Suricata - Feature #629
Add User-Agent to filestore metadata
11/14/2012 01:20 PM - Ludovico Cavedon

Status: Closed
Priority: Normal
Assignee: Ludovico Cavedon
Category:
Target version: 1.4rc1
Effort:
Difficulty:
Label:

Here is a patch to add the content of the User-Agent header to the filestore metadata:
https://github.com/cavedon/suricata/commit/06a1e9fc9fbdd198558557d85f7390271398e95

It would be great if it could be merged into future versions of suricata.

History

#1 - 11/22/2012 09:51 AM - Victor Julien
Can you do a pull request on github for this?

Ideally we’d not loop the headers list for each of those log lines like we do now for LogFilestoreMetaGetHost and LogFilestoreMetaGetReferer.

#2 - 11/26/2012 12:58 PM - Ludovico Cavedon
Victor Julien wrote:

Can you do a pull request on github for this?

Done: https://github.com/inliniac/suricata/pull/226
It actually includes also the commit for #628 as the 2 commits were done on the same branch.

Ideally we'd not loop the headers list for each of those log lines like we do now for LogFilestoreMetaGetHost and LogFilestoreMetaGetReferer.

I see, are you saying that we should not loop for each one of them, but loop once and fetch the three of them?

Thanks

#3 - 11/27/2012 03:09 AM - Victor Julien
Ludovico Cavedon wrote:

Ideally we’d not loop the headers list for each of those log lines like we do now for LogFilestoreMetaGetHost and LogFilestoreMetaGetReferer.

I see, are you saying that we should not loop for each one of them, but loop once and fetch the three of them?

Right. Maybe output directly from the loop.

Although really, it would probably be better to not output while holding a flow lock, but that would involve buffering and in general more significant changes.

#4 - 11/28/2012 03:27 AM - Victor Julien
- Status changed from New to Closed
- Assignee set to Ludovico Cavedon
- Target version set to 1.4rc1
- % Done changed from 0 to 100
Merged the PR, thanks. We can do the optimization later. Feel free to take that task :)