**Malware Sample Artifact**

A new Malware Artifact object could be defined that is similar to the Artifact object, but malware oriented (e.g., known to be malicious). However, the properties of the two objects would be nearly identical, so defining a property extension schema for the Artifact object is the simpler solution.

# Artifact Object Schema – Malware Sample Extension

A primary consideration for sharing malware samples is accidental execution. The addition of a custom property **(is\_safe)** would help users understand the potential risk.

Table 1 shows the custom property—an extension to the Artifact SCO—that can be used to define a malware sample artifact.

**Table 1. Malware Sample Artifact Extension Properties**

| **Property Name** | **Type** | **Description** |
| --- | --- | --- |
| **is\_safe** (required) | boolean | Indicates whether the artifact is safe, i.e., can be opened or processed without risking harm or infection. The default value is false. |

# Example – Malware Sample Artifact

Figure 1 is an example malware sample artifact and includes a STIX Extension Definition object.

{

"id": "extension-definition--8053ffa0-dec7-4aef-870e-a56d0082cf69",

"type": "extension-definition",

"spec\_version": "2.1",

"name": "Malware Artifact Extension",

"description": "This schema creates a new property to indicate whether a malware artifact is safe.",

"created": "2022-10-25T09:00:00.000000Z",

"modified": "2022-10-25T09:00:00.000000Z",

"created\_by\_ref": "identity--8ce3f695-d5a4-4dc8-9e93-a65af453a31a",

"schema": "https://github.com/oasis-open/cti-stix-common-objects/tree/main/ extension-definition-specifications/malware-artifact/",

"version": "1.0.0",

"extension\_types": ["toplevel-property-extension"],

"extension\_properties": ["is\_safe"]

},

{

"type": "artifact",

"spec\_version": "2.1",

"id": "artifact--3057f78d-7d16-5092-99fe-ecff58408b02",

"mime\_type": "application/zip",

"payload\_bin": "VGhpcyBpcyBhIHBsYWNlaG9sZGVyIGZvciBhbiB1bnNhZmUgbWFsd2FyZSBiaW5hcnkh",

"hashes": {

"MD5": "6b885a1e1d42c0ca66e5f8a17e5a5d29",

"SHA-256": "3eea3c4819e9d387ff6809f13dde5426b9466285b7d923016b2842a13eb2888b"

},

"is\_safe": false,

"extensions": {"extension-definition--8053ffa0-dec7-4aef-870e-a56d0082cf69": {"extension\_type": "toplevel-property-extension"}}

}

**Figure** 1**. Example Artifact Object (Malware)**