Suricata - Feature #885

Feature # 549 (Closed): Extract file attachments from emails

smtp file_data support

07/19/2013 06:18 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Giuseppe Longo
Category:
Target version: 2.1beta4
Effort:
Difficulty:

Description

Subtasks:
Feature # 1283: support for snort's file_data keyword

Closed

History

#1 - 07/19/2013 06:19 AM - Victor Julien
- Tracker changed from Bug to Feature

#2 - 07/19/2013 06:20 AM - Victor Julien
We should probably inspect the decoded attachments with it, like Snort does: "When the traffic is SMTP the file_data points to the decoded attachments when decoding is enabled for those preprocessors, otherwise to the entire data body."

#3 - 07/19/2013 06:46 AM - Anoop Saldanha
- headers
- raw_headers
- envelope.from
- envelope.to

to start with. Won't be hard to support these.

Let's start with file_data first of course.

#4 - 10/26/2013 10:21 AM - Victor Julien
- Target version set to TBD

#5 - 11/19/2013 04:20 PM - Will Metcalf
This has been TBD'd?!?! Wheres Peter? I need a shoulder to cry on. We need this.

#6 - 11/19/2013 04:30 PM - Eoin Miller
This type of functionality would be VERY useful for creating alerting based on spammed out/speared attacks coming in via SMTP. Without this, currently you are unable to even create IDS alerting for .exe files, encrypted zip files, etc that are coming to your users through the mail flow.

#7 - 11/20/2013 03:33 AM - Victor Julien
- Target version changed from TBD to 3.0RC2
- Parent task set to #549

This depends on #549.

#8 - 08/13/2014 03:52 AM - Victor Julien
- Assignee changed from Anoop Saldanha to Victor Julien
- Target version changed from 3.0RC2 to 2.1beta2

07/16/2022
#9 - 10/28/2014 02:47 PM - Victor Julien
- Target version changed from 2.1beta2 to 2.1beta3

#10 - 12/19/2014 04:57 AM - Victor Julien
- Target version changed from 2.1beta3 to 2.1beta4

#11 - 05/08/2015 10:18 AM - Victor Julien
- Status changed from Assigned to Closed
- Assignee changed from Victor Julien to Giuseppe Longo

https://github.com/inliniac/suricata/pull/1471