Suricata - Bug #3505

Negations on contents within the http_cookie buffer causes FN if no http_cookie is present

02/26/2020 11:23 PM - Jason Williams

Status: Closed
Priority: Normal
Assignee:
Category:
Target version:
Affected Versions: 5.0.0
Effort:
Difficulty:
Label:

Description

For the below http request:

```
POST /wp-content/uploads/2020/02/phish/phish/process1.php HTTP/1.1
Accept-Encoding: identity
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Host: somewhere.com
Connection: close
username=someusername&password=somepassword&btnlogin/Login
```

and these corresponding rule contents:

```
content:"username="; nocase; depth:9; http_client_body; fast_pattern; content:"&pass"; nocase; http_client_body; distance:0;
content!:"_utma="; http_cookie;
```

In my testing in order to get this to fire in suri4 or 5 notation/engines, the only way to get this to hit would be to do a raw negation without using the http_cookie buffer

However, if we have a header like the below which contains a http_cookie buffer:

```
POST /wp-content/uploads/2020/02/phish/phish/process1.php HTTP/1.1
Accept-Encoding: identity
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Host: somewhere.com
Cookie: PHPSESSID=go4f6lb9g42pwljltqtvc0mgu3
Connection: close
username=someusername&password=somepassword&btnlogin/Login
```

The rule with `content!:"_utma="; http_cookie:_` will hit as expected

Related issues:

- Is duplicate of Bug #2479: http_cookie negation fails if no cookie in traffic

History

#1 - 03/11/2021 08:12 PM - Philippe Antoine
- Is duplicate of Bug #2479: http_cookie negation fails if no cookie in traffic added

#2 - 03/11/2021 08:12 PM - Philippe Antoine
- Status changed from New to Closed