ARTEMIS: Neutralizing BGP Hijacking within a Minute

Pavlos Sermpezis
INSPIRE group (Prof. Xenofontas Dimitropoulos)
FORTH, Greece

ERC Networking Symposium, SIGCOMM 2018

The “ERC history” of ARTEMIS

- ERC NetVolution project
  - 2014 - 2019
  - Starting grant, Prof. Xenofontas Dimitropoulos (www.fontas.net)
  - Objective: innovation in the Internet routing system

- ERC (PoC) PHILOS project
  - 2019 - 2020
  - Proof of Concept (PoC) grant
  - Objective: prefix hijacking defense system, aka. ARTEMIS

The history of ARTEMIS

- [2016] BGP hackathon, CAIDA, UC San Diego
- [2016] Demo, SIGCOMM 2016
  - “ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking”.
- [2016 - 2018] … more research on ARTEMIS (by FORTH & CAIDA) …
  - Basic research + Survey among network operators
- [2018] ACM SIGCOMM CCR - Editorial
  - “A survey among Network Operators on BGP Prefix Hijacking”
- [2018] ACM/IEEE Transactions on Networking
  - “ARTEMIS: Neutralizing BGP Hijacking within a Minute”

[Award] RIPE NCC Community projects 2017

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

FORTH
INSTITUTE OF COMPUTER SCIENCE

The Internet today...

ANDY GREENBERG SECURITY 08.07.14 01:00 PM

HACKER REDIRECTS TRAFFIC FROM 19 INTERNET PROVIDERS TO STEAL BITCOINS

Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 10:20 PM

VANTAGEPOINT
IN: RESEARCH

Large BGP Leak by Google Disrupts Internet in Japan

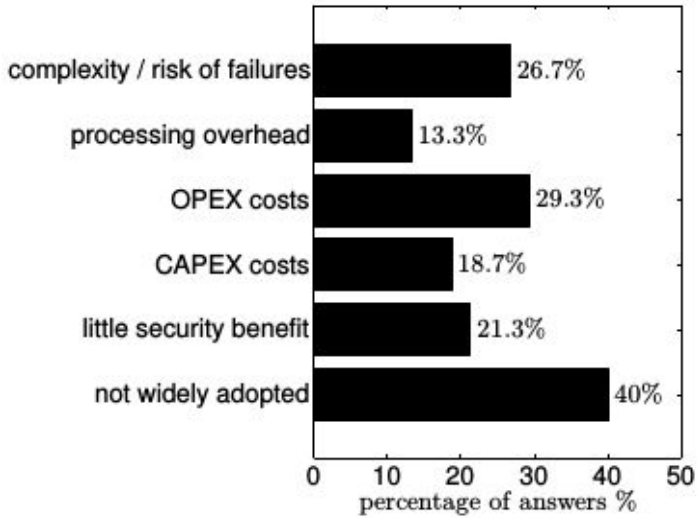
Research // Aug 28, 2017 // Doug Madory

BGP prefix hijacking

- Impact: **service outages** & **traffic interception**
  - Affect million of users
  - Last for hours
  - Can cost 100s of thousands of $$$ (or more) per minute

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

- X Only **8%** of prefixes covered by ROAs [1]
- X Why? → limited adoption & costs/complexity [2]



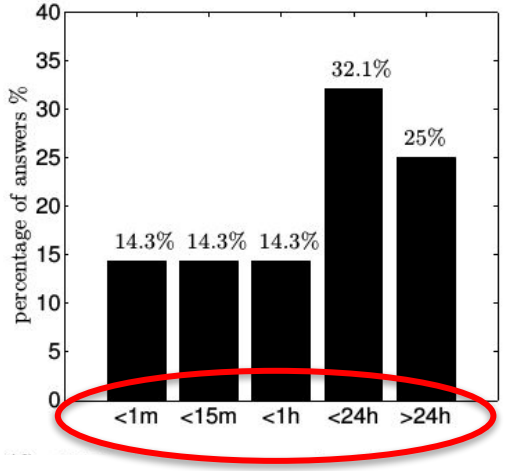
Reasons for not using RPKI [2]

[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 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

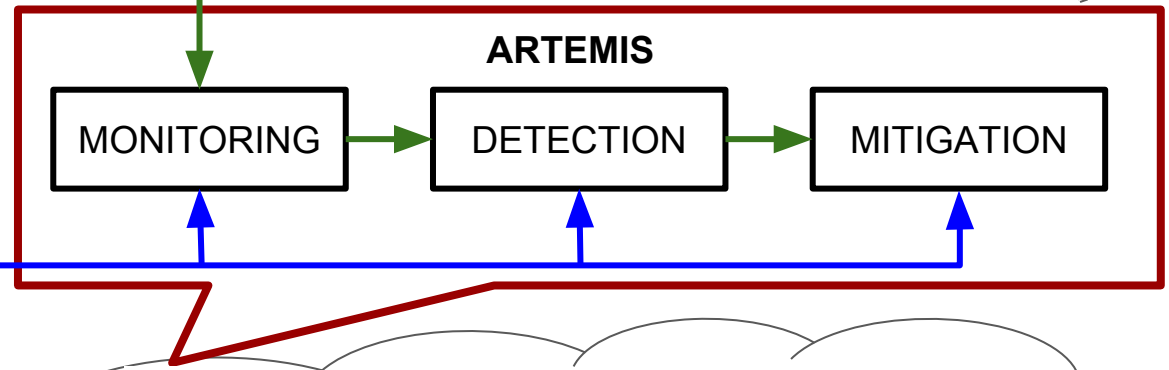
✓ **Comprehensive**: covers *all* hijack types
✓ **Accurate**: *0% FP*, *0% FN* for most hijack types;
low tunable FP-FN trade-off for remaining types
✓ **Fast**: neutralizes (detect & mitigate) attacks in < *1 minute*
✓ **Privacy preserving**: no sensitive info shared
✓ **Flexible**: configurable mitigation per-prefix + per-hijack type

FORTH
INSTITUTE OF COMPUTER SCIENCE

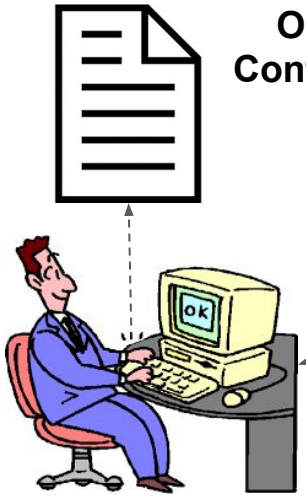
[1] ARTEMIS website www.inspire.edu.gr/artemis/
[2] P. Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute", to appear in ACM/IEEE ToN, arXiv 1801.01085.
[3] G. Chaviaras et al., "ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking", ACM SIGCOMM'16 demo.

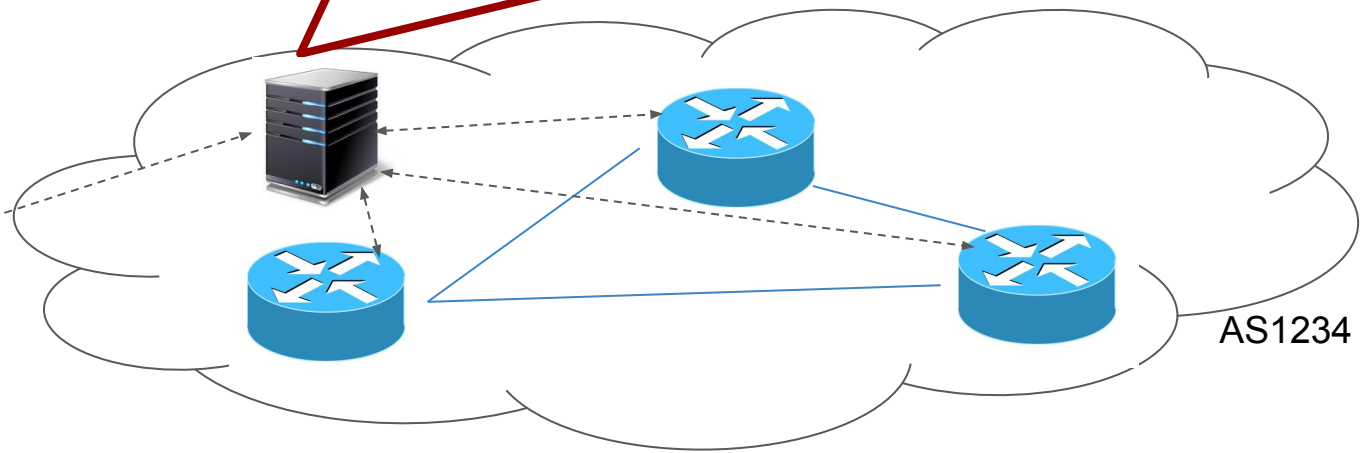
BGP Monitors:
- RIPE RIS
- RouteViews
- BGPStream
- Local (exaBGP)

Runs as a VM in the NOC or in the cloud



Operator Configuration File

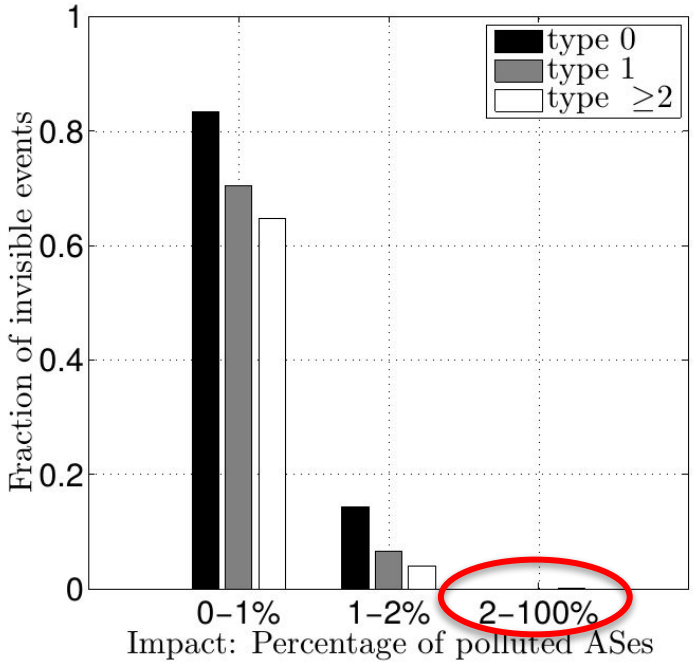




ARTEMIS: Visibility of *all* impactful hijacks

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

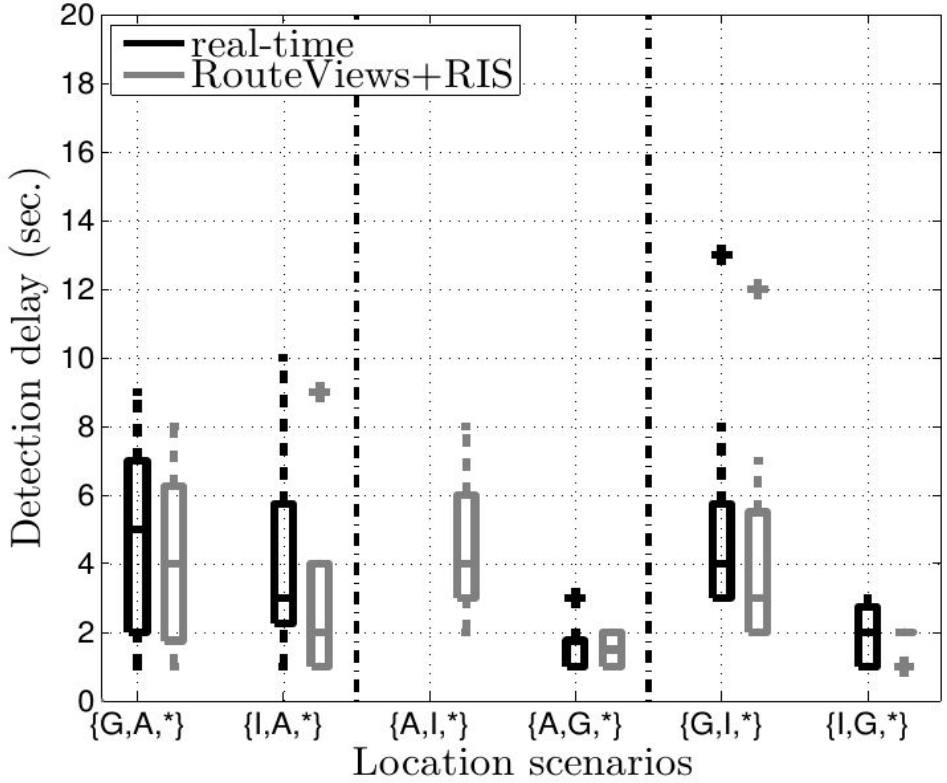
Simulation results on the AS-level graph [1]



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

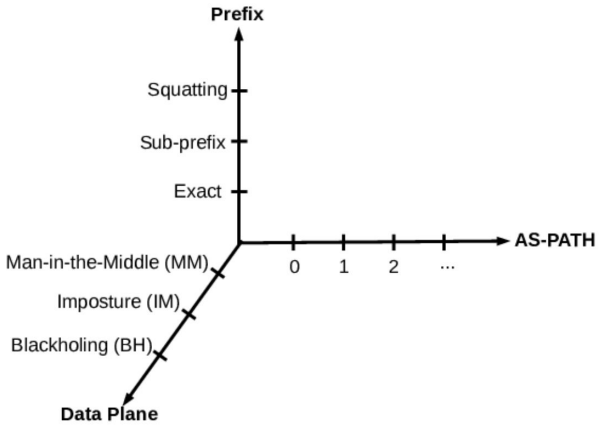
ARTEMIS: real-time monitoring, detection in *5 sec.*!

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



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

BGP prefix hijacking taxonomy



- Hijack types - 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>

ARTEMIS: detection of *all* hijack types (vs. literature)

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	✓	×	×	×	✓	×	×	×

Detection methodology details → in the paper [1]

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

ARTEMIS: *accurate* detection

Hijacking Attack			False Positives (FP)	False Negatives (FN)
Prefix	AS-PATH (Type)	Data Plane		
Sub-prefix	*	*	None	None
Squatting	*	*	None	None
Exact	0/1	*	None	None
Exact	≥ 2	*	< 0.3/day for $> 73\%$ of ASes	None
Exact	≥ 2	*	None for 63% of ASes ($T_{s2} = 5min$, $th_{s2} > 1$ monitors)	$< 4\%$

- With the ARTEMIS approach, detection becomes trivial for most attack types!
  - Zero FP and FN
- Hijack for exact prefix & fake link 2 hops or more from origin
  - Hard problem
  - ARTEMIS detection algorithm: past data + impact estimation
  - Low FPs & Zero FNs
  - … or (configurable) trade-off: even less FPs for a few (potential) FNs with low impact

FORTH INSTITUTE OF COMPUTER SCIENCE

ARTEMIS: mitigation methods

ARTEMIS proceeds automatically to mitigation:

- (Option 1) DIY: react by **de-aggregating** if you can
- (Option 2) **Get help** from other ASes
  - e.g., for /24 prefixes
  - *announcement (MOAS) and tunneling from helper AS(es)*

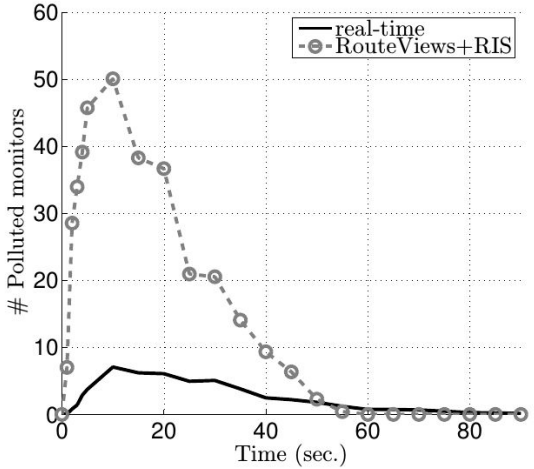
Percentage of polluted ASes when mitigation an exact-prefix hijack **without** or with outsourcing to **large ISPs** or **DoS mitigators**

	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

ARTEMIS: automated mitigation = fast mitigation

Real experiments in the Internet (PEERING testbed)



(b) # polluted monitors

detection + mitigation:

NOW hours/days → ARTEMIS **1 min.**

FORTH INSTITUTE OF COMPUTER SCIENCE

Summarizing ...

- ARTEMIS: a BGP prefix hijacking defense system
  - based on needs of operators (what and how)
  - no 3rd parties, fast, accurate, comprehensive, flexible, privacy preserving
- Neutralize BGP hijacking in 1 minute !
  - Current practices take hours (or even days)
- Ongoing work: Open-source ARTEMIS
  - Co-designed & tested with network operators

work by INSPIRE group (FORTH) & CAIDA :

Pavlos Sermpezis, Vasileios Kotronis, Alberto Dainotti, Alistair King,
Petros Gigis, Dimitris Mavrommatis, Xenofontas Dimitropoulos

www.inspire.edu.gr/artemis