Suricata - Bug #2479

http_cookie negation fails if no cookie in traffic

04/05/2018 07:22 PM - Jason Williams

Status: New
Priority: Normal
Assignee: OISF Dev
Category: 
Target version: TBD
Affected Versions: 

Description

Given the below example rule where we are looking for a HTTP POST with a http_cookie negation:

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"COOKIE Y"; flow:to_server,established; content :":"POST"); http_method; content:"this_doesnt_exist_who_cares_it_should_still_fire"; http_cookie; classtype:trojan-activity; sid:102; rev:1;)

This will fire on this traffic which has a cookie in it...

POST /trach/00/00/980014/index/xb/OF.php HTTP/1.1
Accept-Encoding: identity
Content-Length: 59
Host: vitospetromata.gr
Connection: close
Referer: http://vitospetromata.gr/trach/00/00/980014/index/xb/OF.php
Cookie: _mcnc=1
Content-Type: application/x-www-form-urlencoded

...but will not fire on this traffic that does not have a cookie in it.

POST /index2.php HTTP/1.1
Accept-Encoding: identity
Content-Length: 143
Host: moifesgeucswaytvvxe.altervista.org
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:42.0) Gecko/20100101 Firefox/42.0
Connection: close
Referer: http://moifesgeucswaytvvxe.altervista.org/Update.html
Content-Type: application/x-www-form-urlencoded

It seems like this negation should work in both cases? Tested in 4.0.4, 4.0.1, and latest git.

Related issues:

Related to Bug #2224: Negated http_* match returns false if buffer not populated

History

#1 - 04/07/2018 10:08 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 06/06/2019 01:54 PM - Philippe Antoine
- Related to Bug #2224: Negated http_* match returns false if buffer not populated added

06/13/2020