Malware Behavior Extension

This STIX 2.1 Extension Definition object was defined to capture malware behavior information. It was defined specifically for Malware Behavior Catalog (MBC) objectives, behaviors, and methods [[mbc](https://github.com/MBCProject)], but it is also applicable to other malware-related knowledge bases and use cases.

**Malware Behavior Objects**

Three new STIX Domain Objects (SDOs) are defined to capture malware behavior information. Previously, the STIX Attack Pattern object was extended with STIX 2.0 custom properties. To more accurately represent MBC content, three new SDOs are defined in this document.

* Behavior Object: captures malware behaviors.
* Method Object: captures methods that exemplify behaviors.
* Objective Object: captures higher level malware objectives.

**Malware Corpus**

New properties of the STIX 2.1 Malware SDO, as well as best practice guidance for existing properties, enable better capture of malware in the MBC corpus.

The relationship between the objects defined in this document is shown in Figure 1. Blue arrows denote embedded relationships, and orange arrows denote STIX Relationship Objects (SROs).

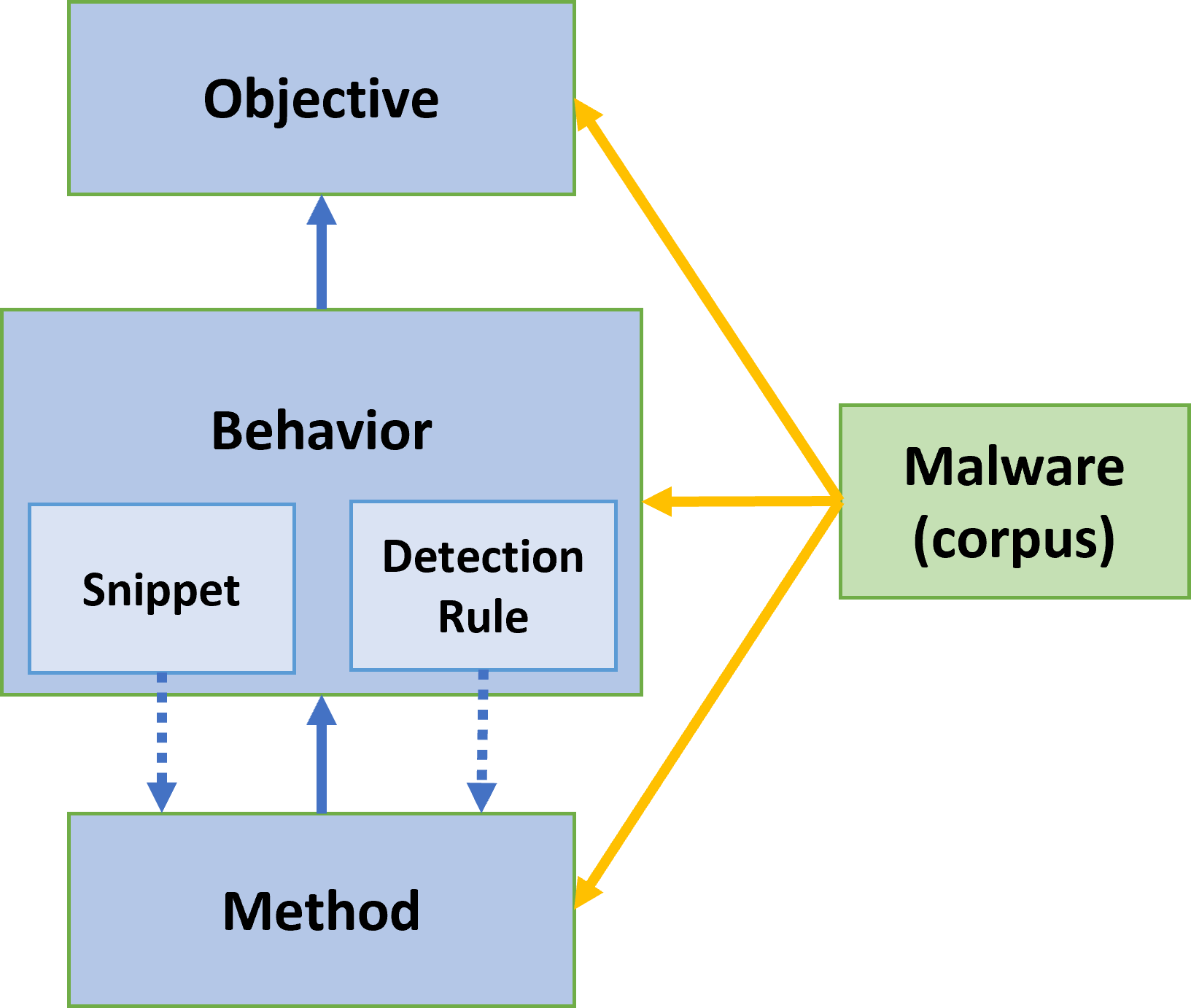


Figure 1. Malware behavior objects

We used the following guidelines when defining the objects.

* Relationships between malware behavior-related objects, for example between behaviors and methods, are embedded because they are inherent to the objects and do not change.
* Code snippets are not referenced outside an MBC object; therefore, they are captured as embedded properties using a new snippet data type, rather than as Artifact objects (which would be associated via SROs).
* Detection information is specific to an MBC object and is therefore captured as an embedded property using a new detection data type.

Section 1 presents the three new behavior-related SDOs, and Section 2 presents the corpus-related extension to the Malware SDO. New data types and vocabularies are defined in Sections 3 and 4, respectively. Section 5 comprises three appendices: the Extension Definition Object used in document examples, a non-MBC knowledge base example, and an example showing how behavior-based analysis results are captured in a Malware Analysis SDO. References are in Section 6.

# ​1​ Malware Behavior SDOs

The new SDOs below enable capture of malware behavior-related information. In the MBC, these are objective, behavior, and method objects.

## ​1.1​ Behavior Object

**Type Name:** malware-behavior

The behavior object captures malware behaviors. In MBC, these objects may correspond to behavior or micro-behaviors. When MBC enhances (modifies) an existing ATT&CK technique, the resulting object that is captured in MBC is considered new, so it will be defined as an MBC behavior object with a new STIX identifier.

### ​1.1.1​ Properties

| **Required Common Properties** | | |
| --- | --- | --- |
| **type**, **spec\_version**, **id**, **created**, **modified** | | |
| **Optional Common Properties** | | |
| **confidence**, **created\_by\_ref**, **extensions**, **revoked**, **labels**, **lang**, **external\_references**, **object\_marking\_refs**, **granular\_markings** | | |
| **Not Applicable Common Properties** | | |
| **defanged** | | |
| **Behavior Specific Properties** | | |
| **name**, **micro**, **obj\_defn**, **obj\_version**, **related\_object\_refs**, **tags**, **objective\_refs**, **snippets**, **detection\_rules**, **contributor\_refs** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this property **MUST** be malware-behavior. |
| **external\_references** (optional) | list of type  external-reference | A list of external references that refer to non-STIX information.  All references used by object properties **MUST** be defined. The **url** property **SHOULD** be populated. The **description** property **SHOULD** contain the citation (without the URL, which should be captured in the **url** property). |
| **created**  (required) | timestamp | The date the behavior was created.  The time portion of the timestamp will be ignored in MBC.  This date may not correspond to the date the STIX object was created and instead may correspond to the date when the MBC behavior was defined. |
| **modified**  (required) | timestamp | The date the behavior was last modified.  The time portion of the timestamp will be ignored in MBC.  This date may not correspond to the date the STIX object was modified and instead may correspond to the date when the MBC behavior was last modified. |
| **name** (required) | string | The name of the behavior (e.g., Request Email Address List). |
| **micro** (optional) | boolean | Indicates whether the object is a micro-behavior. The default value is false. |
| **obj\_defn** (required) | external-reference | The definition of the malware behavior.  When specifying an MBC behavior, the **source\_name** property **MUST** be set to mbc and the **external\_id** property **MUST** be formatted as MBC id (e.g., B0030, C0061). The **description** property **SHOULD** be a textual description of the behavior and **MAY** include citations to references defined in the **external\_references** property. |
| **obj\_version** (optional) | string | Specifies the version of the behavior object. |
| **related\_object\_refs** (optional) | list of type identifier | Related objects from other knowledge bases.  For MBC behaviors, the value of this property **SHOULD** be the identifier of an ATT&CK technique. |
| **tags** (optional) | dictionary | The dictionary keys **MUST** be the tag names where the values are the value of the tag.  The **labels** common property should be used to capture tags with values and without names. |
| **objective\_refs** (optional) | list of type  identifier | The malware objective objects associated with the behavior.  The value of this property **MUST** be the identifier for an objective SDO. |
| **snippets** (optional) | list of type snippet | The code snippets associated with the behavior. |
| **detection\_rules** (optional) | list of type detection-rule | The ways to detect the behavior. |
| **contributor\_refs** (optional) | list of type  identifier | Contributor(s) to the behavior information.  The value of this property **MUST** be the identifier for an identity SDO. |

### ​1.1.2​ Behavior Example

The example below shows basic properties. Some properties that apply to both behavior and method objects are shown in the method example. The extension definition object is shown in the appendix.

{

"type": "malware-behavior",

"spec\_version": "2.1",

"id": "malware-behavior--7fd7253f-274e-4156-be58-7ac900fc221a",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"created": "2019-08-01T00:00:00.000Z",

"modified": "2022-11-21T00:00:00.000Z",

"name": "Sandbox Detection",

"obj\_defn": {

"source\_name": "mbc",

"description": "Detects whether the malware instance is being executed <snip>",

"url": "https://github.com/MBCProject/mbc-markdown <snip> /sandbox-detection.md",

"external\_id": "B0007"

},

"obj\_version": "2.0",

"related\_object\_refs": [

"attack-pattern--29be378d-262d-4e99-b00d-852d573628e6",

"attack-pattern--6ffad4be-bfe0-424f-abde-4d9a84a800ad",

"attack-pattern--91541e7e-b969-40c6-bbd8-1b5352ec2938"

],

"tags": {"Anti-Analysis-Type": "Detection"},

"objective\_refs": ["malware-objective--a6de0a96-50b6-441f-8e62-06eb6db84183"],

"detection\_rules": [{

"rule\_type": "capa",

"rule\_name": "check for sandbox and av modules",

"url": "https://github.com/capa-rules...check-for-sandbox-and-av-modules.yml",

"api\_fncs": ["GetModuleHandle"],

"detect\_ref": "malware-method--5650472c-6f90-44c3-8944-f763507e9220"

}],

"snippets": [{

"snippet": "push ebx, \n add esp, \n 0FFFFFEF4h, \n xor ebx, \n ebx <snip>",

"language": "asm",

"exemplify\_ref": "malware-method--5650472c-6f90-44c3-8944-f763507e9220"

}],

"external\_references": [

{

"source\_name": "cisco",

"url": "https://blogs.cisco.com/security/talos/rombertik",

"description": "B. Baker and A. Chiu, \"Threat Spotlight: Rombertik - Gazing Past the Smoke, Mirrors, and Trapdoors,\" Cisco Threat Research, blog, May 4, 2013 [Online]."

},

{

"source\_name": "lordnoteworthy"

"url": "https://github.com/LordNoteworthy/al-khaser"

"description": "A. Faouzi (LordNoteworthy), \"README.md,\" Al-Khaser v0.81. Accessed Apr. 29, 2023 [Online].

}

],

"extensions": {

"extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0" : {

"extension\_type" : "new-sdo"

}

}

}

## ​1.2​ Method Object

**Type Name:** malware-method

The method object captures methods that further explain or exemplify malware behaviors.

### ​1.2.1​ Properties

| **Required Common Properties** | | |
| --- | --- | --- |
| **type**, **spec\_version**, **id**, **created**, **modified** | | |
| **Optional Common Properties** | | |
| **confidence**, **created\_by\_ref**, **extensions**, **external\_references**, **labels**, **lang**, **revoked**, **object\_marking\_refs**, **granular\_markings** | | |
| **Not Applicable Common Properties** | | |
| **defanged** | | |
| **Method Specific Properties** | | |
| **name**, **micro**, **obj\_defn**, **behavior\_ref**, **contributor\_refs** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this property **MUST** be malware-method. |
| **external\_references** (optional) | list of type  external-reference | A list of external references that refer to non-STIX information.  All references used by object properties **MUST** be defined. The **url** property **SHOULD** be populated. The **description** property **SHOULD** contain the citation (without the URL, which should be captured in the **url** property). |
| **created**  (required) | timestamp | The date the method’s behavior (referenced by the **behavior\_ref** property) was created. |
| **modified**  (required) | timestamp | The date the method’s behavior (referenced by the **behavior\_ref** property) was last modified. |
| **name** (required) | string | The name of the method (e.g., API Hook Detection). |
| **micro** (optional) | boolean | Indicates whether the method belongs to a micro-behavior. The default value is false. |
| **obj\_defn** (required) | external-reference | The definition of the malware method.  When specifying an MBC method, the **source\_name** property **MUST** be set to mbc and the **external\_id** property **MUST** be formatted as MBC id (e.g., B0030.003). The **description** property **SHOULD** be a textual description of the method and **MAY** include citations to external references (which are defined in the **external\_references** property of the parent behavior). The **url** property **MAY** be populated but it is not needed given the implicit link provided through the **behavior\_ref** property. |
| **behavior\_ref** (required) | identifier | The STIX identifier of the parent behavior object associated with the method.  The value of this property **MUST** be the identifier for a behavior SDO. |
| **contributor\_refs** (optional) | list of type  identifier | Contributor(s) to the method information.  The value of this property **MUST** be the identifier for an identity SDO. |

### ​1.2.2​ Method Example

The extension definition object is shown in the appendix.

{

"type": "malware-method",

"spec\_version": "2.1",

"id": "malware-method--5650472c-6f90-44c3-8944-f763507e9220",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"created": "2023-02-01T10:49:59Z",

"modified": "2023-02-01T10:49:59Z",

"name": "Product Key/ID Testing",

"obj\_defn": {

"source\_name": "mbc",

"external\_id": "B0007.005",

"description": "Checking for a particular product key/ID associated..."

},

"behavior\_ref": "malware-behavior--7fd7253f-274e-4156-be58-7ac900fc221a",

"extensions": {

"extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0" : {

"extension\_type" : "new-sdo"

}

}

}

## ​1.3​ Objective Object

**Type Name:** malware-objective

The objective object captures higher level malware objectives.

### ​1.3.1​ Properties

| **Required Common Properties** | | |
| --- | --- | --- |
| **type**, **spec\_version**, **id**, **created**, **modified** | | |
| **Optional Common Properties** | | |
| **confidence**, **created\_by\_ref**, **extensions**, **external\_references**, **labels**, **lang**, **revoked**, **object\_marking\_refs**, **granular\_markings** | | |
| **Not Applicable Common Properties** | | |
| **defanged** | | |
| **Objective Specific Properties** | | |
| **name**, **micro**, **obj\_defn** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this property **MUST** be malware-objective. |
| **external\_references** (optional) | list of type  external-reference | A list of external references that refer to non-STIX information.  All references used by object properties **MUST** be defined. The **url** property **SHOULD** be populated. The **description** property **SHOULD** contain the citation (without the URL, which should be captured in the **url** property). |
| **created**  (required) | timestamp | The date the objective was created.  The time portion of the timestamp will be ignored in MBC.  This date may not correspond to the date the STIX object was created and instead may correspond to the date when the MBC objective was defined. |
| **modified**  (required) | timestamp | The date the objective was last modified.  The time portion of the timestamp will be ignored in MBC.  This date may not correspond to the date the STIX object was modified and instead may correspond to the date when the MBC objective was last modified. |
| **name** (required) | string | Name of the malware objective (e.g., Anti-Behavioral Analysis). |
| **micro** (optional) | boolean | Indicates whether the object is a micro-objective. The default value is false. |
| **obj\_defn** (required) | external-reference | The definition of the malware objective.  When specifying an MBC objective, the **source\_name** property **MUST** be set to mbc and the **external\_id** property **MUST** be formatted as MBC id (e.g., OB0003). The **description** property **MAY** include citations to references defined in the **external\_references** property. |

### ​1.3.2​ Objective Example

The extension definition object is shown in the appendix.

{

"type": "malware-objective",

"spec\_version": "2.1",

"id": "malware-objective--a6de0a96-50b6-441f-8e62-06eb6db84183",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"created": "2019-08-01T00:00:00.000Z",

"modified": "2022-10-31T00:00:00.000Z",

"name": "Anti-Behavioral Analysis",

"obj\_defn": {

"source\_name": "mbc",

"description": "Behaviors that prevent, obstruct, or evade <snip>",

"url": "https://github.com/MBCProject/mbc-markdown <snip> /anti-behavioral-analysis",

"external\_id": "OB0001",

},

"external\_references": [

{

"source\_name": "unprotect",

"url": "https://unprotect.it",

"description": "T. Roccia and J. Lesueur, Unprotect Project, Accessed Apr. 29, 2023. [Online]."

},

{

"source\_name": "poz",

"url": "https://github.com/knowmalware/InDepthUnpacking"

"description": "F. Poz, \"InDepthUnpacking,\" 2016. Accessed Apr. 29, 2023. [Online]."

}

],

"extensions": {

"extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0" : {

"extension\_type" : "new-sdo"

}

}

}

# ​2​ Malware Corpus

We use a property extension of the STIX 2.1 Malware object to capture corpus elements.

## ​2.1​ Object Extension

Three new properties are defined on the Malware SDO. In addition, please note:

* A malware instance or family is associated with an objective, behavior, or method via an SRO (i.e., “Malware uses Malware Behavior”). The fully specified object name (malware objective, malware behaviors, and/or malware method) **SHOULD** be included in the SRO description (e.g., Anti-Behavioral Analysis::Sandbox Detection::Self Check, Discovery::Taskbar Discovery).
* Malware alias information can be captured in the Malware SDO **alias** property.
* Indicator of compromise information can be captured in an Indicator SDO that is then associated with the Malware object via an SRO (i.e., “Indicator indicates Malware”).

| **Property Name** | **Type** | **Description** |
| --- | --- | --- |
| **external\_references** (optional) | list of type  external-reference | A list of external references that refer to non-STIX information.  All references used by object properties **MUST** be defined. The **url** property **SHOULD** be populated. The **description** property **SHOULD** contain the citation (without the URL, which should be captured in the **url** property). |
| **obj\_defn** (required) | external-reference | Reference to the malware.  When specifying malware from the MBC corpus, the **source\_name** property **MUST** be set to mbc and the **external\_id** property **MUST** be formatted as MBC id (e.g., X0021). The **description** property **MAY** include citations to references defined in the **external\_references** property. |
| **year** (optional) | string | This property denotes the year the malware instance or family was first seen. |
| **platforms** (optional) | list of type  open-vocab | This property denotes the operating system affected by the malware.  The values for this property **SHOULD** come from the os-type-ov open vocabulary. |

## ​2.2​ Relationships

These are the relationships defined between the Malware object and malware behavior extension objects.

| **Source** | **Name** | **Target** | **Description** |
| --- | --- | --- | --- |
| malware | uses | malware-objective, malware-behavior, malware-method | This Relationship indicates that the malware exhibits the malware objective, behavior, and/or method. |

## ​2.3​ Malware Corpus Examples

### ​2.3.1​ Gamut

The example below for the Gamut malware includes three behaviors for illustration purposes (the full list includes more than 30). It also shows an SRO between the Gamut Malware object and an indicator of compromise (Indicator object). The extension definition object is shown in the appendix.

[

{

"type": "malware",

"spec\_version": "2.1",

"id": "malware--47e74de4-bf1d-4210-a087-2becffdaa455",

"created": "2019-08-01T00:00:00.000Z",

"modified": "2023-03-01T00:00:00.000Z",

"name": "Gamut",

"aliases": ["bobax"],

"is\_family": true,

"external\_references": [

{

"source\_name": "trustwave",

"url": "https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/gamut- spambot-analysis/",

"description": "R. Mendrez, \"Gamut Spambot Analysis,\" Trustwave, blog, Mar. 4, 2014 [Online]."

},

{

"source\_name": "capa analysis",

"description": "Analysis output, capa 4.0, analyzed at MITRE on Oct. 12, 2022.",

"url": "https://github.com/mandiant/capa-rules"

}

],

"extensions": {"extension-definition--8e9e338f-c9ee-4d4f-8cac-85b4dcfdf3c1": {

"extension\_type": "property-extension",

"obj\_defn": {

"source\_name": "mbc",

"description": "Gamut is a spamming botnet.",

"url": "https://github.com/MBCProject/mbc-markdown <snip> /xamples",

"external\_id": "X0013"

},

"year": "2014",

"platforms": ["windows"]

}}

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--3b3a781f-23a1-4fa9-b6b4-1bb327b2929a",

"created": "2023-03-20T00:00:00.000Z",

"modified": "2023-03-20T00:00:00.000Z",

"relationship\_type": "uses",

"source\_ref": "malware--47e74de4-bf1d-4210-a087-2becffdaa455",

"target\_ref": "attack-pattern--0a5231ec-41af-4a35-83d0-6bdf11f28c65",

"description": "Execution::Shared Modules (T1129) -- Gamut links functions <snip> (Citation: trustwave gamut analysis) <snip>"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--96cd8697-4467-4df0-a41f-1c53b05b2431",

"created": "2023-03-20T00:00:00.000Z",

"modified": "2023-03-20T00:00:00.000Z",

"relationship\_type": "uses",

"source\_ref": "malware--47e74de4-bf1d-4210-a087-2becffdaa455",

"target\_ref": "malware-method--b95c3961-ce77-4e2e-9d3d-202d89b9db54",

"description": "Command and Control::C2 Communication::Receive Data (B0030.002) -- The malware sends data to the C2. (Citation: trustwave gamut analysis)"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--c8194de8-c2ba-4c74-896a-fd746232e7d0",

"created": "2023-03-20T00:00:00.000Z",

"modified": "2023-03-20T00:00:00.000Z",

"relationship\_type": "uses",

"source\_ref": "malware--47e74de4-bf1d-4210-a087-2becffdaa455",

"target\_ref": "malware-behavior--a446fac9-4d4e-439e-9b06-a3a7665c2281",

"description": "File System::Delete File (C0047)-- Gamut deletes files. (Citation: capa analysis output)"

},

{

"type": "indicator",

"spec\_version": "2.1",

"id": "indicator--25ad5feb-3716-44b6-9867-8643f5b2aac8",

"created": "2023-03-01T00:00:00.000Z",

"modified": "2023-03-01T00:00:00.000Z",

"indicator\_types": ["malicious-activity"],

"name": "Gamut hash",

"description": "This is an IoC for Gamut",

"pattern": "[ file:hashes.'SHA-256' = 'a56162bc623841102301df...1c838fcf256654932' ]",

"pattern\_type": "stix",

"valid\_from": "2023-03-01T00:00:00.000Z"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--1cffe80b-7cf8-416e-b2fe-a89c3fba7d9b",

"created": "2023-03-01T00:00:00.000Z",

"modified": "2023-03-01T00:00:00.000Z",

"relationship\_type": "indicates",

"source\_ref": "indicator--25ad5feb-3716-44b6-9867-8643f5b2aac8",

"target\_ref": "malware--47e74de4-bf1d-4210-a087-2becffdaa455"

}

]

### ​2.3.2​ GravityRAT

The example below shows capture of a relationship between a Malware object in the MBC corpus and a software (Malware) object in ATT&CK (**relationship\_type** is “related-to”).

[

{

"type": "malware",

"spec\_version": "2.1",

"id": "malware--ccdec6fb-3f9e-4bb6-922b-e16d37ee1ebf",

"created": "2019-08-01T00:00:00.000Z",

"modified": "2023-03-01T00:00:00.000Z",

"name": "GravityRAT",

"is\_family": true,

"external\_references": [{

"source\_name": "capa analysis",

"url": "https://github.com/mandiant/capa-rules",

"description": "Analysis output, capa 4.0, analyzed at MITRE on Oct. 12, 2022."

}],

"extensions": {"extension-definition--8e9e338f-c9ee-4d4f-8cac-85b4dcfdf3c": {

"extension\_type": "property-extension",

"obj\_defn": {

"source\_name": "mbc",

"description": "GravityRAT evades detection by <snip>",

"url": "https://github.com/MBCProject/<snip>/xample-malware/gravity-rat.md",

"external\_id": "X0016"

},

"year": "2018",

"platforms": ["windows"]

}}

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--1ca370e5-6fd3-4f7a-bd04-7bb3ab37b3db",

"created": "2023-05-03T00:00:00.000Z",

"modified": "2023-05-03T00:00:00.000Z",

"relationship\_type": "uses",

"source\_ref": "malware--ccdec6fb-3f9e-4bb6-922b-e16d37ee1ebf",

"target\_ref": "attack-pattern--72b74d71-8169-42aa-92e0-e7b04b9f5a08",

"description": "Discovery::Account Discovery (T1087) -- GravityRAT gets session username (Citation: capa analysis)."

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--39c88be9-803c-46fe-9ba2-5a465a2b3218",

"created": "2023-05-03T00:00:00.000Z",

"modified": "2023-05-03T00:00:00.000Z",

"relationship\_type": "related-to",

"source\_ref": "malware--ccdec6fb-3f9e-4bb6-922b-e16d37ee1ebf",

"target\_ref": "malware--1d1fce2f-0db5-402b-9843-4278a0694637"

}

]

# ​3​ Data Types

## ​3.1​ Detection Rule

**Type Name:** detection-rule

The detection rule data type captures details associated with detecting a behavior or method object. At least one of the **rule** or **url** properties **MUST** be present. Please see Section 1.1.2 for an example detection rule.

### ​3.1.1​ Properties

| **Property Name** | **Type** | **Description** |
| --- | --- | --- |
| **rule\_type** (required) | string | The type of rule (tool) used to detect the behavior or method. The values of this property **MUST** come from the detection-tool-ov enumeration. |
| **rule\_name** (optional) | string | The name of the rule or signature. |
| **rule** (optional) | string | The detection rule or signature. If this property is not populated, then the **url** property **MUST** be populated. |
| **url** (optional) | string | A URL reference to an external resource that defines the rule or signature [[RFC3986](https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#kix.vaucl8w7ov0y)]. If this property is not populated, then the **rule** property **MUST** be populated. |
| **detect\_ref** (optional) | identifier | When a rule detects a specific method, as opposed to a behavior more generally, this property specifies the method.  If defined, the value of this property **MUST** be the identifier of a Method SDO. |
| **description** (optional) | string | The description of the rule, signature, or manual method. |
| **api\_fncs** (optional) | list of type string | The Windows API functions associated with the rule or signature. |

## ​3.2​ Snippet

**Type Name:** snippet

The code snippet data type captures details associated with code snippets that exemplify behaviors. Please see Section 1.1.2 for an example snippet.

### ​3.2.1​ Properties

| **Property Name** | **Type** | **Description** |
| --- | --- | --- |
| **snippet** (required) | string | The code snippet. |
| **exemplify\_ref** (optional) | identifier | When a snippet exemplifies a specific method, as opposed to a behavior more generally, this property specifies the method.  If defined, the value of this property **MUST** be the identifier of a method SDO. |
| **language** (optional) | string | The language of the code snippet.  The value of this property **SHOULD** come from the STIX 2.1 implementation-language-ov open vocabulary or the list of additional values defined in Section 5.1. |
| **description** (optional) | string | The description of the code snippet. Citations referencing external references **MAY** be included. |
| **references** (optional) | list of type external-reference | References external sources that define the snippet. If the reference is to the malware sample from which the code snippet was extracted, the hash value associated with the URL **SHOULD** correspond to the hash of the sample. |
| **hash** (optional) | string | The hash of the malware sample from which the code snippet was extracted. This property **SHOULD NOT** be used if the **references** property provides a URL and hash property of the sample. |
| **author\_ref** (optional) | identifier | The **author** property specifies the **id** property of the identity object that describes the author of the snippet. |

# ​4​ Vocabularies and Enumerations

## ​4.1​ Implementation Language Vocabulary (Extension)

**Vocabulary Name:**implemention-language-ov

The table shows additional values defined for the implementation language vocabulary.

| **Vocabulary Summary** | |
| --- | --- |
| asm, cmd, delphi, masm | |
| **Vocabulary Value** | **Description** |
| asm | Specifies assembly programming language. |
| cmd | Specifies the cmd shell scripting language. |
| delphi | Specifies the Delphi programming language. |
| masm | Specifies the Microsoft Macro Assembler language. |

## ​4.2​ Detection Tool Vocabulary (New)

**Vocabulary Name:**detection-tool-ov

The detection tool open vocabulary, used in the detection rule data type, denotes the tool used to detect the object.

| **Vocabulary Summary** | |
| --- | --- |
| capa, cape, manual, sigma, yara | |
| **Vocabulary Value** | **Description** |
| capa | The capa static analysis tool. |
| cape | The CAPE sandbox. |
| manual | A manual rule or text-based information. |
| sigma | A Sigma rule. |
| yara | A YARA rule. |

## ​4.3​ OS Type Vocabulary (New)

**Vocabulary Name:**os-type-ov

The OS type open vocabulary denotes the operating system affected by malware.

| **Vocabulary Summary** | |
| --- | --- |
| android, ios, linux, macos, windows | |
| **Vocabulary Value** | **Description** |
| android | The Android platform. |
| ios | The iOS platform. |
| linux | The Linux platform. |
| macos | The MacOS platform. |
| windows | The Windows platform. |

# ​5​ Appendix

## ​5.1​ Extension Definition Objects

The following Extension Definition objects define the new and extended SDOs discussed above.

{

"extension-definition--8e9e338f-c9ee-4d4f-8cac-85b4dcfdf3c1",

"type": "extension-definition",

"spec\_version": "2.1",

"name": “Malware Behavior Extension for the Malware Object",

"description": "An extension to the Malware object to support malware behaviors.",

"created": "2023-03-12T10:12:00.000Z",

"modified": "2023-03-12T10:12:00.000Z",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"schema": "https://raw.githubusercontent.com/oasis-open/cti-stix-common-objects/main/extension-definition-specifications/mbc/extension-definition--8e9e338f-c9ee-4d4f-8cac-85b4dcfdf3c1.json",

"version": "1.0.0",

"extension\_types": [

"property-extension"

]

}

{

"id": "extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0",

"type": "extension-definition",

"spec\_version": "2.1",

"name": "Malware Behavior Extension",

"description": "This schema defines new SDOs to capture malware behaviors.",

"created": "2023-03-12T10:12:00.000Z",

"modified": "2023-03-12T10:12:00.000Z",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"schema": "https://raw.githubusercontent.com/oasis-open/cti-stix-common-objects/main/extension-definition-specifications/mbc/extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0.json",

"version": "1.0.0",

"extension\_types": [

"new-sdo"

]

}

## ​5.2​ Unprotect Project Example

This example illustrates how the Malware Behavior Extension Definition object can capture a category and technique from the Unprotect Project [[up](https://www.unprotect.it/)]. Note that sometimes the Unprotect Project assigns multiple IDs to their techniques, which is reflected in the **external\_id** property.

[{

"type": "malware-objective",

"spec\_version": "2.1",

"id": "malware-objective--a624a7a-ef64-46ce-b582-b963b7d6113f",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"created": "2023-04-21T00:00:00.000Z",

"modified": "2023-04-21T00:00:00.000Z",

"name": "Anti-Debugging",

"obj\_defn": {

"source\_name": "unprotect-project",

"url": "https://www.unprotect.it/category/anti-debugging/"

},

"extensions": {

"extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0" : {

"extension\_type" : "new-sdo"

}

}

},

{

"type": "malware-behavior",

"spec\_version": "2.1",

"id": "malware-behavior--b4ab6e5e-82b2-4699-938a-778f840a80fa",

"created\_by\_ref": "identity--b73c59c1-8560-449a-b8d0-c2ce0533c5bf",

"created": "2019-03-18T00:00:00.000Z",

"modified": "2023-02-27T00:00:00.000Z",

"name": "GetTickCount",

"obj\_defn": {

"source\_name": "unprotect-project",

"description": "This is typical timing function which is used to measure <snip>",

"url": "https://www.unprotect.it/technique/gettickcount/",

"external\_id": "U0125, B0001.032"

},

"labels": ["gettickcount"],

"objective\_refs": ["malware-objective--6a624a7a-ef64-46ce-b582-b963b7d6113f"],

"detection\_rules": [{

"rule\_type": "capa",

"rule": "rule: \n meta: \n name: check for time delay via GetTickCount <snip>",

}],

"snippets": [{

"snippet": "bool IsDebugged(DWORD dwNativeElapsed) \n{ \n DWORD <snip>",

"language": "c++",

}],

"external\_references": [

{

"source\_name": "palo alto networks",

"url": "https://researchcenter.paloaltonetworks.com/2015/10/ticked-off-upatre- malwares -simple-anti-analysis-trick-to-defeat-sandboxes/"

},

{

"source\_name": "checkpoint",

"url": "https://anti-debug.checkpoint.com/techniques/timing.html#kernel-timing"

}

],

"extensions": {

"extension-definition--d57b7c9c-7fa6-436b-b82c-8e6f69cdc3d0" : {

"extension\_type" : "new-sdo"

}

}

}]

## ​5.3​ Malware Analysis SDO Example

This example illustrates capture of a malware method identified during analysis and captured as a relationship between a Malware Analysis object and a Malware Method object (the Malware Method object is defined in the example in Section 1.2.2).

[

{

"type": "malware",

"spec\_version": "2.1",

"id": "malware--69ee752f-416b-4850-8839-c8f211b8ab17",

"created": "2023-05-02T00:00:00.000Z",

"modified": "2023-05-02T00:00:00.000Z",

"malware\_types": ["unknown"],

"is\_family": false,

"sample\_refs": ["file--cd46f4ec-ae7e-4e49-babe-8fce238fa4da"]

},

{

"type": "file",

"id": "file--cd46f4ec-ae7e-4e49-babe-8fce238fa4da",

"spec\_version": "2.1",

"size": 65536,

"name": "sample.exe",

"hashes": {

"MD5": "ffd05678341dcfed98bf019fbbe3409c",

"SHA-1": "6634de093251ff6cf441770d1b9b1253556c8d18",

"SHA-256": "bddff46c7300e87a7301266cf41ce397e3f0adf6bd9c7e227b56452437769999"

}

},

{

"type": "malware-analysis",

"spec\_version": "2.1",

"id": "malware-analysis--fbcd0450-8879-48cb-a72b-37d2b039892c",

"created": "2023-05-02T12:12:00.000Z",

"modified": "2023-05-02T12:12:00.000Z",

"product": "cuckoo",

"version": "2.0.7",

"analysis\_started": "2023-03-09T11:52:55.06523Z",

"analysis\_ended": "2023-03-09T11:53:13.081646Z",

"result": "suspicious",

"sample\_ref": "file--cd46f4ec-ae7e-4e49-babe-8fce238fa4da"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--35462d99-0872-adfe-1288-65748cbd9433",

"created": "2020-05-02T12:12:00.000Z",

"modified": "2020-05-02T12:12:00.000Z",

"relationship\_type": "dynamic-analysis-of",

"source\_ref": "malware-analysis--fbcd0450-8879-48cb-a72b-37d2b039892c",

"target\_ref": "malware--69ee752f-416b-4850-8839-c8f211b8ab17"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--5342743f-034d-02bc-3829-1023543377df",

"created": "2020-05-29T01:01:46.369Z",

"modified": "2020-05-29T01:01:46.369Z",

"relationship\_type": "derived-from",

"source\_ref": "malware-method--5650472c-6f90-44c3-8944-f763507e9220",

"target\_ref": "malware-analysis--fbcd0450-8879-48cb-a72b-37d2b039892c"

},

{

"type": "relationship",

"spec\_version": "2.1",

"id": "relationship--84750981-cdfe-4637-2022-bd7af2534712",

"created": "2020-05-29T01:01:46.370Z",

"modified": "2020-05-29T01:01:46.370Z",

"relationship\_type": "uses",

"source\_ref": "malware--69ee752f-416b-4850-8839-c8f211b8ab17",

"target\_ref": "malware-method--5650472c-6f90-44c3-8944-f763507e9220",

"description": "Sandbox Detection::Product Key/ID Testing"

}

]

# ​6​ References

[mbc] The Malware Behavior Catalog, <https://github.com/MBCProject>

[up] The Unprotect Project, [Home - Unprotect Project](https://www.unprotect.it/)