First time seen JA3/JA3s hashes

You might need to identify the times that JA3 and JA3s hashes were first seen on your servers when doing the following:

- Detecting software supply chain attacks

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst, threat hunter
- Technologies: Splunk Cloud Platform or Splunk Enterprise
- Data: Deep packet inspection data

Example

You can run a search which uses JA3 and JA3s hashes to detect abnormal activity on critical servers which are often targeted in supply chain attacks. JA3 is an open-source methodology that allows for creating an MD5 hash of specific values found in the SSL/TLS handshake process, and JA3s is a similar methodology for calculating the JA3 hash of a server session.

This search is most effectively run in the following circumstances:

- with an allow list that limits the number of perceived false positives.
- against network connectivity that is not encrypted over SSL/TLS.
- with internal hosts or netblocks that have limited outbound connectivity as a client.
- in networks without SSL/TLS interceptions or inspection.

To optimize the search shown below, you should specify an index and a time range. In this example, Zeek is used to generate JA3 and JA3s data but you can use any other tool which can generate that data.

1. Run the following search:

```Splunk
sourcetype="bro:ssl:json" ja3="*" ja3s="*" src_ip IN (192.168.70.0/24)
| stats earliest(_time) AS earliest latest(_time) AS latest by ja3, ja3s, src_ip, server_name
| eval maxlatest=now()
| eval isOutlier=if(earliest >= relative_time(maxlatest, "-1d@d"), 1, 0)
| table ja3, ja3s, src_ip, server_name, earliest, latest, maxlatest, isOutlier
| convert ctime(earliest) ctime(latest) ctime(maxlatest)
```

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.
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><code>sourcetype=&quot;bro:ssl:json&quot; ja3=&quot;*&quot; ja3s=&quot;*&quot; src_ip IN (192.168.70.0/24)</code></td>
<td>Search Zeek data for JA3 and JA3s hashes within the critical server defined.</td>
</tr>
<tr>
<td>`</td>
<td>stats earliest(_time) AS earliest latest(_time) AS latest by ja3, ja3s, src_ip, server_name`</td>
</tr>
<tr>
<td>`</td>
<td>eval maxlatest=now()`</td>
</tr>
<tr>
<td>`</td>
<td>eval isOutlier=if(earliest &gt;= relative_time(maxlatest, &quot;-1d@d&quot;), 1, 0)`</td>
</tr>
<tr>
<td>`</td>
<td>table ja3, ja3s, src_ip, server_name, earliest, latest, maxlatest, isOutlier`</td>
</tr>
<tr>
<td>`</td>
<td>convert ctime(earliest) ctime(latest) ctime(maxlatest)`</td>
</tr>
<tr>
<td>`</td>
<td>sort earliest desc`</td>
</tr>
</tbody>
</table>

**Result**

This search will return the first seen JA3 and JA3s hashes. In the example below, you can see four TLS sessions which look suspicious for manic.imperial-stout.org and update.lunarstiiiness.com.
The results of this search are temporal, so the results can vary widely based on the timeframe specified. If the time window is too wide or narrow, potential malicious abnormal activity may be missed or blended with legitimate traffic. In many cases, a time window of 7 days can provide the best results for finding targeted malicious activity within the top 20 results.

You can improve the accuracy by adding an allow list of the most common JA3s hashes and/or server_name to remove known entities.