**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 sample STIX Extension Definition object.

{  
 "id": "extension-definition--bd736433-33be-0466-ad33-bef32424a776",  
 "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": "2020-10-31T09:00:00.000000Z",  
 "modified": "2020-10-31T09:00:00.000000Z",  
 "created\_by\_ref": "identity--66948562-8321-4537-4539-86756453bbbd",  
 "schema": "https://www.ais.dhs.gov/schema-malware-artifact/v1/",  
 "version": "1.0",  
 "extension\_types": ["toplevel-property-extension"],

"extension\_properties": ["is\_safe"]  
},  
{  
 "type": "artifact",  
 "spec\_version": "2.1",  
 "id": "artifact--b67d30ff-02ac-498a-92f9-32f845f448cf",  
 "mime\_type": "application/zip",  
 "payload\_bin": "VNEKDAAAJDeudjDjedkedDjj==... <snip>",  
 "hashes": {  
 "MD5": "84730cc04f0a433fce5336b7c7504d2c",  
 "SHA-256": "f432cf964b998e582fd2c191a0c986430cb632a315435f80798dd2a2…e5f5"  
 },

"is\_safe": "false",  
 "extensions": {"extension-definition--bd736433-33be-0466-ad33-bef32424a776": {

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

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