**Malware Sample Artifact**

A new Malware Artifact object could be defined that is similar to the Artifact object, but malware oriented (i.e., known/assumed 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 SDO—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--2dd00d09-9f42-554c-9dd7-75175b98a6c1",

"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--a1223c56-7f5e-5c71-8d72-a3d9b24fcb6f",

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

"payload\_bin": "VNEKDAAAJDeudjDjedkedDjj==<snip>",

"hashes": {

"MD5": "84730cc04f0a433fce5336b7c7504d2c",

"SHA-256": "f432cf964b998e582fd2c191a0c986430cb632a315435f80798dd2a2…"

},

"is\_safe": "false",

"extensions": {"extension-definition--2dd00d09-9f42-554c-9dd7-75175b98a6c1": {

"extension\_type": "toplevel-property-extension"

}}

}

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