Windows process and JA3s hash correlation

You might need to identify the Windows processes communicating outbound and correlate them with their JA3/s 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:
  - Microsoft: Sysmon
  - Deep packet inspection data

Example

Network data combined with local process executions is a very valuable data source for threat hunters. If you are collecting Sysmon19 data within Splunk, you can identify the processes communicating outbound and correlate them with their JA3/s hashes. This allows you to correlate Windows processes with JA3/s hashes along with the server_name. 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 searches 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.
Option 1

1. Ensure that Sysmon is configured to collect network connection initiated (EventCode 3) events.
2. Run the following search:

   ```
   (source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3 src_ip IN (192.168.70.0/24))
   OR (sourcetype="bro:ssl:json" ja3= "ja3s=")
   | eval src_ip=if(sourcetype == "bro:ssl:json",'id.orig_h','src_ip')
   | eval src_port=if(sourcetype == "bro:ssl:json",'id.orig_p','src_port')
   | eval dest_ip=if(sourcetype == "bro:ssl:json",'id.resp_h','dest_ip')
   | eval dest_port=if(sourcetype == "bro:ssl:json",'id.resp_p','dest_port')
   | stats values(ja3) AS ja3 values(ja3s) AS ja3s values(process_path) AS process_path values(server_name) AS server_name BY src_ip dest_ip dest_port
   | search ja3= "ja3s= *, process_path= *, NOT process_path IN ("&lt;unknown process&gt;")
   ```

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>(source=&quot;XmlWinEventLog:Microsoft-Windows-Sysmon/Operational&quot; EventCode=3 src_ip IN (192.168.70.0/24)) OR (sourcetype=&quot;bro:ssl:json&quot; ja3= * ja3s= *)</td>
<td>Searches Sysmon operational logs for network connections initiated within the critical server defined, or search Zeek data for JA3 and JA3s hashes. 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>eval src_ip=if(sourcetype == &quot;bro:ssl:json&quot;,'id.orig_h','src_ip')</td>
<td>Sets the value for each field shown according to whether it was found in the Zeek data or Sysmon.</td>
</tr>
<tr>
<td>eval src_port=if(sourcetype == &quot;bro:ssl:json&quot;,'id.orig_p','src_port')</td>
<td></td>
</tr>
<tr>
<td>eval dest_ip=if(sourcetype == &quot;bro:ssl:json&quot;,'id.resp_h','dest_ip')</td>
<td>Produces a table with renamed fields as shown, grouped by src_ip, dest_ip, and dest_port.</td>
</tr>
<tr>
<td>eval dest_port=if(sourcetype == &quot;bro:ssl:json&quot;,'id.resp_p','dest_port')</td>
<td></td>
</tr>
<tr>
<td>stats values(ja3) AS ja3 values(ja3s) AS ja3s values(process_path) AS process_path values(server_name) AS server_name BY src_ip dest_ip dest_port</td>
<td></td>
</tr>
<tr>
<td>search ja3= * ja3s= *, process_path= *, NOT process_path IN (&quot;&lt;unknown process&gt;&quot;)</td>
<td>Matches Windows event processes with JA3 and JA3s</td>
</tr>
</tbody>
</table>
Option 2

This search provides identical results as the search above. However, this method, designed for use with the Network traffic data model, runs around 4 times faster. For information on installing and using the CIM, see the Common Information Model documentation.

| multisearch [ from datamodel:Network_Traffic.All_Traffic | search sourcetype="xmlwineventlog" source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" src_ip IN (192.168.70.0/24) | rename app AS process_path | search sourcetype="bro:ssl:json" ja3=* ja3s=*
| eval src_ip=if(sourcetype == "bro:ssl:json","id.orig_h","src_ip") | eval src_port=if(sourcetype == "bro:ssl:json","id.orig_p","src_port") | eval dest_ip=if(sourcetype == "bro:ssl:json","id.resp_h","dest_ip") | eval dest_port=if(sourcetype == "bro:ssl:json","id.resp_p","dest_port") | stats count values(ja3) AS ja3 values(ja3s) AS ja3s values(process_path) AS process_path, values(server_name) AS server_name BY src_ip dest_ip dest_port | search ja3=* ja3s=* process_path=* NOT process_path IN ("<unknown process>"

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>multisearch [ from datamodel:Network_Traffic.All_Traffic</td>
<td>Search the Network_Traffic.All_Traffic datamodel using Sysmon operational logs for network connections initiated within the critical server defined, or search Zeek data for JA3 and JA3s hashes.</td>
</tr>
<tr>
<td>search sourcetype=&quot;xmlwineventlog&quot; source=&quot;XmlWinEventLog:Microsoft-Windows-Sysmon/Operational&quot; src_ip IN (192.168.70.0/24)</td>
<td>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>[ rename app AS process_path</td>
<td></td>
</tr>
</tbody>
</table>
| ] [ search sourcetype="bro:ssl:json" ja3=* ja3s=*
| eval src_ip=if(sourcetype == "bro:ssl:json","id.orig_h","src_ip") | Sets the value for each field shown according to whether it was found in the Zeek data or Sysmon. |
| eval src_port=if(sourcetype == "bro:ssl:json","id.orig_p","src_port") | |
| eval dest_ip=if(sourcetype == "bro:ssl:json","id.resp_h","dest_ip") | |
| eval dest_port=if(sourcetype == "bro:ssl:json","id.resp_p","dest_port") | |
| stats count values(ja3) AS ja3 values(ja3s) AS ja3s values(process_path) AS process_path, values(server_name) AS server_name BY src_ip dest_ip dest_port | |
| search ja3=* ja3s=* process_path=* NOT process_path IN ("<unknown process>"|

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.
Splunk Search

"bro:ssl:json","id.resp_h","dest_ip"
| eval dest_port=if(sourcetype == "bro:ssl:json","id.resp_p","dest_port")

| stats count values(ja3) AS ja3 values(ja3s) AS ja3s values(process_path) AS process_path, values(server_name) AS server_name BY src_ip dest_ip dest_port

Produces a table with renamed fields as shown grouped, by src_ip, dest_ip, and dest_port.

| search ja3=* ja3s=* process_path=* NOT process_path IN (<unknown process>*)

Matches Windows event processes with JA3 and JA3s hashes.

Result

This search identifies processes communicating outbound and correlates them with their JA3/s hashes. In the example below, you can see powershell.exe making an outbound connection with what look like bad hosts.

![Table showing processes and connections](image)

Depending on the environment, these queries may only be useful for triaging potential malicious activity rather than identifying anomalous activity. You may want to use a different method to identify possible malicious abnormal activity, then triage the event using the JA3s with Sysmon query. However, because the server_name is also included where it is available, it may be helpful to identify abnormal or suspicious activity manually.