Suricata - Feature #2695
websocket support

11/21/2018 11:16 AM - Victor Julien

<table>
<thead>
<tr>
<th>Status:</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jason Ish</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

Description
At Suricon2018 support for WebSockets was requested.

Jason Ish, Danny Browning and Matt offered to work on this.

Rust would be preferred.

Related issues:
Related to Task #2685: SuriCon 2018 brainstorm
Related to Feature #3285: rules: XOR keyword

History

#1 - 11/21/2018 11:16 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#2 - 03/13/2019 07:56 PM - Bryant Smith
I have a Lua script I've developed to unmask websockets. I can add this to the git repo while a rust parser is being created.

#3 - 11/01/2019 09:30 AM - Jason Ish
- Related to Feature #3285: rules: XOR keyword added

#4 - 01/30/2020 01:45 PM - Victor Julien
- Label Protocol added

#5 - 03/14/2022 02:30 PM - Brandon Murphy
just wanted to bump this request WebSockets is still used by malware, recently case of it is documented here https://isc.sans.edu/forums/diary/Keep+an+Eye+on+WebSockets/28430/

#6 - 03/16/2022 09:39 PM - Brandon Murphy
just another bump - APT actor using websockets
https://cert.gov.ua/article/37704
Translated to English -- https://cert.gov.ua.translate.goog/article/37704?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

I was able to confirm this traffic using WebSockets - can share a pcap privately if needed, but looks like standard websockets use here.