ARTEMIS: Neutralizing BGP Hijacking within a Minute
(funded by RIPE NCC 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 Comments

Earlier today several people noticed network reachability problems on Twitter, Google and others. The root cause turned out to be another BGP mishap.
Hijacks: Malicious Attacks

“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
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]

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

How do people deal with this today? → **Third 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.

---

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

MONITORING → DETECTION → MITIGATION

AS1234
"I own 10.0.0.0/22 and announce it from AS1 and AS2; both have AS3 as upstream."

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."

React to hijack!
BGP Monitors:
- RIPE RIS
- BGPStream
  -- Live
  -- Historical
- Local (exaBGP)

Operator Configuration File

“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.”

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

React to hijack!
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]

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

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: <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

- 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>
<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><strong>Affected prefix</strong></td>
<td><strong>AS-PATH</strong></td>
<td><strong>Data plane</strong></td>
<td><strong>ARTEMIS</strong></td>
</tr>
<tr>
<td><strong>prefix</strong></td>
<td><strong>(Type)</strong></td>
<td></td>
<td><strong>Cyclops</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>PHAS</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>iSpy</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Zheng et al.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>HEAP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Argus</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Hu et al.</strong></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>ARTEMIS Detection</th>
<th>Needed Local Information</th>
<th>Detection Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-prefix</td>
<td>*</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx.</td>
</tr>
<tr>
<td>Squatting</td>
<td>*</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx.</td>
</tr>
<tr>
<td>Exact</td>
<td>0/1</td>
<td>None</td>
<td>None</td>
<td>Config. vs BGP updates</td>
<td>Pfx. + ASN (+ neighbor ASN)</td>
</tr>
<tr>
<td>Exact</td>
<td>≥ 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>
</tr>
<tr>
<td>Exact</td>
<td>≥ 2</td>
<td>None for 89% of ASes <em>(T_{s2} = 5min, th_{s2} &gt; 1 monitors)</em></td>
<td>&lt; 4%</td>
<td>BGP updates (waiting interval, bidirectional link)</td>
<td>Pfx.</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></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.
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
ARTEMIS configuration file

- Configure manually, react automatically
  - Define prefix, ASN, monitor groups
  - Declare ARTEMIS rules:
    - (Optionally) define mitigation parameters
- Future work: configuration automation
  - Extract from routers/RR
  - Extract from RADB/RIR
## ARTEMIS UI

### Monitor Logs

<table>
<thead>
<tr>
<th>ID</th>
<th>Prefix</th>
<th>Origin AS</th>
<th>Peer AS</th>
<th>AS Path</th>
<th>Service</th>
<th>Type</th>
<th>Timestamp</th>
<th>Hijack ID</th>
<th>Handled</th>
</tr>
</thead>
<tbody>
<tr>
<td>107</td>
<td>139.91.0.0</td>
<td>8522</td>
<td>52888</td>
<td>52888 1916 27750 20965 5408 8522</td>
<td>RIPErs rrc15</td>
<td>A</td>
<td>5/7/18, 3:35 PM</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>139.91.0.0</td>
<td>8522</td>
<td>36236</td>
<td>36236 16397 26615 6762 2603 21320 5408 8522</td>
<td>bgpstream</td>
<td>routeviews</td>
<td>route-views4</td>
<td>A</td>
<td>5/7/18, 2:47 PM</td>
</tr>
<tr>
<td>105</td>
<td>139.91.0.0</td>
<td>8522</td>
<td>24482</td>
<td>24482 174 21320 21320 21320 21320 5408 8522</td>
<td>bgpstream</td>
<td>routeviews</td>
<td>route-views4</td>
<td>A</td>
<td>5/7/18, 2:47 PM</td>
</tr>
<tr>
<td>104</td>
<td>139.91.0.0</td>
<td>8522</td>
<td>24482</td>
<td>24482 174 21320 21320 21320 21320 5408 8522</td>
<td>bgpstream</td>
<td>routeviews</td>
<td>route-views.sg</td>
<td>A</td>
<td>5/7/18, 2:46 PM</td>
</tr>
<tr>
<td>103</td>
<td>139.91.0.0</td>
<td>8522</td>
<td>24482</td>
<td>24482 2603 21320 5408 8522</td>
<td>bgpstream</td>
<td>routeviews</td>
<td>route-views.sg</td>
<td>A</td>
<td>5/7/18, 2:46 PM</td>
</tr>
</tbody>
</table>
### ARTEMIS UI

#### Hijack Logs

<table>
<thead>
<tr>
<th>tID</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>
What do we need from you?

- Feedback
  - E.g., try current test version at: [http://inspire.edu.gr/artemis/demo/](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
Thank you! Questions?

www.inspire.edu.gr/artemis

- **Toy version for testing:**

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

- **A survey among Network Operators on BGP Prefix Hijacking**

---

**funded by:**

[NSF](https://www.nsf.gov)
[RIPE NCC](https://www.ripe.net)
[European Research Council](https://erc.europa.eu)