**JA3/JA3s hash overview**

You might need to search for an overview of JA3/JA3s hashes 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**

Before searching for abnormal activities using JA3 and JA3s hashes, you might want to identify all JA3/JA3s hashes in your data. 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:

```
 sourcetype="bro:ssl:json" ja3="*" ja3s="*" src_ip IN (192.168.70.0/24) 
| stats sparkline values(server_name) AS Domains, values(src_ip) AS Clients, values(dest_ip) AS Server count  BY ja3, ja3s 
| sort count desc
```
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>sourcetype=&quot;bro:ssl:json&quot; ja3=&quot;<em>&quot; ja3s=&quot;</em>&quot; src_ip IN (192.168.70.0/24)</td>
<td>Search Zeek data for JA3 and JA3s hashes within the critical server defined. This part of the search uses critical server netblock, 192.168.70.0/24. It's important that you adjust this part of the search to include your own critical servers.</td>
</tr>
<tr>
<td></td>
<td>Return the results in a table with a sparkline, with columns for Domains, Clients and Servers, grouped by JA3 and JA3s.</td>
</tr>
<tr>
<td></td>
<td>Sort the results in descending order.</td>
</tr>
</tbody>
</table>

Result

This search returns all JA3 and JA3s hashes. In the example below, you can see multiple domains and multiple IP addresses within one JA3s hash. This is useful as it allows you to minimize the amount of data that you have to analyze and maximize its value.