Suricata - Optimization #3077

FTP parser command lookup
07/06/2019 02:30 PM - Jeff Lucovsky

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

Description
The FTP parser should use mpm when looking for commands instead of performing a linear search over the command coordinates with squashed case.

Related issues:
Related to Feature #2315: eve: ftp logging

History

#1 - 07/08/2019 09:12 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to Soon
- Effort deleted (low)

#2 - 07/17/2019 01:59 PM - Philippe Antoine
- Related to Feature #2315: eve: ftp logging added

#3 - 07/17/2019 03:10 PM - Jeff Lucovsky
Also, address this comment from the FTP logging PR https://github.com/OISF/suricata/pull/3967#discussion_r302236153

"Ok. but then could output-json-ftp.c call some new parsing function in app-layer-ftp.c ?
This way, we will defer parsing until needed and the parsing will be in app-*.c files"

#4 - 08/26/2019 08:59 PM - Jeff Lucovsky
- Status changed from Assigned to Closed

Merged in https://github.com/OISF/suricata/pull/4123

#5 - 08/27/2019 08:13 AM - Victor Julien
- Target version changed from Soon to 5.0rc1