ARTEMIS: Neutralizing BGP Hijacking within a Minute
(funded by RIPE Community Projects 2017)

Vasileios Kotronis & Xenofontas Dimitropoulos

RIPE76, Routing WG, Marseille, France, 17 May, 2018
How do people deal with hijacks 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]

---

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

- **Comprehensiveness**: detect only route leaks or 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.

![Graph showing the percentage of networks affected by hijacks](image)

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

---

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

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

Operator Configuration File

RUNS AS A VM IN THE NOC OR IN THE CLOUD
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."

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

React to hijack!

Operator Configuration File

MONITORING → DETECTION → MITIGATION

ARTEMIS

MON 1

AS5

AS3

AS1

< 10.0.0.0/22, AS1 >

MON 2

AS4

AS5

AS5

< 10.0.0.0/23, AS1, AS2, AS4 >
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]

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

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: \(<\text{my\_prefix, MY\_AS}>\)
  - Type-0 hijack: \(<\text{my\_prefix, BAD\_AS, …}>\)
  - Type-1 hijack: \(<\text{my\_prefix, MY\_AS, BAD\_AS, …}>\)
  - Type-2 hijack: \(<\text{my\_prefix, MY\_AS, MY\_PEER, BAD\_AS, …}>\)
  - …
  - Type-N hijack: \(<\text{my\_prefix, MY\_AS, …, BAD\_AS, …}>\)
  - Type-U hijack: \(<\text{my\_prefix, unaltered\_path}>\)
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.

<table>
<thead>
<tr>
<th>Class of Hijacking Attack</th>
<th>Control-plane System/Service</th>
<th>Data-plane System/Service</th>
<th>Hybrid System/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected prefix</td>
<td>AS-PATH (Type)</td>
<td>Data plane</td>
<td></td>
</tr>
<tr>
<td>Sub</td>
<td>U</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1 BH</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1 IM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1 MM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sub ≥ 2</td>
<td>BH</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sub ≥ 2</td>
<td>IM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sub ≥ 2</td>
<td>MM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1 BH</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1 IM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1 MM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact ≥ 2</td>
<td>BH</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact ≥ 2</td>
<td>IM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exact ≥ 2</td>
<td>MM</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
**ARTEMIS: accurate detection**

<table>
<thead>
<tr>
<th>Hijacking Attack</th>
<th>False Positives (FP)</th>
<th>False Negatives (FN)</th>
<th>Detection Rule</th>
<th>Needed Local Information</th>
<th>Detection Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub-prefix</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx.</td>
<td>Sec. 5.2</td>
</tr>
<tr>
<td>Squatting</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx.</td>
<td>Sec. 5.2</td>
</tr>
<tr>
<td>Exact 0/1</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx. + ASN (+ neighbor ASN)</td>
<td>Sec. 5.3</td>
</tr>
<tr>
<td>Exact ≥ 2</td>
<td>&lt; 0.3/day for &gt; 80% of ASes</td>
<td>None</td>
<td>Past Data vs BGP updates (bidirectional link)</td>
<td>Pfx. + Past AS links</td>
<td>Sec. 5.4 Stage 1</td>
</tr>
<tr>
<td>Exact ≥ 2</td>
<td>None for 89% of ASes ($T_{s2} = 5min, ; th_{s2} &gt; 1$ monitors)</td>
<td>&lt; 4%</td>
<td>BGP updates (waiting interval, bidirectional link)</td>
<td>Pfx.</td>
<td>Sec. 5.4 Stage 2</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Type</th>
<th>without outsourcing</th>
<th>top ISPs</th>
<th>AK</th>
<th>CF</th>
<th>VE</th>
<th>IN</th>
<th>NE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type0</td>
<td>50.0%</td>
<td>12.4%</td>
<td>2.4%</td>
<td>4.8%</td>
<td>5.0%</td>
<td>7.3%</td>
<td>11.0%</td>
</tr>
<tr>
<td>Type1</td>
<td>28.6%</td>
<td>8.2%</td>
<td>0.3%</td>
<td>0.8%</td>
<td>0.9%</td>
<td>2.3%</td>
<td>3.3%</td>
</tr>
<tr>
<td>Type2</td>
<td>16.9%</td>
<td>6.2%</td>
<td>0.2%</td>
<td>0.4%</td>
<td>0.4%</td>
<td>1.3%</td>
<td>1.1%</td>
</tr>
<tr>
<td>Type3</td>
<td>11.6%</td>
<td>4.5%</td>
<td>0.1%</td>
<td>0.4%</td>
<td>0.3%</td>
<td>1.1%</td>
<td>0.5%</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Affected prefix</th>
<th>AS-PATH (Type)</th>
<th>Data plane</th>
<th>ARTEMIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub</td>
<td>0</td>
<td>*</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1</td>
<td>BH</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1</td>
<td>IM</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>0/1</td>
<td>MM</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>≥ 2</td>
<td>BH</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>≥ 2</td>
<td>IM</td>
<td>✓</td>
</tr>
<tr>
<td>Sub</td>
<td>≥ 2</td>
<td>MM</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1</td>
<td>BH</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1</td>
<td>IM</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1</td>
<td>MM</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>≥ 2</td>
<td>BH</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>≥ 2</td>
<td>IM</td>
<td>✓</td>
</tr>
<tr>
<td>Exact</td>
<td>≥ 2</td>
<td>MM</td>
<td>✓</td>
</tr>
</tbody>
</table>
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
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/
Thank you! Questions?

www.inspire.edu.gr/artemis

- **Questionnaire**: [https://goo.gl/forms/PETugofb2wspSPez2](https://goo.gl/forms/PETugofb2wspSPez2)
- **ARTEMIS: Neutralizing BGP Hijacking within a Minute** under revision in ACM/IEEE ToN, [https://arxiv.org/abs/1801.01085](https://arxiv.org/abs/1801.01085)

funded by:
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Prefix</th>
<th>Hijack AS</th>
<th>CNum Peers Seen</th>
<th>CNum ASNs Infected</th>
<th>Time Started</th>
<th>Time Last Updated</th>
<th>Time Ended</th>
<th>Mit Pending</th>
<th>Mit Started</th>
<th>Mitigate</th>
<th>Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>139.91.250.0/24</td>
<td>56910</td>
<td>1</td>
<td>3</td>
<td>5/7/18, 2:33 PM</td>
<td>5/7/18, 2:33 PM</td>
<td>5/7/18, 5:26 PM</td>
<td>False</td>
<td>5/7/18, 5:26 PM</td>
<td>Mitigate</td>
<td>Resolved</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>139.91.250.0/24</td>
<td>56910</td>
<td>1</td>
<td>2</td>
<td>5/7/18, 2:20 PM</td>
<td>5/7/18, 2:20 PM</td>
<td>False</td>
<td>Mitigate</td>
<td>Resolved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>139.91.250.0/24</td>
<td>56910</td>
<td>1</td>
<td>2</td>
<td>5/7/18, 2:00 PM</td>
<td>5/7/18, 2:00 PM</td>
<td>False</td>
<td>Mitigate</td>
<td>Resolved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>139.91.250.0/24</td>
<td>56910</td>
<td>1</td>
<td>2</td>
<td>5/7/18, 2:00 PM</td>
<td>5/7/18, 2:00 PM</td>
<td>False</td>
<td>Mitigate</td>
<td>Resolved</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>