Increases in DNS packet size and volume

You might want to review the size and number of DNS packets being transmitted over your network when doing the following:

- Monitoring a network for DNS exfiltration

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 for large DNS packets or an unusually high volume of DNS packets, both of which can be an early sign of data exfiltration.

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.

1. Run the following search:

```bash
eventtype="stream_dns" message_type="Query"
| mvexpand query
| eval queryLength=len(query)
| stats count BY queryLength, src
| sort -queryLength, count
| table src queryLength count
| head 1000
```

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>mvexpand query</td>
<td>Create a new event for each value found in the query field.</td>
</tr>
<tr>
<td>eval queryLength=len(query)</td>
<td>Calculate the length of the string in the query field.</td>
</tr>
<tr>
<td>stats count BY queryLength, src</td>
<td>Count the number of times each query length and source combination occurred.</td>
</tr>
<tr>
<td>sort -queryLength, count</td>
<td>Sort results with the largest requests first.</td>
</tr>
<tr>
<td>table src queryLength count</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
<tr>
<td>head 1000</td>
<td>Show only the first 1,000 records.</td>
</tr>
</tbody>
</table>

**Result**

Using the scatter chart visualization might help you see the outliers better. A high number of requests or large packets can indicate a security risk. For example, many common domains (www.google.com and www.bbc.co.uk) have a small query string length and will have a small query count. If, however, the malicious software opens a sensitive document that’s 5 Mb in size, chops it into 255-byte packets, and sends via DNS requests, then you’re likely to see many 255-byte packets.