Suricata - Feature #2409

Push signatures without reloading the entire set.

01/11/2018 11:38 AM - Mario Lefebvre

<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>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>high</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>high</td>
</tr>
</tbody>
</table>

Description

Good morning,

We discussed this yesterday at Flocon 2018 with Eric Leblond and Peter Manev.

We would like to see the Suricata engine to be able to load one or more new signatures without having to reload the entire set of signatures everytime via an API call. Reloading is heavy on the network to ship and non efficient. We want to keep the capability to reload the entire set as this can be convenient, but adding signatures as we produce them one at the time would better fit our inter-systems design. Also, some of our signatures are time sensitive and need to be pushed as fast as possible. Pushing a single signature should expedite the time of loading (reload time is currently 3 minutes for ~20000 sigs).

As a secondary requirement, it would be a bonus if new versions of a signature could be also managed the same way.

As a secondary requirement, it would be a bonus if deletion of signatures could be managed the same way. We have legal/policy constraints to remove some signatures depending of operations and would again prefer not have to reload the entire set as it is very heavy in our perspective.

Let me know if you need more details.

Related issues:

- Related to Task #2685: SuriCon 2018 brainstorm
- Related to Task #3288: Suricon 2019 brainstorm

Related to Task #2685: SuriCon 2018 brainstorm added

History

#1 - 01/20/2018 06:18 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 07/17/2018 10:06 AM - Victor Julien
- Effort set to high
- Difficulty set to high

#3 - 11/21/2018 11:01 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous

Due to the complexity of the detection engine, this is not easily possible. Perhaps it would be possible to do this for the simpler rule types, but it seems to be requested mostly for complex rule types. Assigning to 'community' as there are no plans to work on this.

#4 - 11/21/2018 11:01 AM - Victor Julien
- Related to Task #2685: SuriCon 2018 brainstorm added

#5 - 11/27/2018 10:30 AM - Kenneth Kolano
Note similar functionality would be useful when updating fileMD5 entries

#6 - 02/23/2019 10:04 PM - Andreas Herz
- Assignee set to Community Ticket

#7 - 11/01/2019 07:48 AM - Victor Julien
The datasets support allows live updates over unix-socket. So for the file md5 matching and the many other datasets usecases this is now supported. The rules stay static, but the datasets referenced by them are dynamic.

#8 - 11/01/2019 02:25 PM - Andreas Herz
- Status changed from New to Closed

#9 - 11/04/2019 11:53 AM - Victor Julien
We've closed this as we don't see this happen w/o massive redesigns of how the detection engine works. We think the datasets work will support a good deal of the possible use cases. For others, we'll have to fall back to regular rule reloads.

#10 - 11/04/2019 11:53 AM - Victor Julien
- Related to Task #3288: Suricon 2019 brainstorm added