Suricata - Feature #2054
Extracting HTTPS URL’s from SMTP, currently only HTTP is supported
02/28/2017 06:29 AM - Per Le

Status: New
Priority: Normal
Assignee: Community Ticket
Category: TBD
Target version: TBD
Effort: medium
Difficulty: medium

Description
Hello :) We are looking for extracting HTTPS URL’s from SMTP. Currently, only HTTP is supported. Can you please add this?

Related issues:
Has duplicate Feature #2724: extract-urls in email mime decoder increasingly obsolete

Rejected

History
#1 - 05/03/2017 04:10 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#2 - 10/18/2017 03:06 PM - Drew G
Ideally, it would be great if this had some granularity that was configurable. Something like:

#Default (same result as current code)
extract-urls: yes
extract-urls-schemes: [http]
log-url-scheme: no

eve.json ->

....,"url": ["suricata-ids.org"],...

#Proposed Feature
extract-urls: yes
extract-urls-schemes: [http, https, ftp, mailto]
log-url-scheme: yes

eve.json ->


#3 - 10/19/2017 02:15 AM - Victor Julien
- Assignee changed from OISF Dev to Anonymous

I like the idea. Happy to take a pull request.

#4 - 07/13/2018 08:08 PM - Victor Julien
- Effort set to medium
- Difficulty set to medium

#5 - 12/07/2018 06:21 AM - Victor Julien
- Has duplicate Feature #2724: extract-urls in email mime decoder increasingly obsolete added
#6 - 02/23/2019 10:19 PM - Andreas Herz
- Assignee set to Community Ticket

#7 - 04/09/2020 07:12 PM - Aaron Bungay
Looking into this.