Detecting Internet Traffic Interception based on Route Hijacking

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

Joint work with:
Pavlos Sermpezis, Vasileios Kotronis,
Petros Gigis, Xenofontas Dimitropoulos,
Jae Hyun Park, Danilo Cicalese, Alistair King
INTERNET ROUTE HIJACKING
a threat to your organization and to critical infrastructure
INTERNET ROUTE HIJACKING

a threat to your organization and to critical infrastructure

man-in-the-middle (MITM) hijack

Foundation for Research and Technology-Hellas
University of Crete,

Center for Applied Internet Data Analysis
University of California San Diego
INTERNET ROUTE HIJACKING

many MITM events documented

Polluted AS (remote users)

BAD_AS

oAS (your network)

Nov. 2013

The attackers initiated the hijacks at least 38 times, grabbing traffic from about 1,500 individual IP blocks sometimes for minutes, other times for days — and at:

http://research.dyn.com/2013/11/mitm-internet-hijacking/
many MITM events documented

In few minutes, a single attack can manipulate millions of flows causing: service disruption, fraud, data theft, bad reputation, …
ATTACKS UNDER THE RADAR can have large impact

- Hijack Types:
  - **Type 0** hijack: `<prefix: BAD_AS, ...>` (a.k.a. “prefix origin hijack”)
  - **Type 1** hijack: `<prefix: oAS, BAD_AS, ...>`
  - **Type 2** hijack: `<prefix: oAS, ASI, BAD_AS, ...>`
  - ...

lots of attention
ATTACKS UNDER THE RADAR
can have large impact

• Hijack Types:
  • **Type 0** hijack: `<prefix: BAD_AS, ...>` (a.k.a. “prefix origin hijack”)
  • **Type 1** hijack: `<prefix: oAS, BAD_AS, ...>`
  • **Type 2** hijack: `<prefix: oAS, ASl, BAD_AS, ...>`
  • ...

![Graph showing CDF of hijack types](image)
STATE OF THE ART

False Positives + False Negatives

• **Third-party Detection Services**
  • False Positives
    • unless you promptly communicate changes to your network configuration
    • Privacy?
  • False Negatives
    • Most services focus on Type-0 attacks
    • Hard to detect more sophisticated attacks (*Type-1, Type-2, …*)
  • Mitigation?
    • No integration with mitigation solutions
    • Btw, would you mitigate if uncertain? how later?
NEED

EARLY & ACCURATE DETECTION

+ FAST MITIGATION
OUR APPROACH

**ARTEMIS (1/3)**

- **Realtime BGP Monitoring** using public infrastructure
  - ~200 vantage points worldwide (BGP routers)
    - source: RouteViews, RIPE RIS, Colorado State Univ. BGPMon
    - processing: CAIDA’s BGPStream

- **Provides visibility of all impactful events**

- **Detect events in few seconds!**
  (tested with experiments on the real Internet)

![Graph showing percentage of invisible events and impact on polluted ASes]
OUR APPROACH

ARTEMIS (2/3)

• Detection without outsourcing
  • Run locally: leverages knowledge of your network configuration
  • Accurate:
    • Detects all types of attacks!
    • No false negatives for all visible attacks
    • No false positives for most types of attacks;
      • demonstrated extremely low rate otherwise
  • No sharing of private data
  • Transparency: open source code

ARTEMIS: Neutralizing BGP Hijacking within a Minute

Pavlos Sermpezis¹, Vasileios Kotronis¹, Petros Gigis¹, Xenofontas Dimitropoulos¹,²,³
Jae Hyun Park³, Danilo Cicalèse²,³,⁴, Alistair King³, Alberto Dainotti³

¹FORTH  ²University of Crete  ³CAIDA, UC San Diego  ⁴Telecom ParisTech

ABSTRACT
BGP prefix hijacking is a threat to Internet operators and users. Several mechanisms or modifications to BGP that protect the Internet against it have been proposed. However, the reality is that most operators have not deployed them and are reluctant to do so in the near future. Instead, they rely on basic - and usually inefficient - proactive defenses to reduce the impact of hijacking events, or on inaccurate detection based on third party services and reactive approaches that might take up to several hours. In this paper, based on the analysis of the hijacking event a moment that triggered the launch of the Awa project, we present an approach that could react to hijacking events in less than a minute, achieving this by neutralizing BGP prefix hijacking.
OUR APPROACH

ARTEMIS (3/3)

• **Mitigation**
  • Automated + flexible (it can be configured on a per-prefix basis)
  • Both autonomous or outsourced
    • Prefix de-aggregation
    • Announcement and tunneling from other ASes
    • Contact offending AS and its neighbors

<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>

Table 3: Mean percentage of polluted ASes, when outsourcing BGP announcements to organizations providing DDoS protection services.
ARTEMIS CONFIGURATION

sample

• Configuration file
  • configure manually
  • extract from routers / route reflector
  • pre-populate from RADB?
  • ...

// Artemis configuration for our main prefixes
prefixes: 123.123.0.0/16, 111.111.111.0/24
  origin_asns: 4131, 4132
  neighbors: 4000, 3112, 2670, 45, 2800, 7462, 4123
  mitigation: deaggregate

// Artemis configuration for prefixes we use only at site #2
prefixes: 123.124.125.0/24, 222.222.222.0/24
  origin_asns: 4131
  neighbors: 2800, 7462, 4123
  mitigation: deaggregate, outsource
PILOT DEPLOYMENT

try ARTEMIS

- **Pilot** deployment of detection component
  - *all you need is a box with Python*
- Feedback
- Read our paper draft
- Contribute to the development of scripts etc.
THANKS

alberto@caida.org
ONE LAST SLIDE

- We are also developing a centralized service (an Internet observatory for BGP hijacks and anomalies) which does not need deployment in your network

- Soon you’ll be able to subscribe to receive notifications and inspect events on a dashboard

- If you upload your ARTEMIS configuration file it is going to be more accurate and may provide more information about the incident