Neutralizing BGP Hijacking with the ARTEMIS Open-source Tool

Alberto Dainotti
alberto@caida.org
Center for Applied Internet Data Analysis
University of California, San Diego

Joint work with:
Vasileios Kotronis, Dimitris Mavrommatis
Petros Gigis, Pavlos Sermpezis, Xenofontas Dimitropoulos, Alistair King, Mingwei Zhang
BGP HIJACKING

stealing/manipulating your routes
BGP HIJACKING

stealing/manipulating your routes

Polluted AS
(remote users)

BAD_AS

simple hijack

oAS
(your network)
BGP HIJACKING

stealing/manipulating your routes

BAD_AS

man-in-the-middle (MITM) hijack

oAS
(your network)

Polluted AS
(remote users)
SOLUTIONS IN USE (1/2)

Proactive: RPKI

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

SOLUTIONS IN USE (2/2)

Reactive: 3rd Party Services

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

DETECTION BY 3RD PARTIES

3rd Party Detection

Polluted AS (remote users)

BAD_AS

Simple hijack

oAS (your network)
ARTEMIS APPROACH

self-managed detection & mitigation

Polluted AS
(your network)

simple hijack

BAD_AS

oAS
(remote users)
A PARADIGM SHIFT
From 3rd party monitoring to Self-Operated

3rd Party

- **Evasion**
  - Detect only simple attacks

- **Accuracy**
  - Potential for lots of FPs
  - or alternatively lots of FNs

- **Speed**
  - Manual verification & then manual mitigation

- **Privacy**
  - Need to share private information

ARTEMIS

- **Evasion**
  - Covers all attack configurations

- **Accuracy**
  - 0% FP, 0% FN: for most attacks
  - 0% FN for the remaining ones (or manage FP-FN trade-off)

- **Speed**
  - Automated mitigation: neutralize attacks in a minute

- **Privacy & Flexibility**
  - full privacy

*Sermpezis et al., “ARTEMIS: Neutralizing BGP Hijacking within a Minute“*  
*IEEE/ACM Transactions on Networking 2018*
ARTEMIS

self-managed detection & mitigation

https://github.com/FORTH-ICS-INSPIRE/artemis
TEST DEPLOYMENT

https://github.com/FORTH-ICS-INSPIRE/artemis

Center for Applied Internet Data Analysis
University of California San Diego

Foundation for Research and Technology-Hellas
University of Crete,

NSF OAC-1848641 — Sep 2018 - Aug 2019
Experimental Deployment of the ARTEMIS
BGP Hijacking Detection Prototype in Research and Educational Networks
## Hijacks

**ARTEMIS DEMO**

http://www.inspire.edu.gr/artemis/demo/

username: “guest” — password: "guest@artemis2018"

<table>
<thead>
<tr>
<th>Time Detected</th>
<th>Status</th>
<th>Prefix</th>
<th>Type</th>
<th>Hijack AS</th>
<th># Peers Seen</th>
<th># ASes Infected</th>
<th>Seen</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-12-13 07:19:01</td>
<td>Ignored</td>
<td>139.91.0.0/16</td>
<td>1</td>
<td>1299</td>
<td>1</td>
<td>1</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-13 02:26:22</td>
<td>Ignored</td>
<td>139.91.0.0/24</td>
<td>S</td>
<td>Unknown</td>
<td>1</td>
<td>5</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-12 23:38:27</td>
<td>Resolved, Outdated</td>
<td>139.91.250.0/24</td>
<td>Q</td>
<td>8522</td>
<td>1</td>
<td>4</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-12 23:36:25</td>
<td>Resolved</td>
<td>139.91.250.0/24</td>
<td>S</td>
<td>56910</td>
<td>1</td>
<td>4</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-12 23:32:27</td>
<td>Resolved, Outdated</td>
<td>139.91.0.0/16</td>
<td>1</td>
<td>5408</td>
<td>1</td>
<td>3</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-12 23:28:18</td>
<td>Resolved, Outdated</td>
<td>139.91.250.0/24</td>
<td>0</td>
<td>8522</td>
<td>5</td>
<td>10</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>2018-12-12 23:28:18</td>
<td>Resolved, Outdated</td>
<td>139.91.0.0/16</td>
<td>0</td>
<td>8522</td>
<td>4</td>
<td>9</td>
<td></td>
<td>View</td>
</tr>
</tbody>
</table>

Showing 1 to 7 of 7 entries

*Ongoing / Resolved / Ignored / Under Mitigation / Withdrawn / Outdated*
THANKS

alberto@caida.org