Request for Information Service (RFI) is an annual subscription-based service that extends and supports customer intelligence needs through Requests for Information. These RFI’s are completed by seasoned analysts and researchers with 5 – 10 years of experience in enterprise incident response, computer forensics, malware analysis, and other defensive operations. The service allows clients to make formal Requests for Information within the ThreatStream platform. RFI’s are based on customer need, but generally fall into three categories: triage, analysis, and custom work.

### Triage

Triage tasks are **completed in 24–48 hours** and involve preliminary analysis of topics like:

- Sources of credential exposure
- Context surrounding indicators of interest
- Intelligence analysis, actor, and campaign information
- Intelligence requests around news items
- Malware triage and basic details

**As an example:**

During the analysis of the data 3 different campaigns were observed. One is more active than others but overall each one of the campaigns provided a unique insight into the malware’s c2 communications. The table below illustrates the insights gathered for the different campaigns.

<table>
<thead>
<tr>
<th>Campaign_id</th>
<th>Track 1 data total</th>
<th>Track 2 data total</th>
<th>Campaign started</th>
<th>Campaign ended</th>
<th>Total Bot id’s</th>
<th>Total of victim ip’s</th>
<th>Terminal Names Associated</th>
</tr>
</thead>
<tbody>
<tr>
<td>grp03</td>
<td>0</td>
<td>0</td>
<td>2015-10-05</td>
<td>2015-12-09</td>
<td>5</td>
<td>60</td>
<td>kLnd2t5, ViGn</td>
</tr>
<tr>
<td>grp05</td>
<td>22,202</td>
<td>21,525</td>
<td>2015-08-09</td>
<td>2016-02-07</td>
<td>4</td>
<td>4</td>
<td>ALOHABoH, ALOHABoH2</td>
</tr>
<tr>
<td>grp10</td>
<td>13</td>
<td>12</td>
<td>2015-11-21</td>
<td>2016-02-10</td>
<td>8</td>
<td>62</td>
<td>WWINMICROs, QVVW, DPSServer, ViGn, 0ussx5i, 8YGard</td>
</tr>
</tbody>
</table>

### Analysis

Analysis tasks involve more in-depth investigations, generally requiring **a week or more** to complete. These tasks include the Triage tasks above, as well as:

- Threat Bulletins and associated intelligence concerning news items
- Details regarding campaigns, actors, incidents, indicators, signatures
- Malware analysis including functionality, End-point/SIEM queries, and signatures
Custom

Custom tasks are available based on customer need. Generally these require a greater degree of investigation than Triage or Analysis tasks.

As an Example, the below timeline was provided as part of a custom task:

<table>
<thead>
<tr>
<th>MD5</th>
<th>Associated Campaign</th>
<th>Compile_date</th>
<th>First VT submission</th>
<th>Last VT submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>90372a5e387e42c63b37d8845sabde0a</td>
<td>grp03</td>
<td>[Fri Jul 24 08:25:13 2015 UTC]</td>
<td>2015-11-28 02:17:58 UTC (2 months, 3 weeks ago)</td>
<td>2015-11-29 05:54:55 UTC (2 months, 2 weeks ago)</td>
</tr>
<tr>
<td>feacbbe3b63d95f2e3c9fd6d769635c30b</td>
<td>grp10</td>
<td>[Fri Jul 24 08:25:50 2015 UTC]</td>
<td>2015-11-06 13:11:20 UTC (3 months, 1 week ago)</td>
<td>2015-11-20 20:18:18 UTC (2 months, 4 weeks ago)</td>
</tr>
<tr>
<td>591e820591e10500fe939d6bd50e6776</td>
<td>grp05</td>
<td>[Fri Jul 24 08:25:13 2015 UTC]</td>
<td>2016-01-16 09:20:34 UTC (1 month ago)</td>
<td>2016-01-16 09:20:34 UTC (1 month ago)</td>
</tr>
</tbody>
</table>

Reports and Implementation

The results of these requests for information are curated into a formal report that is given to the client upon completion. The Professional Services team then works with the client to incorporate the research and gathered threat intelligence information into the ThreatStream platform. Clients are incentivized to share the results where practicable within the platform, which is reflected in the cost of each task or effort.

For additional information or to schedule a consultation please contact: cso-ps@anomali.com

Corporate Office: 808 Winslow Street, Redwood City, CA 94063