Suricata - Feature #2987
Task # 4380 (Assigned): tracking: improvements to bits, ints, vars

Suggestions for new keywords (streambits)
05/20/2019 01:09 PM - Jungho Yoon

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</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>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Hi. I thought I needed a new keyword while analyzing the encryption stream.

I think new keywords can overcome the following issues:

1. Sometimes it is necessary to match dsize consecutively to identify the encryption stream.
   - Flowbits do not identify sequences, making continuous matches difficult and vulnerable to "TCP out of order".
2. It is impossible to precisely determine how far from sequence B is from sequence A.
   - stream_size can only check absolute position.

Example
In the figure(rdp_over_ssh.png), the consecutive matches of the red boxes are as follows.

AS-IS

```powershell
alert tcp-pkt $EXTERNAL_NET 22 -> $HOME_NET [1024:] (msg:"RDP over SSH (Reverse) pre0"; flow:to_cl
ient,established; dsize:100<>300; prefilter; flowbits:set,rostr0; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre1"; priority:4
; flow:to_server,established; flowbits:isset,rostr0; dsize:96; prefilter; flowbits:unset,rostr0; fl
owbits:set,rostr1; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre1"; priority:4
; flow:to_server,established; flowbits:isset,rostr0; dsize:96; prefilter; flowbits:unset,rostr0; fl
owbits:uniset,rostr1; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre2"; priority:4
; flow:to_server,established; flowbits:isset,rostr1; dsize:304; prefilter; flowbits:uniset,rostr1; fl
owbits:set,rostr2; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre2"; priority:4
; flow:to_server,established; flowbits:isset,rostr1; dsize:304; prefilter; flowbits:uniset,rostr1; fl
owbits:set,rostr2; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre2 flush"; flow :
to_server,established; flowbits:isset,rostr1; dsize:304; prefilter; flowbits:uniset,rostr1; noal
ert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre2 flush"; flow :
to_server,established; flowbits:isset,rostr1; dsize:304; prefilter; flowbits:uniset,rostr1; noal
ert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre3"; priority:4
; flow:to_server,established; flowbits:isset,rostr2; dsize:400; prefilter; flowbits:uniset,rostr2; fl
owbits:set,rostr3; noalert;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre3 flush"; flow :
to_server,established; flowbits:isset,rostr2; dsize:400; prefilter; flowbits:uniset,rostr2; noale
rt;)
alert tcp-pkt HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre3 flush"; flow :
to_server,established; flowbits:isset,rostr2; dsize:400; prefilter; flowbits:uniset,rostr2; noal
ert;)
```

07/15/2022
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre4"; priority:4; flow:to_server,established; flowbits:isset,rostr3; dsize:192; prefilter; flowbits:unset,rostr3; flowbits:set,rostr4; noalert;)
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre4 flush"; flow:to_server,established; flowbits:isset,rostr3; dsize:>192; prefilter; flowbits:unset,rostr3; noalert;)
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre4 flush"; flow:to_server,established; flowbits:isset,rostr3; dsize:0<>192; prefilter; flowbits:unset,rostr3; noalert;)

TO-BE New keywords can significantly reduce the number of rules:

alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre1"; flow:to_server,established; dsize:96; streambits:set, rdp_over_ssh1, client; noalert;)
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre2"; flow:to_server,established; dsize:304; streambits:isset, rdp_over_ssh1, client, <, 305; prefilter; streambits:set, rdp_over_ssh2, client; noalert;)
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre3"; flow:to_server,established; dsize:400; streambits:isset, rdp_over_ssh2, client, <, 401; prefilter; streambits:set, rdp_over_ssh3, client; noalert;)
alert tcp-pkt $HOME_NET [1024:] -> $EXTERNAL_NET 22 (msg:"RDP over SSH (Reverse) pre4"; flow:to_server,established; dsize:192; streambits:isset, rdp_over_ssh3, client, <, 193; prefilter;)

And it is possible to make a relative match from a certain point:

The details are shown in the figure(streambits_concept.png).

pkt N
- to_server
- pattern: jpg
- seq: 4100, ack:105, len:600
- streambits:set,foo

pkt N+1
- to_client
- seq:105, ack:4700, len:1100

pkt N+2
- to_client
- pattern: IHDR
- seq: 1205, ack:4700, len: 200
- streambits: isset, foo

pkt N+3
- to_server
- pattern: POST
- seq: 4700, ack:1405, len:300
- streambits: isset, foo

alert tcp-pkt any any -> any 80 (msg:"pkt N"; flow:to_server,established; content:"jpg"; streambits:set, foo, both;)
alert tcp-pkt any 80 -> any any (msg:"pkt N+2"; flow:to_client,established; content:"IHDR"; streambits:isset, foo, server, <, 1406;)
alert tcp-pkt any any -> any 80 (msg:"pkt N+3"; flow:to_server,established; content:"POST"; streambits:isset, foo, client, <, 301;)

streambits Format:

When streambits is set, it registers SEQ(+ LEN) and ACK information
"prefilter" logic such as flowbits(Feature #2486) / stream_size(Feature #2697) 
when "streambits: set" is set, can't not use "either" in format 
Supports both tcp-pkt and tcp-stream / For tcp-stream, it records the information of the last segm(right_edge)

streambits:<set|isset|unset|toggle>, name, <client|server|both|either>[, <modifier>, <number>];

modifier:

> greater than
< less than
Please consider the above.
Thank you.

History

#1 - 05/23/2019 08:52 PM - Andreas Herz
- Assignee set to Community Ticket
- Target version set to TBD
- Effort set to medium
- Difficulty set to medium

#2 - 03/06/2021 08:06 AM - Victor Julien
- Parent task set to #4380

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdp_over_ssh.png</td>
<td>64.9 KB</td>
<td>05/20/2019</td>
<td>Jungho Yoon</td>
</tr>
<tr>
<td>streambits_concept.png</td>
<td>27.9 KB</td>
<td>05/20/2019</td>
<td>Jungho Yoon</td>
</tr>
</tbody>
</table>