Suricata - Feature #4876
Additional FTP Buffers
12/06/2021 05:09 PM - Brandon Murphy

Status: New
Priority: Normal
Assignee:
Category:
Target version: 7.0rc1
Effort:
Difficulty:

Description
We continue to see popular commodity and APT based malware using FTP as an exfil protocol (https://attack.mitre.org/techniques/T1048/003/). There are currently very few FTP buffers and even signatures as simple as looking for specific usernames require unbuffered content matches, often times increasing the complexity of the rule and making it more prone to FN/FP.

I'd be open to provide feedback on buffers required, though I think a general purpose client -> server buffers of ftp.command, ftp.command_data and server -> client of ftp.completion_code and ftp.reply which match the current logging would be a good improvement.

As a side note - The current ftp-data example contained here https://suricata.readthedocs.io/en/latest/rules/ftp-keywords.html is a bit confusing as it makes use of the "filename:" and "password:" however, as I understand it, that option can be used in non filestore signatures.

Related issues:
Related to Feature #4906: ftp: add stream app-layer frame support

History
#1 - 02/22/2022 07:47 PM - Victor Julien
- Related to Feature #4906: ftp: add stream app-layer frame support added

#2 - 02/22/2022 07:48 PM - Victor Julien
- Target version set to 7.0rc1

This should come automatically when #4876 is done.