Suricata - Feature #5190
new tls.random keyword
03/13/2022 03:58 PM - Brandon Murphy

Status: Closed
Priority: Normal
Assignee: Shivani Bhardwaj
Category:
Target version: 7.0rc1
Effort:
Difficulty:

Description
While updating some older TLS sigs in the ET Ruleset which do not make use of existing suricata buffers, I came across this a
signature which detects malware using a hard-coded TLS request, specifically leveraging the first four bytes of the client random
representing the GMT Unix Time.

Until this buffer is added, I am unable to fully convert the use to making use of buffers.

I see this is mentioned in https://redmine.openinfosecfoundation.org/issues/1766 and documented in
https://redmine.openinfosecfoundation.org/projects/suricata/wiki/TLS_keyword_expansion. However that issue is nondiscrete in it's

Related issues:
Related to Feature #1766: TLS keyword expansion

History
#1 - 06/10/2022 08:50 AM - Victor Julien
- Related to Feature #1766: TLS keyword expansion added

#2 - 06/10/2022 09:08 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Shivani Bhardwaj
- Target version changed from TBD to 7.0rc1

I think this comes down to adding a 4 byte array to the state, then filling that from TLSDecodeHSHelloRandom and registering a new sticky buffer
keyword to match on it.

#3 - 07/27/2022 07:08 AM - Shivani Bhardwaj
- Status changed from Assigned to In Review

Closed by https://github.com/OISF/suricata/pull/7787

#4 - 08/30/2022 11:14 AM - Shivani Bhardwaj
- Status changed from In Review to Closed