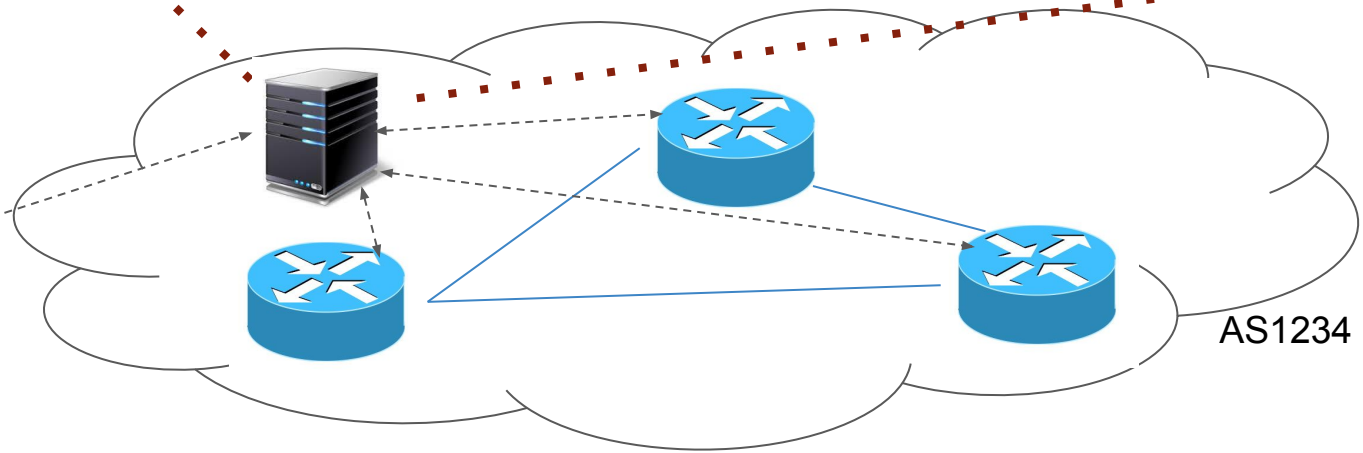
**BGP Monitors:**
- RIPE RIS
- BGPStream
  -- Live
  -- Historical
- Local (exaBGP)

Runs as a VM in the NOC or in the cloud

**ARTEMIS**

MONITORING → DETECTION → MITIGATION

**Operator Configuration File**

AS1234

FORTH INSTITUTE OF COMPUTER SCIENCE

caida

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

"2 monitors saw in last 5 minutes < 10.0.0.0/23, AS1, AS2, AS4, … >"

"Link AS2-AS4 not seen in last 10 months for any prefix, in any direction. Path manipulation sub-prefix HIJACK by AS4 against 10.0.0.0/23."

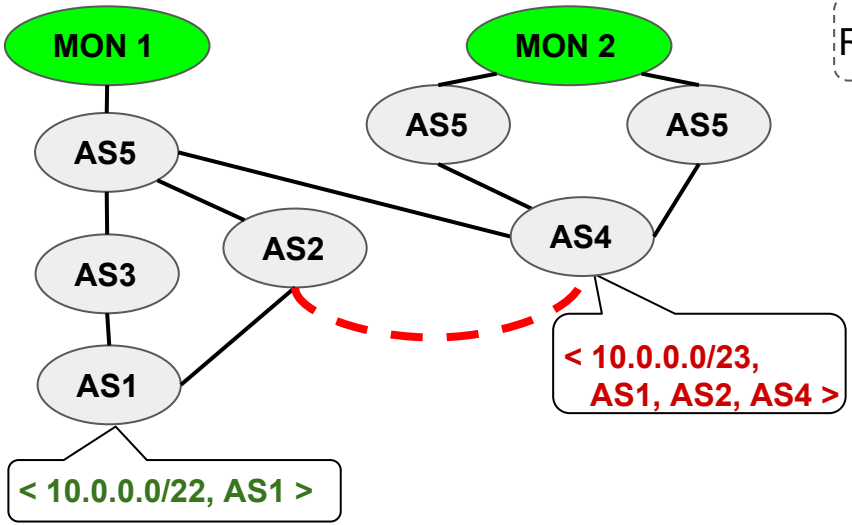
**ARTEMIS**

MONITORING → DETECTION → MITIGATION

React to hijack!

**Operator Configuration File**

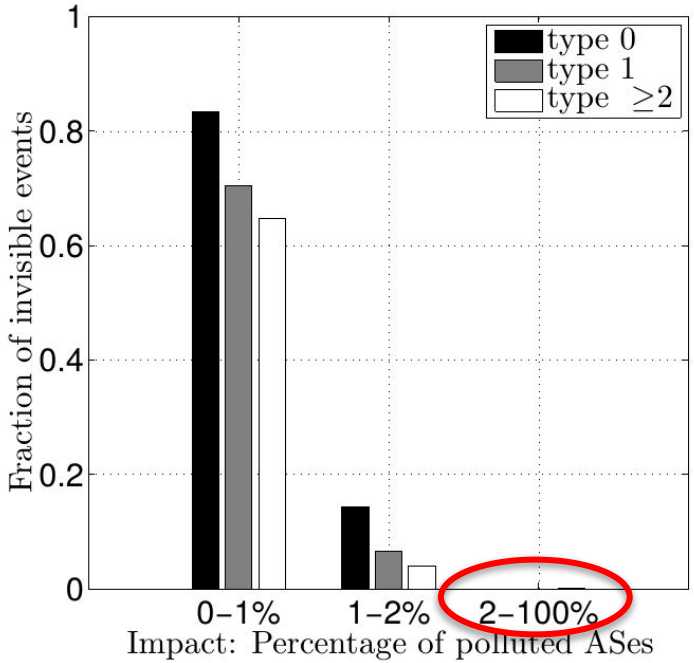
"I own 10.0.0.0/22 and announce it from AS1 with AS2 and AS3 as upstreams."

# ARTEMIS: Visibility of *all* impactful hijacks

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

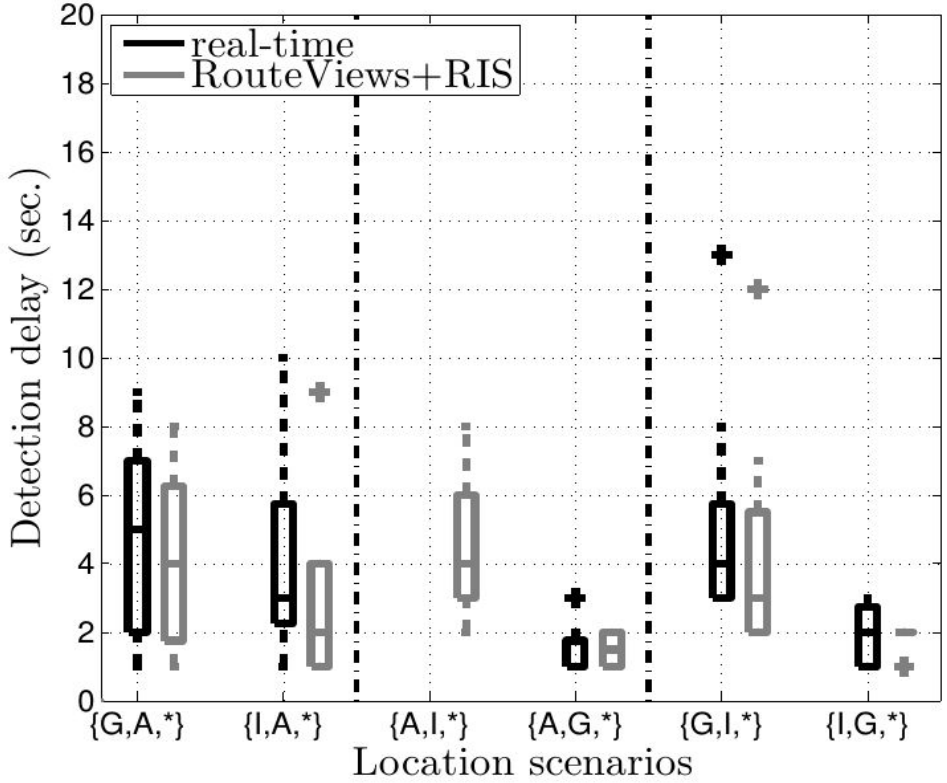
Simulation results on the AS-level graph [1]




[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.*!

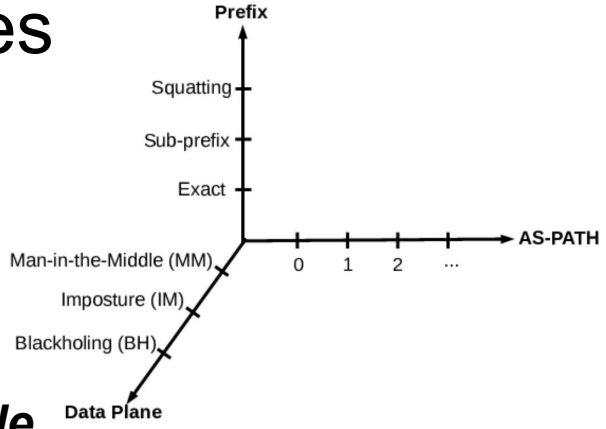
Real experiments in the Internet [1] (PEERING testbed)






[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

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 | $\geq 2$ | BH | ✓ | × | × | × | × | ✓ | ✓ | ✓ |
| Sub | $\geq 2$ | IM | ✓ | × | × | × | × | ✓ | × | ✓ |
| Sub | $\geq 2$ | MM | ✓ | × | × | × | × | × | × | × |
| Exact | 0/1 | BH | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ |
| Exact | 0/1 | IM | ✓ | ✓ | ✓ | × | ✓ | × | × | ✓ |
| Exact | 0/1 | MM | ✓ | ✓ | ✓ | × | ✓ | × | × | × |
| Exact | $\geq 2$ | BH | ✓ | × | × | ✓ | × | × | ✓ | ✓ |
| Exact | $\geq 2$ | IM | ✓ | × | × | × | ✓ | × | × | ✓ |
| Exact | $\geq 2$ | 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 | $\geq 2$ | * | $< 0.3$/day for $> 80\%$ of ASes | None | Past Data vs BGP updates (bidirectional link) | Pfx.+ Past AS links | Sec. 5.4 *Stage 1* |
| Exact | $\geq 2$ | * | 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% |

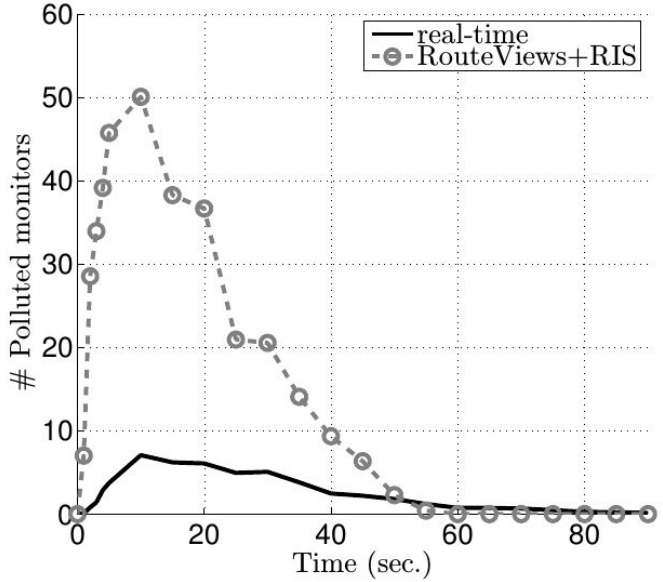
FORTH INSTITUTE OF COMPUTER SCIENCE caida

# 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:
  - 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 local routers
  - Extract from IRR (e.g., RADB, RPKI DBs)
  - Collect from RIPE RIS / RouteViews datasets

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
#                    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

# What do we need from you?

- Feedback
  - Answer our questionnaire at: https://goo.gl/forms/PETugofb2wspSPez2
  - Try current test version at: http://inspire.edu.gr/artemis/demo/
    (credentials: test / ripe76_artemis)
  - 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

- ***Questionnaire:*** *https://goo.gl/forms/PETugofb2wspSPez2*
- ***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:* RIPE NCC RIPE NETWORK COORDINATION CENTRE

erc European Research Council Established by the European Commission
EU338402

# BACKUP: 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