HEAP BGP Observatory

Johannes Zirngibl, Patrick Sattler, Markus Sosnowski, Georg Carle

Acknowledgements: Johann Schlamp, Ralph Holz, Quentin Jacquemart, Ernst Biersack

Thursday 27th February, 2020

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich
Goal: Investigating BGP hijacking events

- Identify false positives based on three independent filters
- Active research since 2015
- Initial work:
  Heap: Reliable Assessment of BGP Hijacking Attacks
  by J. Schlamp, R. Holz, Q. Jacquemart, G. Carle, E. Biersack
  in IEEE JSAC, June 2016 [2]
Hijacking Event Analysis Program (HEAP)

HEAP Input

- Possible hijacks
- subMOAS from local BGP dumps and updates
- Published events from BGPMON

1 https://bgpstream.com/
Hijacking Event Analysis Program (HEAP)

**Registry Inference**
- Legitimizing relations between actors disprove an attack
- Based on Internet Routing Registries
- Historical data available

**Topology Analysis**
- An upstream provider should filter attacks
- Based on AS paths
- Extracted from local BGP dumps and collectors
Cryptographic Assurance
An attacker does not possess private keys and can not perform successful SSL/TLS handshakes with the according certificate.

- **Ground truth:**
  - Host behavior before a possible hijack
  - Regular updates
  - Good coverage, Internet-wide

- **Event scans**
  - Host behavior during a possible hijack
  - Fast reaction to events
Ground truth: Internet-wide Scans

- Regularly collects certificates from HTTPS capable IPv4 Hosts
  - Complete IPv4 ZMAP scan towards port 443
  - SSL/TLS connections to each host with an open port
- Results:
  - ~47 M hosts with open port 443
  - ~35 M successful SSL/TLS handshakes
  - Covering 3 M /24 networks
Alert Scans

- Establish SSL/TLS connections during an alert
- Scan alerts in seconds
  - Only consider hosts from ground truth
  - Small number of hosts
  - High scan rate
- Average daily events:
  - subMOAS: ~5000
  - BGPMON: ~5-10 → ~30% benign
**Prefix Top List**

**Ranking the Importance of Events**

**How can the importance and impact of a hijack be evaluated?**

- Rank events based on the hijacked prefix

  → **Prefix Top Lists** [https://prefixtoplists.net.in.tum.de/](https://prefixtoplists.net.in.tum.de/)

  - Provides a new top list type
  - Ranks prefixes and ASes as important Internet resources
  - Assigns weights based on domain based top lists
  - Prefix Top Lists: Gaining Insights with Prefixes from Domain-based Top Lists on DNS Deployment

<table>
<thead>
<tr>
<th>Rank</th>
<th>Prefix</th>
<th>Weight</th>
<th># Domains</th>
<th># IP addr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.217.18.0/24, AS15169 – GOOGLE</td>
<td>0.0178</td>
<td>1039</td>
<td>35</td>
</tr>
<tr>
<td>2</td>
<td>172.217.16.0/24, AS15169 – GOOGLE</td>
<td>0.0175</td>
<td>1000</td>
<td>33</td>
</tr>
<tr>
<td>3</td>
<td>172.217.22.0/24, AS15169 – GOOGLE</td>
<td>0.0173</td>
<td>1041</td>
<td>42</td>
</tr>
<tr>
<td>4</td>
<td>216.58.206.0/23, AS15169 – GOOGLE</td>
<td>0.0165</td>
<td>973</td>
<td>35</td>
</tr>
<tr>
<td>5</td>
<td>216.58.207.0/24, AS15169 – GOOGLE</td>
<td>0.0164</td>
<td>775</td>
<td>23</td>
</tr>
<tr>
<td>6</td>
<td>140.205.64.0/18, AS37963 – CNNIC-ALIBABA</td>
<td>0.0160</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>216.58.208.0/24, AS15169 – GOOGLE</td>
<td>0.0154</td>
<td>443</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>111.160.0.0/13, AS4837 – CHINA169-BACKBONE</td>
<td>0.0134</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

BGP Prefix Ranking for August 1, 2019 based on Alexa List.
Joint Platform
Enable Data Sharing and Joint Work

• Ongoing project to build a platform that enables to share **data and analysis tools**
• Provide VMs connected to a scientific data store
  • Allow collaboration on data
  • Easy reproduction of results
  • Work close to the data
• We share data from HEAP and other work through this platform
• If you are interested in access and collaborations contact us via
  → heap@net.in.tum.de
  → joint-platform@net.in.tum.de
• **We will be happy to collaborate!**
Prefix top lists: Gaining insights with prefixes from domain-based top lists on dns deployment.  

Heap: Reliable assessment of bgp hijacking attacks.  