Suricata - Feature #2675

Split out SMB parser to be reusable

11/12/2018 08:02 PM - Ed Page

Status: New
Priority: Normal
Assignee: Ed Page
Category:
Target version: TBD
Effort:
Difficulty:

Label:

Description
Suricata has a built-in SMB parser written in Rust, https://github.com/OISF/suricata/tree/master/rust/src/smb

Splitting this out into a dedicated crate can allow leverage/collaboration between Suricata and other projects.

History
#1 - 11/12/2018 08:36 PM - Ed Page
I've got a rough start on a repo for this, https://github.com/epage/smb-parser

This doesn't even build. I wanted to post it now to ensure I'm aligning with how all you'd want this done, like what repo is used, structure, etc.

#2 - 11/28/2018 07:41 AM - Victor Julien
Hi Ed, apologies for not responding earlier. Suricon + catchup afterwards took quite a bit of time & energy.

Some thoughts on how to do this:
- the crates should contain the lower level logic that is not Suricata specific. Pierre Chifflier has done a bunch that we use (der-parser, ntp-parser, etc).
- if we're moving this out, I think it needs to be to a repo we (OISF) control so that we will not depend on 3rd parties for fixing bugs and doing releases. Here not all protocols are equal, and smb is more important to the project than some of the other protocols
- for contributing to Suricata's code base we have a CLA, we need to think about whether that would apply to this logic as well (initial thought: yes).
- I understand your current branch is a test, but just to be sure I think the repo should only contain the parser, not other tooling. That seems more something for another repo & crate. Or perhaps it lib would be primary, and some tools would be secondary in a tools/ subdir or something.

#3 - 06/15/2019 09:51 PM - Andreas Herz
- Target version set to TBD