Real Time Analytics of DNS packets using Apache STORM

Lightning talk

Francisco Cifuentes
francisco@niclabs.cl
These are DSC presenters!
DSC: A DNS Statistics Collector

- DNS Server
- System with port mirroring
- PCAP
- DSC Collector
- Every 60s
- Cron Job
- XML File
- DSC Presenter
What’s Apache Storm!? 

“Apache Storm is a (...) distributed realtime computation system.”

https://storm.apache.org/
“Storm has many use cases: realtime analytics, online machine learning, continuous computation, distributed RPC, ETL, and more…”

https://storm.apache.org/
What it is used for!?

And many others...
“One example is security monitoring where we are leveraging Storm to analyze the network telemetry data of our globally distributed infrastructure in order to detect and mitigate cyber attacks”

http://storm.apache.org/documentation/Powered-By.html
Proposed Architecture

- DNS Server
- System with port mirroring
- Parser
- Queue Middleware

Flow:
- PCAP → Parser → JSON → Queue Middleware
Proposed Architecture

Apache Storm Framework

- QNAME Analysis
- Server location vs. Query source location
- DSC Collector*
Proposed Architecture

Apache Storm Framework
## Inspiration

<table>
<thead>
<tr>
<th>emojiTracker: Realtime Emoji Use on Twitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>682182002</td>
</tr>
<tr>
<td>190720616</td>
</tr>
<tr>
<td>84762525</td>
</tr>
<tr>
<td>58849703</td>
</tr>
<tr>
<td>51588095</td>
</tr>
<tr>
<td>41304209</td>
</tr>
<tr>
<td>31699021</td>
</tr>
<tr>
<td>24791764</td>
</tr>
<tr>
<td>21357601</td>
</tr>
<tr>
<td>18359688</td>
</tr>
<tr>
<td>14462397</td>
</tr>
<tr>
<td>11944513</td>
</tr>
<tr>
<td>10498875</td>
</tr>
<tr>
<td>9621791</td>
</tr>
<tr>
<td>8788692</td>
</tr>
<tr>
<td>7246275</td>
</tr>
<tr>
<td>6914490</td>
</tr>
<tr>
<td>6277043</td>
</tr>
</tbody>
</table>
Inspiration

Distance between client and server reached the threshold!
Some choices reasons

- Why do we need real time analysis?
- Why Apache Storm?
What has been done

- DNS Packet Parser.
- Tested different topologies.
Suggestions / Ideas accepted!

Francisco Cifuentes
francisco@niclabs.cl
http://ratadns.niclabs.cl