Add option to re-initialise Lua output scripts

11/14/2016 01:05 PM - Chris Wakelin

<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>Community Ticket</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

Description

It would be useful to be able to re-initialise Lua output scripts without restarting Suricata; for example when adding known cryptographic keys to a malware traffic decoding script, or adding a new output.

It would also be nice to be able to cycle Lua output logs in the same way as the main ones.

History

#1 - 11/15/2016 06:46 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jason Ish
- Target version set to TBD

This could perhaps be done by honouring the rotation flag so that a HUP will reinit the script(s).

#2 - 03/08/2017 08:10 AM - Jason Ish
There are 2 things here, the first being able to reload the output scripts which fits better with SIGUSR2.

The log rotation could probably be done by registering a flag or something? The Lua script would be in charge of actually doing the rotation right? As it manages the file, but at least it could get notification that rotation was requested.

#3 - 03/12/2019 11:20 AM - Victor Julien
- Assignee changed from Jason Ish to Community Ticket
- Priority changed from Low to Normal
- Effort set to medium
- Difficulty set to medium

#4 - 09/27/2019 11:37 AM - Victor Julien
Agree with Jason. Not sure on what the mechanics should look like. The 'reinit' could simply call deinit followed by init. Or maybe a 'reinit' if it is present. The rotation should probably be separate function the script defined. Just 'rotate' probably?