STIX Working Call

2019-05-28

Agenda

- Review Project Plan (1 minutes)
- Editorial Status Report (3 minutes)
- Items to Discuss (50* minutes)
- Action Items (2 minutes)

Editorial Status Review

- Identifier text has been resolved per last week's working call
- Changed the vocabulary type name from artifact-encryption-enum to encryption-algorithm-enum
- Added an aliases property to the Tool Object per Github Issue: 64
- Really close to releasing working draft 04
- Started flagging items in Github for working draft 05 and later
- Out of 150 issues that were not triaged, we are down to 39 to do

Add Malware Type Entries

- Add Benign to Malware Type vocab, Github Issue: 23
- Add some additional entries to Malware Type vocab, Github Issue: 24
  - Requested values:
    - Already added: Spyware, Screen-Capture, Rogue-Security-Software, DDOS, resource-exploitation
    - TBD: Bootkit, downloader, wiper, webshell, and unknown.

Observed Data Change

- John-Mark has a suggestion on Observed Data

List of type Dictionary

- 6.6.1 and 6.12.2.1 use a dictionary for header information, but headers can have duplicate data and flattening the headers into this structure loses information.
- Github Issues 137 and 138
- We should solve both of these in the same way

6.6.1 - Github Issue: 138

additional_header_fields (optional)	`dictionary`	Specifies any other header fields (except for **date**, **received_lines**, **content_type**, **from_ref**, **sender_ref**, **to_refs**, **cc_refs**, **bcc_refs**, and **subject**) found in the email message, as a dictionary. Each key/value pair in the dictionary represents the name/value of a single header field or names/values of a header field that occurs more than once. Each dictionary key **SHOULD** be a case-preserved version of the header field name. For cases where a header field occurs exactly once, the corresponding value for the dictionary key **MUST** be a `string`. For cases where a header field occurs more than once, the corresponding value for the dictionary key **MUST** be a `list` of type `string`, where each `string` in the `list` represents a single value of the header field.

6.6.1 - Github Issue: 138

Each key/value pair in the dictionary represents the name/value of a single header field or names/values of a header field that occurs more than once. Each dictionary key **SHOULD** be a case-preserved version of the header field name. For cases where a header field occurs exactly once, the corresponding value for the dictionary key **MUST** be a `string`. For cases where a header field occurs more than once, the corresponding value for the dictionary key **MUST** be a `list` of type `string`, where each `string` in the `list` represents a single value of the header field.

6.12.2.1 - Github Issue: 137

request_header (optional)	`list of type dictionary`	Specifies all of the HTTP header fields that may be found in the HTTP client request, as a list of dictionaries~~y~~. Each dictionary in the list **MUST** contain only the following keys: • name:~~Each key in the dictionary **MUST** be capture~~the ~~the~~ name of the header field; ~~and~~ **SHOULD** preserve case, e.g., `User-Agent`. • value:~~The corresponding value~~ the corresponding value of the header field specified by the name key;~~for each dictionary key~~ **MUST** be a `string`.

Github Issues: 137 & 138

- Proposal
- Say that all values MUST be a list of type string

Changes to SCOs

- We added the common “created” and “modified” to all SCOs at the end of the last F2F. However, we did not realize that they collided with a few SCO objects:
  - Directory Object
  - File Object
  - Process Object
  - Windows™ Registry Key Object

Changes to SCOs

- What should we do for working draft 04
  - Remove the “created” and “modified” common properties for working draft 04
    - We would add them back later when we address versioning holistically
    - Least risky option at this stage since we may need to make additional changes once we fully address versioning of SCOs
- Make a breaking change to the various SCO objects?

Action Items

- We have not addressed any of the patterning issues for Working Draft 04, the project plan calls them out for Working Draft 05.
- Review Working Draft 04 when it comes out
- Make all suggestions in the google docs or send to the email list.