Suricata - Task #4146
Research: Hand off packet streams on alerts
11/14/2020 02:37 PM - Jeff Lucovsky

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

Description
Chris G Nov 12th at 11:08 AM
We have avoided use of LUA in our environment because of many of the issues raised. Curious to hear how other people are using it, but we are mostly responding to logs/events that Suricata generates. We prefer pub/sub approach to events as opposed to the overhead and sec issues involved with interacting directly with Suricata.
One thing we are missing as Eric Liu Leblond mentioned, is a generic way for Suricata to hand off a packet stream. If a rule could trigger Suricata to send a stream to generic pcap interface or socket, then users could use their own scripting languages to work with it. Would that negate or replace the most common use case for Lua here?

Eric Leblond 1 day ago
Should it be the packet stream or any fields extracted by Suri?

Danny Browning 1 day ago
Yeah, from this conversation, maybe we don't need wasm or lua

Danny Browning 1 day ago
If we had a way to forward packets, http bodies, or file streams, you may not need lua

Danny Browning 1 day ago
This is part of the reason we forward packets to suricata, so then we can process them after suricata alerts on them

Corrado 1 day ago
We use Lua extensively, not much for complex operations on a specific packet and more instead for maintaining state across packets of the same flow (propagating the state with flowbits). We implement via lua stuff like beaconing behavior detection or ssh events. But we have the advantage that we control the appliance that runs the rules and the lua engine itself.

Chris G 1 day ago
I think it needs to be a raw packet stream to support advanced operations. I was thinking of how we used to use PF and pflog iface to process dropped traffic. Every scripting language has the ability to interact with an interface device (or socket) (edited)

Jason Ish 1 day ago
Seems like a different feature than allowing rules to use rule scripts. Want to drop this idea in #topic-suggestions (edited)

Related issues:
Related to Task #4097: Suricon 2020 brainstorm

History
#1 - 11/14/2020 02:37 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added

#2 - 11/19/2020 09:06 PM - Victor Julien
- Tracker changed from Feature to Task
- Subject changed from Hand off packet streams on alerts to Research: Hand off packet streams on alerts

I think the conclusion in the call was that this needs a bit more thought and needs a use case description.

#3 - 11/19/2020 09:10 PM - Victor Julien
- Assignee set to Community Ticket
- Target version set to TBD