VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes

Fabian Fischer\textsuperscript{1}, J. Fuchs\textsuperscript{1}, P.-A. Vervier\textsuperscript{2}, F. Mansmann\textsuperscript{1}, O. Thonnard\textsuperscript{3}

\textsuperscript{1} University of Konstanz, Germany
\textsuperscript{2} Institut Eurecom, France
\textsuperscript{3} Symantec Research Labs, France
Imagine YOU were a spammer...

and you want to send large amounts of spam.

Problem:
- Spam Filtering
- IP Reputation
- IP Blacklists

large amounts of spam messages

Spam E-Mails
Imagine YOU were a spammer...

and you want to send large amounts of spam.

YOU

Bot Network
to make use of
thousands of hosts

large amounts of spam messages

Spam E-Mails
Imagine YOU were a spammer...

and you want to send large amounts of spam.

But why not:
Steal someone's else IP space using BGP Hijacking?

**Border Gateway Protocol – BGP is insecure...**

BGP is responsible for routing in the Internet.

How can a particular IP prefix be reached?

VisTracer: Helps the analyst to explore malicious activities (e.g., Spam) with respect to routing changes based on traceroutes.
Data Collection of Spamtracer

- **Target Host**: IP address, domain name
- **SPAMTRACER**
  - IP traceroute
    - IP hops
    - hop count latency
  - IP-to-AS mapping
- **IP ADDRESS FEED**
- **IP/AS TRACEROUTE**
- **ROUTE ENRICHMENT**
  - IP Hops information
    - domain name, geolocation, OS
  - ASes information
    - owner, RIR, allocation date, geolocation
  - Target Network information
    - routing state, allocation status, blacklist hits

---

Visual Analytics Workflow – Overview

(i) Spamtracer Database → Routing Anomalies Extraction

(ii) Selection of Candidate Suspicious Cases
- ASN Overview

(iii) Investigation of Candidate Suspicious Cases
- Graph Visualization
  - Target History Visualization

(iv) User Feedback → Report of Investigation Result
Extraction of Routing Anomalies

- Extraction of *routing anomalies* based on known BGP hijack scenarios

- Prefix Ownership Conflict
- BGP AS Path Anomaly
- Traceroute Destination Anomaly
- Traceroute Path Anomaly
Defined Routing Anomalies

### Prefix Ownership Conflict

**Possible Reason:**
Advertising someone else's IP space

**Possibilities:**
- Same prefix (→ MOAS)
- Slightly different prefix (→ subMOAS)

### BGP AS Path Anomaly

**Possible Reason:**
Changed location in Internet topology

**Possibilities:**
- Different next hop AS
- Sequence change in complete AS path

### Traceroute Destination Anomaly

**Possible Reason:**
Suspicious values in trace metadata

**Possibilities:**
- Host/AS reachability changed
- Traceroute hop count changed

### Traceroute Path Anomaly

**Possible Reason:**
Significant change in the traceroute

**Possibilities:**
- AS sequence changed
- Country sequence changed
Used Glyph Representations

Design Decisions for Glyph Representations

- Using glyphs as compact representations for different visualization types.

Anomaly Glyph

Hop Glyph

Clock Glyph
Graphical User Interface of VisTracer
Pixel-Based ASN Overview Matrix
Identifying General Patterns and Combinations

AS 31733

Prefix Ownership Conflict
BGP AS Path Anomaly
Traceroute Destination Anomaly
Traceroute Path Anomaly
• Many diverse routing anomalies occurred within a limited period of time.
• Several anomalies occurred on the same day
Glyph-Based Target History Visualization

Compact Traceroute History

<table>
<thead>
<tr>
<th>Time</th>
<th>Tracehops (AS Level or IP Level)</th>
<th>Anomaly Patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-08-21</td>
<td>FR FR FR US EU US</td>
<td>RU</td>
</tr>
<tr>
<td>2011-08-22</td>
<td>FR FR FR US EU US</td>
<td>RU</td>
</tr>
<tr>
<td>2011-08-23</td>
<td>FR FR FR US EU US</td>
<td>RU</td>
</tr>
<tr>
<td>2011-08-24</td>
<td>FR FR                     US</td>
<td>RU</td>
</tr>
<tr>
<td>2011-08-29</td>
<td>FR FR                     EU</td>
<td>RU   RU</td>
</tr>
<tr>
<td>2011-09-01</td>
<td>FR FR                     EU</td>
<td>RU   RU</td>
</tr>
<tr>
<td>2011-09-04</td>
<td>FR FR                     EU</td>
<td>RU   RU</td>
</tr>
</tbody>
</table>
Graph-Based Visualization

Usage of Clock Glyph to encode temporal information

- Graph showing the sequence of traceroutes
- Nodes represent IPs / ASes / Countries
- Temporal information as Clock Glyph
- Different Layouts
Graph-Based Visualization
Usage of Clock Glyph to encode temporal information

close-up of an AS node, which was part of seven consecutive traceroutes
– with three traceroutes failing (gray segments)
Malicious BGP Hijack
Visual Exploration with VisTracer

- **Link Telecom BGP Hijack**
  - Spammer stole IP address space

- **The network administrator complained on 2011-08-20.**
  - Observed changes were the result of the owner regaining control over his network.
Map-Based Geographic Representation

Link Telecom BGP Hijack (April to August 2011)
Future Work

• Improve the usability of the expert tool.
• Integrate additional views, based on analysts' feedback.
• Layout improvements for the graph layout (reduce clutter).
• Alternative sorting algorithms for overview visualization.
Contributions

i. A visual analytics tool to analyze traceroutes.

ii. Integration into our large-scale automatic analysis system for traceroutes (*Spamtracer*).

iii. Pixel-, glyph- and graph-based visualizations for traceroutes.
Thank you very much for your attention!

Questions?

For more information about this work please contact

Fabian Fischer
Tel. +49 7531 88-2780
Fabian.Fischer@uni-konstanz.de

http://www.vis-sense.eu/

The research leading to these results has received funding from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257465.
Dataset 1: April until end of August 2011

• Collected Data:
  – 848,916 data plane routes collected
  – towards 239,907 IP addresses and 5,912 ASes

• After extracting routing anomalies:
  – 41,430 destination IP addresses
    • with at least one anomaly.