Signs of beaconing activity

Beaconing activity is when a compromised host ‘checks in’ with the command infrastructure, potentially waiting for new instructions or updates to the malicious software itself.

You might want to use Splunk for beacon detection to help with the following use cases:

- Monitoring a network for DNS exfiltration
- Detecting lateral movement with Active Directory data

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- DNS data

Example

You want to monitor your network to see whether any hosts are beaconing—or checking in with—malicious command and control infrastructure.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Stream DNS data. You can replace this source with any other DNS data used in your organization.

Run the following search:

```
eventtype="stream_dns" message_type="Query"
| fields _time, query
| streamstats current=f last(_time) AS last_time BY query
| eval gap=last_time - _time
| stats count avg(gap) AS AverageBeaconTime var(gap) AS VarianceBeaconTime BY query
| eval AverageBeaconTime=round(AverageBeaconTime,3), VarianceBeaconTime=round(VarianceBeaconTime,3)
| sort -count
| where VarianceBeaconTime < 60 AND count > 2 AND AverageBeaconTime>1.000
| table query VarianceBeaconTime  count AverageBeaconTime
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventtype=&quot;stream_dns&quot;</td>
<td>Search only Stream DNS events.</td>
</tr>
<tr>
<td>message_type=&quot;Query&quot;</td>
<td>Search for queries.</td>
</tr>
<tr>
<td></td>
<td>fields _time, query</td>
</tr>
<tr>
<td></td>
<td>streamstats current=f last(_time) AS last_time BY query</td>
</tr>
<tr>
<td></td>
<td>eval gap=last_time - _time</td>
</tr>
<tr>
<td></td>
<td>stats count avg(gap) AS AverageBeaconTime var(gap) AS VarianceBeaconTime BY query</td>
</tr>
<tr>
<td></td>
<td>eval AverageBeaconTime=round(AverageBeaconTime,3), VarianceBeaconTime=round(VarianceBeaconTime,3)</td>
</tr>
<tr>
<td></td>
<td>sort -count</td>
</tr>
<tr>
<td></td>
<td>where VarianceBeaconTime &lt; 60 AND count &gt; 2 AND AverageBeaconTime&gt;1.000</td>
</tr>
<tr>
<td>table query VarianceBeaconTime count AverageBeaconTime</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

**Result**

Low time variance in time in queries may indicate that hosts are contacting command and control infrastructure on a predetermined time slot. You might want to investigate activity on those hosts more closely. You can also add the src field to the | fields line of this search:

```
| fields _time, src, query
```

and a distinct count to the | stats line

```
| stats count dc(src) AS NumHosts avg(gap) AS AverageBeaconTime var(gap) AS VarianceBeaconTime BY query
```

to see the number of distinct hosts engaging in the same beaconing behavior.