CybOXTM Version 2.1.1 Part 24: File Object

Working Draft 01

15 December 2015

Technical Committee:

[OASIS Cyber Threat Intelligence (CTI) TC](https://www.oasis-open.org/committees/cti)

Chair:

Richard Struse ([Richard.Struse@HQ.DHS.GOV](mailto:Richard.Struse@HQ.DHS.GOV)), [DHS Office of Cybersecurity and Communications (CS&C)](http://www.dhs.gov/office-cybersecurity-and-communications)

Editors:

Desiree Beck ([dbeck@mitre.org](mailto:ikirillov@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Trey Darley ([trey@soltra.com](mailto:trey@soltra.com)), [Soltra](http://www.soltra.com/)

Ivan Kirillov ([ikirillov@mitre.org](mailto:ikirillov@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Rich Piazza ([rpiazza@mitre.org](mailto:ikirillov@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Additional artifacts:

This prose specification is one component of a Work Product which consists of:

* *CybOXTM Version 2.1.1 Part 1: Overview*. [URI]
* *CybOXTM Version 2.1.1 Part 2: Common*. [URI]
* *CybOXTM Version 2.1.1 Part 3: Core*. [URI]
* *CybOXTM Version 2.1.1 Part 4: Default Extensions*. [URI]
* *CybOXTM Version 2.1.1 Part 5: Vocabularies*. [URI]
* *CybOXTM Version 2.1.1 Part 6: UML Model*. [URI]
* *CybOXTM Version 2.1.1 Part 7: API Object*. [URI]
* *CybOXTM Version 2.1.1 Part 8: ARP Cache Object*. [URI]
* *CybOXTM Version 2.1.1 Part 9: AS Object*. [URI]
* *CybOXTM Version 2.1.1 Part 10: Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 11: Address Object*. [URI]
* *CybOXTM Version 2.1.1 Part 12: Archive File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 13: Artifact Object*. [URI]
* *CybOXTM Version 2.1.1 Part 14: Code Object*. [URI]
* *CybOXTM Version 2.1.1 Part 15: Custom Object*. [URI]
* *CybOXTM Version 2.1.1 Part 16: DNS Cache Object*. [URI]
* *CybOXTM Version 2.1.1 Part 17: DNS Query Object*. [URI]
* *CybOXTM Version 2.1.1 Part 18: DNS Record Object*. [URI]
* *CybOXTM Version 2.1.1 Part 19: Device Object*. [URI]
* *CybOXTM Version 2.1.1 Part 20: Disk Object*. [URI]
* *CybOXTM Version 2.1.1 Part 21: Disk Partition Object*. [URI]
* *CybOXTM Version 2.1.1 Part 22: Domain Name Object*. [URI]
* *CybOXTM Version 2.1.1 Part 23: Email Message Object*. [URI]
* *CybOXTM Version 2.1.1 Part 24: File Object*. (this document)
* *CybOXTM Version 2.1.1 Part 25: GUI Dialogbox Object*. [URI]
* *CybOXTM Version 2.1.1 Part 26: GUI Object*. [URI]
* *CybOXTM Version 2.1.1 Part 27: GUI Window Object*. [URI]
* *CybOXTM Version 2.1.1 Part 28: HTTP Object*. [URI]
* *CybOXTM Version 2.1.1 Part 29: Hostname Session Object*. [URI]
* *CybOXTM Version 2.1.1 Part 30: Image File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 31: Library File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 32: Link Object*. [URI]
* *CybOXTM Version 2.1.1 Part 33: Linux Package Object*. [URI]
* *CybOXTM Version 2.1.1 Part 34: Memory Object*. [URI]
* *CybOXTM Version 2.1.1 Part 35: Mutex Object*. [URI]
* *CybOXTM Version 2.1.1 Part 36: Network Connection Object*. [URI]
* *CybOXTM Version 2.1.1 Part 37: Network Flow Object*. [URI]
* *CybOXTM Version 2.1.1 Part 38: Network Packet Object*. [URI]
* *CybOXTM Version 2.1.1 Part 39: Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 40: Network Route Object*. [URI]
* *CybOXTM Version 2.1.1 Part 41: Network Socket Object*. [URI]
* *CybOXTM Version 2.1.1 Part 42: Network Subnet Object*. [URI]
* *CybOXTM Version 2.1.1 Part 43: PDF File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 44: Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 45: Port Object*. [URI]
* *CybOXTM Version 2.1.1 Part 46: Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 47: Product Object*. [URI]
* *CybOXTM Version 2.1.1 Part 48: SMS Message Object*. [URI]
* *CybOXTM Version 2.1.1 Part 49: Semaphore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 50: Socket Address Object*. [URI]
* *CybOXTM Version 2.1.1 Part 51: System Object*. [URI]
* *CybOXTM Version 2.1.1 Part 52: URI Object*. [URI]
* *CybOXTM Version 2.1.1 Part 53: URL History Object*. [URI]
* *CybOXTM Version 2.1.1 Part 54: Unix File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 55: Unix Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 56: Unix Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 57: Unix Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 58: Unix User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 59: Unix Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 60: User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 61: User Session Object*. [URI]
* *CybOXTM Version 2.1.1 Part 62: Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 63: Whois Object*. [URI]
* *CybOXTM Version 2.1.1 Part 64: Win Computer Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 65: Win Critical Section Object*. [URI]
* *CybOXTM Version 2.1.1 Part 66: Win Driver Object*. [URI]
* *CybOXTM Version 2.1.1 Part 67: Win Event Log Object*. [URI]
* *CybOXTM Version 2.1.1 Part 68: Win Event Object*. [URI]
* *CybOXTM Version 2.1.1 Part 69: Win Executable File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 70: Win File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 71: Win Filemapping Object*. [URI]
* *CybOXTM Version 2.1.1 Part 72: Win Handle Object*. [URI]
* *CybOXTM Version 2.1.1 Part 73: Win Hook Object*. [URI]
* *CybOXTM Version 2.1.1 Part 74: Win Kernel Hook Object*. [URI]
* *CybOXTM Version 2.1.1 Part 75: Win Kernel Object*. [URI]
* *CybOXTM Version 2.1.1 Part 76: Win Mailslot Object*. [URI]
* *CybOXTM Version 2.1.1 Part 77: Win Memory Page Region Object*. [URI]
* *CybOXTM Version 2.1.1 Part 78: Win Mutex Object*. [URI]
* *CybOXTM Version 2.1.1 Part 79: Win Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 80: Win Network Share Object*. [URI]
* *CybOXTM Version 2.1.1 Part 81: Win Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 82: Win Prefetch Object*. [URI]
* *CybOXTM Version 2.1.1 Part 83: Win Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 84: Win Registry Key Object*. [URI]
* *CybOXTM Version 2.1.1 Part 85: Win Semaphore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 86: Win Service Object*. [URI]
* *CybOXTM Version 2.1.1 Part 87: Win System Object*. [URI]
* *CybOXTM Version 2.1.1 Part 88: Win System Restore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 89: Win Task Object*. [URI]
* *CybOXTM Version 2.1.1 Part 90: Win Thread Object*. [URI]
* *CybOXTM Version 2.1.1 Part 91: Win User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 92: Win Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 93: Win Waitable Timer Object*. [URI]
* *CybOXTM Version 2.1.1 Part 94: X509 Certificate Object*. [URI]

Related work:

This specification is related to:

* *STIXTM Version 1.2.1 (placeholder)*

Abstract:

The Cyber Observable Expression (CybOX) is a standardized language for encoding and communicating high-fidelity information about cyber observables, whether dynamic events or stateful measures that are observable in the operational cyber domain. By specifying a common structured schematic mechanism for these cyber observables, the intent is to enable the potential for detailed automatable sharing, mapping, detection and analysis heuristics. This specification document defines the File Object data model, which is one of the Object data models for CybOX content.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

URI patterns:

Initial publication URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/csd01/part1-overview/stix-v1.2.1-csd01-part1-overview.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part1-overview.docx

(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2015. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Portions copyright © United States Government 2012-2015.  All Rights Reserved.  
  
STIX™, TAXII™, AND CybOX™ (STANDARD OR STANDARDS) AND THEIR COMPONENT PARTS ARE PROVIDED “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THESE STANDARDS OR ANY OF THEIR COMPONENT PARTS WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE STANDARDS OR THEIR COMPONENT PARTS WILL BE ERROR FREE, OR ANY WARRANTY THAT THE DOCUMENTATION, IF PROVIDED, WILL CONFORM TO THE STANDARDS OR THEIR COMPONENT PARTS. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THESE STANDARDS OR THEIR COMPONENT PARTS OR ANY PROVIDED DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE STANDARDS, THEIR COMPONENT PARTS, AND ANY PROVIDED DOCUMENTATION. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THE STANDARDS OR THEIR COMPONENT PARTS ATTRIBUTABLE TO ANY THIRD PARTY, IF PRESENT IN THE STANDARDS OR THEIR COMPONENT PARTS AND DISTRIBUTES IT OR THEM “AS IS.”

Table of Contents

[1 Introduction 6](#_Toc437950182)

[1.1 CybOXTM Specification Documents 6](#_Toc437950183)

[1.2 Document Conventions 6](#_Toc437950184)

[1.2.1 Fonts 6](#_Toc437950185)

[1.2.2 UML Package References 7](#_Toc437950186)

[1.2.3 UML Diagrams 7](#_Toc437950187)

[1.2.3.1 Class Properties 7](#_Toc437950188)

[1.2.3.2 Diagram Icons and Arrow Types 7](#_Toc437950189)

[1.2.4 Property Table Notation 8](#_Toc437950190)

[1.2.5 Property and Class Descriptions 8](#_Toc437950191)

[1.3 Terminology 9](#_Toc437950192)

[1.4 Normative References 9](#_Toc437950193)

[2 Background Information 10](#_Toc437950194)

[2.1 Cyber Observables 10](#_Toc437950195)

[2.2 Objects 10](#_Toc437950196)

[3 Data Model 11](#_Toc437950197)

[3.1 FileObjectType Class 11](#_Toc437950198)

[3.2 FilePathType Class 16](#_Toc437950199)

[3.3 FileAttributeType Class 16](#_Toc437950200)

[3.4 FilePermissionsType Class 17](#_Toc437950201)

[3.5 PackerListType Class 17](#_Toc437950202)

[3.6 PackerType Class 17](#_Toc437950203)

[3.7 PackerClassType Class 18](#_Toc437950204)

[3.8 EPJumpCodeType Class 18](#_Toc437950205)

[3.9 EntryPointSignatureListType Class 19](#_Toc437950206)

[3.10 EntryPointSignatureType Class 19](#_Toc437950207)

[3.11 SymLinksListType Class 20](#_Toc437950208)

[3.12 DetectedTypeEnum Enumeration 20](#_Toc437950209)

[3.13 PackerClassEnum Enumeration 20](#_Toc437950210)

[4 Conformance 22](#_Toc437950211)

[Acknowledgments 23](#_Toc437950212)

[Revision History 24](#_Toc437950213)

# Introduction

[All text is normative unless otherwise labeled]

The Cyber Observable Expression (CybOXTM) provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security. CybOX improves the consistency, efficiency, and interoperability of deployed tools and processes, and it increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics.

This document serves as the specification for the CybOX File Object Version 2.1.1 data model, which is one of eighty-eight CybOX Object data models.

In Section **1.1** we discuss additional specification documents, in Section **1.2** we provide document conventions, and in Section **1.3** we provide terminology. References are given in Section **1.4**. In Section **2**, we give background information necessary to fully understand the File Object data model. We present the File Object data model specification details in Section **3** and conformance information in Section **4**.

## CybOXTM Specification Documents

The CybOX specification consists of a formal UML model and a set of textual specification documents that explain the UML model. Specification documents have been written for each of the individual data models that compose the full CybOX UML model.

CybOX has a modular design comprising two fundamental data models and a collection of Object data models. The fundamental data models – CybOX Core and CybOX Common – provide essential CybOX structure and functionality. The CybOX Objects, defined in individual data models, are precise characterizations of particular types of observable cyber entities (e.g., HTTP session, Windows registry key, DNS query).

Use of the CybOX Core and Common data models is required; however, use of the CybOX Object data models is purely optional: users select and use only those Objects and corresponding data models that are needed. Importing the entire CybOX suite of data models is not necessary.

The [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) document provides a comprehensive overview of the full set of CybOX data models, which in addition to the Core, Common, and numerous Object data models, includes various extension data models and a vocabularies data model, which contains a set of default controlled vocabularies. [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) also summarizes the relationship of CybOX to other languages, and outlines general CybOX data model conventions.

## Document Conventions

The following conventions are used in this document.

### Fonts

The following font and font style conventions are used in the document:

* Capitalization is used for CybOX high level concepts, which are defined in [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts).

Examples: Action, Object, Event, Property

* The Courier New font is used for writing UML objects.

Examples: ActionType, cyboxCommon:BaseObjectPropertyType

Note that all high level concepts have a corresponding UML object. For example, the Action high level concept is associated with a UML class named, ActionType.

* The ‘*italic’* font (withsingle quotes) is used for noting actual, explicit values for CybOX Language properties. The *italic* font (without quotes) is used for noting example values.

Example:  *‘HashNameVocab-1.0,’ high, medium, low*

### UML Package References

Each CybOX data model is captured in a different UML package (e.g., Core package) where the packages together compose the full CybOX UML model. To refer to a particular class of a specific package, we use the format package\_prefix:class, where package\_prefix corresponds to the appropriate UML package. The [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) document contains the full list of CybOX packages, along with the associated prefix notations, descriptions, and examples.

The package\_prefix for the File data model is FileObj. Note that in this specification document, we do not explicitly specify the package prefix for any classes that originate from the File Object data model.

### UML Diagrams

This specification makes use of UML diagrams to visually depict relationships between CybOX Language constructs. Note that the diagrams have been extracted directly from the full UML model for CybOX; they have not been constructed purely for inclusion in the specification documents.  Typically, diagrams are included for the primary class of a data model, and for any other class where the visualization of its relationships between other classes would be useful.  This implies that there will be very few diagrams for classes whose only properties are either a data type or a class from the CybOX Common data model.  Other diagrams that are included correspond to classes that specialize a superclass and abstract or generalized classes that are extended by one or more subclasses.

In UML diagrams, classes are often presented with their attributes elided, to avoid clutter. The fully described class can usually be found in a related diagram. A class presented with an empty section at the bottom of the icon indicates that there are no attributes other than those that are visualized using associations.

#### Class Properties

Generally, a class property can be shown in a UML diagram as either an attribute or an association (i.e., the distinction between attributes and associations is somewhat subjective). In order to make the size of UML diagrams in the specifications manageable, we have chosen to capture most properties as attributes and to capture only higher level properties as associations, especially in the main top-level component diagrams. In particular, we will always capture properties of UML data types as attributes.

#### Diagram Icons and Arrow Types

Diagram icons are used in a UML diagram to indicate whether a shape is a class, enumeration, or a data type, and decorative icons are used to indicate whether an element is an attribute of a class or an enumeration literal. In addition, two different arrow styles indicate either a directed association relationship (regular arrowhead) or a generalization relationship (triangle-shaped arrowhead). The icons and arrow styles we use are shown and described in **Table 1‑1**.

Table 1‑1. UML diagram icons

|  |  |
| --- | --- |
| **Icon** | **Description** |
|  | This diagram icon indicates a class. If the name is in italics, it is an abstract class. |
|  | This diagram icon indicates an enumeration. |
|  | This diagram icon indicates a data type. |
|  | This decorator icon indicates an attribute of a class. The green circle means its visibility is public. If the circle is red or yellow, it means its visibility is private or protected. |
|  | This decorator icon indicates an enumeration literal. |
|  | This arrow type indicates a directed association relationship. |
|  | This arrow type indicates a generalization relationship. |

### Property Table Notation

Throughout Section **3**, tables are used to describe the properties of each data model class. Each property table consists of a column of names to identify the property, a type column to reflect the datatype of the property, a multiplicity column to reflect the allowed number of occurrences of the property, and a description column that describes the property. Package prefixes are provided for classes outside of the File Object data model (see Section **1.2.2**).

Note that if a class is a specialization of a superclass, only the properties that constitute the specialization are shown in the property table (i.e., properties of the superclass will not be shown). However, details of the superclass may be shown in the UML diagram.

### Property and Class Descriptions

Each class and property defined in CybOX is described using the format, “The X property verbY.” For example, in the specification for the CybOX Core data model, we write, “The id property specifies a globally unique identifier for the Action.” In fact, the verb “specifies” could have been replaced by any number of alternatives: “defines,” “describes,” “contains,” “references,” etc.

However, we thought that using a wide variety of verb phrases might confuse a reader of a specification document because the meaning of each verb could be interpreted slightly differently. On the other hand, we didn’t want to use a single, generic verb, such as “describes,” because although the different verb choices may or may not be meaningful from an implementation standpoint, a distinction could be useful to those interested in the modeling aspect of CybOX.

Consequently, we have preferred to use the three verbs, defined as follows, in class and property descriptions:

|  |  |
| --- | --- |
| **Verb** | **CybOX Definition** |
| captures | Used to record and preserve information without implying anything about the structure of a class or property. Often used for properties that encompass general content. This is the least precise of the three verbs. |
|  | *Examples*:  The Observable\_Source property characterizes the source of the Observable information. Examples of details captured include identifying characteristics, time-related attributes, and a list of the tools used to collect the information.  The Description property captures a textual description of the Action. |
| characterizes | Describes the distinctive nature or features of a class or property. Often used to describe classes and properties that themselves comprise one or more other properties. |
|  | *Examples*:  The Action property characterizes a cyber observable Action.  The Obfuscation\_Technique property characterizes a technique an attacker could potentially leverage to obfuscate the Observable. |
| specifies | Used to clearly and precisely identify particular instances or values associated with a property. Often used for properties that are defined by a controlled vocabulary or enumeration; typically used for properties that take on only a single value. |
|  | *Example*:  The cybox\_major\_version property specifies the major version of the CybOX language used for the set of Observables. |

## Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[**RFC2119**]**.

## Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

# Background Information

In this section, we provide high level information about the File Object data model that is necessary to fully understand the specification details given in Section **3**.

## Cyber Observables

A cyber observable is a dynamic event or a stateful property that occurs, or may occur, in the operational cyber domain. Examples of stateful properties include the value of a registry key, the MD5 hash of a file, and an IP address. Examples of events include the deletion of a file, the receipt of an HTTP GET request, and the creation of a remote thread.

A cyber observable is different than a cyber indicator. A cyber observable is a statement of fact, capturing what was observed or could be observed in the cyber operational domain. Cyber indicators are cyber observable patterns, such as a registry key value associated with a known bad actor or a spoofed email address used on a particular date.

## Objects

Objects in CybOX are individual data models for characterizing a particular cyber entity, such as a Windows registry key, or an Email Message. Accordingly, each release of the CybOX language includes a particular set of Objects that are part of the release. The data model for each of these Objects is defined by its own specification that describes the context-specific classes and properties that compose the Object.

# Data Model

## FileObjectType Class

The FileObjectType class is intended to characterize generic files. The UML diagram corresponding to the FileObjectType class is shown in **Figure 3‑1**.

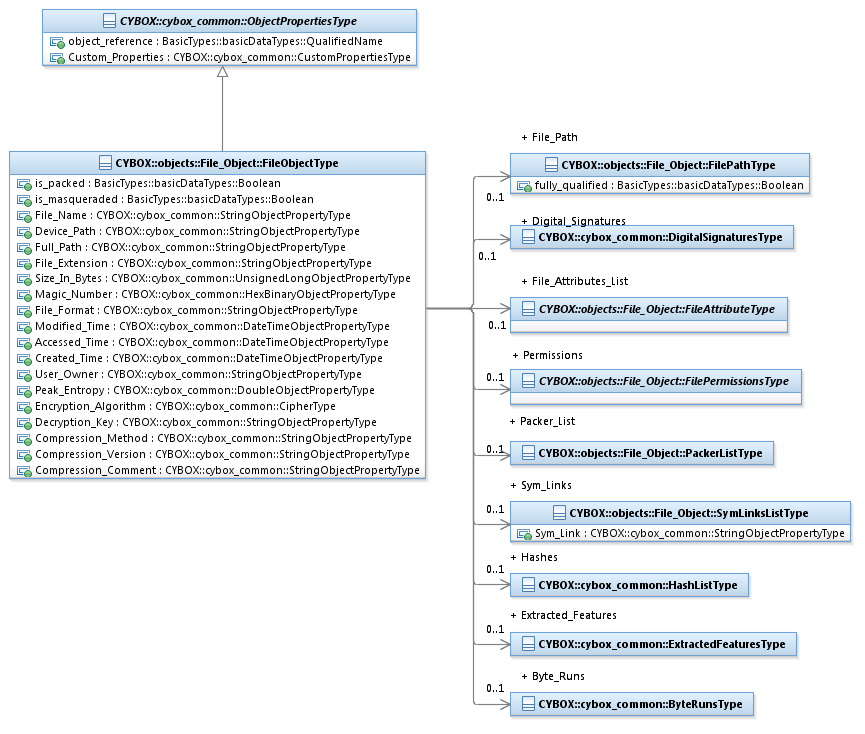


Figure 3‑1. UML diagram of the FileObjectType class

The property table of the FileObjectType class is given in **Table 3‑1**.

Table 3‑1. Properties of the FileObjectType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **is\_packed** | basicDataTypes:Boolean | 0..1 | The is\_packed property is used to indicate whether the file is packed or not. |
| **is\_masqueraded** | basicDataTypes:Boolean | 0..1 | The is\_masqueraded property specifies whether the file is masqueraded as another type of file; e.g., a PDF file that has had its extension changed to TXT to masquerade itself as a text file. |
| **File\_Name** | cyboxCommon:  StringObjectPropertyType | 0..1 | The File\_Name property specifies the base name of the file (including an extension, if present). |
| **File\_Path** | FilePathType | 0..1 | The File\_Path property specifies the relative or fully-qualified path to the file, not including the path to the device where the file system containing the file resides. Whether the path is relative or fully-qualified can be specified via the 'fully\_qualified' property. The File\_Path field may include the name of the file; if so, it must not conflict with the File\_Name field. If not, the File\_Path field should contain the path of the directory containing the file, and should end with a terminating path separator ("\" or "/"). |
| **Device\_Path** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Device\_Path property specifies the path to the physical device where the file system containing the file resides. |
| **Full\_Path** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Full\_Path property specifies the complete path to the file, including the device path. It should contain the contents that would otherwise be in the Device\_Path and File\_Path properties, and can be used in case the producer is unable or does not wish to separate the Device\_Path and File\_Path properties. If the Full\_Path property is specified along with the File\_Path and/or Device\_Path properties, it must not conflict with either. The Full\_Path property may include the name of the file; if so, it must not conflict with the File\_Name property. If not, the File\_Path property should contain the path of the directory containing the file, and should end with a terminating path separator ("\" or "/"). |
| **File\_Extension** | cyboxCommon:  StringObjectPropertyType | 0..1 | The File\_Extension property specifies the extension of the name of the file. The File\_Extension property must not conflict with the ending of the File\_Name property. The File\_Extension property should not begin with a "." character, but may contain a "." character in the case of a compound file extension, such as "tar.gz". |
| **Size\_In\_Bytes** | cyboxCommon:  UnsignedLongObjectPropertyType | 0..1 | The Size\_In\_Bytes property specifies the size of the file, in bytes. |
| **Magic\_Number** | cyboxCommon:  HexBinaryObjectPropertyType | 0..1 | The Magic\_Number property specifies the particular magic number (typically a hexadecimal constant used to identify a file format) corresponding to the file, if applicable. |
| **File\_Format** | cyboxCommon:  StringObjectPropertyType | 0..1 | The File\_Format property specifies the particular file format of the file, most typically specified by a tool such as the UNIX file command. |
| **Hashes** | cyboxCommon:  HashListType | 0..1 | The Hashes property specifies any hashes of the file. |
| **Digital\_Signatures** | cyboxCommon:  DigitalSignaturesType | 0..1 | The Digital\_Signatures property captures one or more digital signatures for the file. |
| **Modified\_Time** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Modified\_Time property specifies the date/time the file was last modified. |
| **Accessed\_Time** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Accessed\_Time property specifies the date/time the file was last accessed. |
| **Created\_Time** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Created\_Time property specifies the date/time the file was created. |
| **File\_Attributes\_List** | FileAttributeType | 0..1 | The File\_Attributes\_List property specifies the particular special attributes set for the file. Since this is a platform-specific Object property, it is defined here as an abstract type and then implemented in any platform specific derived file objects. |
| **Permissions** | FilePermissionsType | 0..1 | The Permissions property specifies that particular permissions that a file may have. Since this is a platform-specific Object property, it is defined here as an abstract type and then implemented in any platform specific derived file objects. |
| **User\_Owner** | cyboxCommon:  StringObjectPropertyType | 0..1 | The User\_Owner property specifies the name of the user that owns the file. |
| **Packer\_List** | PackerListType | 0..1 | The Packer\_List property specifies any packers that the file may be packed with. The term 'packer' here refers things like archivers and installers. |
| **Peak\_Entropy** | cyboxCommon:  DoubleObjectPropertyType | 0..1 | The Peak\_Entropy property specifies the calculated peak entropy of the file. |
| **Sym\_Links** | SymLinksListType | 0..1 | The Sym\_Links property specifies any symbolic links that may exist for the file. |
| **Byte\_Runs** | cyboxCommon:ByteRunsType | 0..1 | The Byte\_Runs property contains a list of byte runs from the raw file or its storage medium. |
| **Extracted\_Features** | cyboxCommon:  ExtractedFeaturesType | 0..1 | The Extracted\_Features property specifies a description of features extracted from this file. |
| **Encryption\_Algorithm** | cyboxCommon:CipherType | 0..1 | The Encryption\_Algorithm property specifies the algorithm used to encrypt the file. |
| **Decryption\_Key** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Decryption\_Key property specifies the key used to decrypt the file. |
| **Compression\_Method** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Compression\_Method property specifies the method used to compress the file. |
| **Compression\_Version** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Compression\_Version property specifies the version of the compression method used to compress the file. |
| **Compression\_Comment** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Compression\_Comment property specifies the comment string associated with the compressed file. |

## FilePathType Class

The FilePathType class specifies the path to the file, not including the device. Whether the path is relative or fully-qualified can be specified via the 'fully\_qualified' property.

The property table of the FilePathType class is given in **Table 3‑2**.

Table 3‑2. Properties of the FilePathType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **fully\_qualified** | basicDataTypes:Boolean | 0..1 | The fully\_qualified property specifies whether the path is fully qualified. |

## FileAttributeType Class

The FileAttributeType class specifies attribute(s) of a file. Since this is a platform-specific Object property, it is defined here as an abstract type.

## FilePermissionsType Class

The FilePermissionsType class specifies a permission of a file. Since this is a platform-specific Object property, it is defined here as an abstract type and then implemented in any platform specific derived file objects.

## PackerListType Class

The PackerListType class specifies a list of file packers.

The property table of the PackerListType class is given in **Table 3‑3**.

Table 3‑3. Properties of the PackerListType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Packer** | PackerType | 1..\* | The Packer property specifies a single file packer. |

## PackerType Class

The PackerType class specifies the fields that characterize a particular file packer, such as name and version. The UML diagram corresponding to the PackerType class is shown in Figure 3‑2.

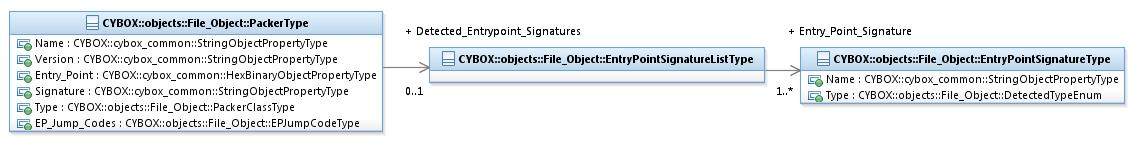


Figure 3‑2. UML diagram of the PackerType class

The property table of the PackerType class is given in **Table 3‑4**.

Table 3‑4. Properties of the PackerType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Name** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Name property specifies the name of the packer. |
| **Version** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Version property specifies the version of the packer. |
| **Entry\_Point** | cyboxCommon:  HexBinaryObjectPropertyType | 0..1 | The Entry\_Point property specifies the entry point address of the packer, if applicable. |
| **Signature** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Signature property specifies the matching signature detected for the packer, if applicable. |
| **Type** | PackerClassType | 0..1 | The Type property specifies the type of packer being characterized. |
| **Detected\_Entrypoint\_Signatures** | EntryPointSignatureListType | 0..1 | The Detected\_Entrypoint\_Signatures property specifies the entrypoint signatures that were detected for the packer. |
| **EP\_Jump\_Codes** | EPJumpCodeType | 0..1 | The EP\_Jump\_Codes property characterizes the entry point jump codes of the packer. |

## PackerClassType Data Type

The PackerCassType data type specifies the packer class. Its core value SHOULD be a literal from the PackerClassEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e. regular-expression based) specifications.

## EPJumpCodeType Class

The EPJumpCodeType class specifies an entry-point jump code used by a packer.

The property table of the EPJumpCodeType class is given in **Table 3‑5**.

Table 3‑5. Properties of the EPJumpCodeType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Depth** | cyboxCommon:  IntegerObjectPropertyType | 0..1 | The Depth property specified the frequency that a jump instruction is found to be immediately followed by another jump instruction within the PE (Portable Executable) entry point. |
| **Opcodes** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Opcodes property specifies the hex value of the bytes located at the jump location for a relative jump identified in the PE (Portable Executable) entry point up to 10 bytes or the end of the RVA (Relative Virtual Address) section. |

## EntryPointSignatureListType Class

The EntryPointSignatureListType class specifies a list of entry point signatures for a packer.

The property table of the EntryPointSignatureListType class is given in **Table 3‑6**.

Table 3‑6. Properties of the EntryPointSignatureListType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Entry\_Point\_Signature** | EntryPointSignatureType | 1..\* | The Entry\_Point\_Signature property specifies a single property in a list of entry point signatures. |

## EntryPointSignatureType Class

The EntryPointSignatureType class specifies an entry point signature for a packer.

The property table of the EntryPointSignatureType class is given in **Table 3‑7**.

Table ‑. Properties of the EntryPointSignatureType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Name** | cyboxCommon:StringObjectPropertyType | 0..1 | The Name property specifies the signature name. |
| **Type** | DetectedTypeEnum | 0..1 | The Type property specifies the type of entry point detected (e.g., packer, compiled file). |

## SymLinksListType Class

The SymLinksListType class specifies a list of symbolic links.

The property table of the SymLinksListType class is given in **Table 3‑8**.

Table 3‑8. Properties of the SymLinksListType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Sym\_Link** | cyboxCommon:  StringObjectPropertyType | 1..\* | The Sym\_Link property specifies a single symbolic link. |

## DetectedTypeEnum Enumeration

The literals of the DetectedTypeEnum enumeration are given in **Table 3‑9**.

Table 3‑9. Literals of the DetectedTypeEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **None** | Specifies a type other than those listed. |
| **Compiler** | Specifies an executable that acts as a compiler. |
| **Packer** | Specifies an executable that acts as a packer. |
| **Installer** | Specifies an executable that acts as an installer. |

## PackerClassEnum Enumeration

The literals of the PackerClassEnum enumeration are given in **Table 3‑10**.

Table 3‑10. Literals of the PackerClassEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **Archiver** | Indicates that the packer is an archiver. |
| **Installer** | Indicates that the packer is an installer. |
| **Self-Extracting Archiver** | Indicates that the packer is a self-extracting archiver. |
| **Crypter** | Indicates that the packer is a crypter. |
| **Packer** | Indicates a packer. |
| **Protector** | Indicates that the packer is a protector. |
| **Bundler** | Indicates that the packer is a bundler. |
| **Other** | Indicates a different type of packer from the ones listed. |

# Conformance

Implementations have discretion over which parts (components, properties, extensions, controlled vocabularies, etc.) of CybOX they implement (e.g., Observable/Object).

[1] Conformant implementations must conform to all normative structural specifications of the UML model or additional normative statements within this document that apply to the portions of CybOX they implement (e.g., implementers of the entire Observable class must conform to all normative structural specifications of the UML model regarding the Observable class or additional normative statements contained in the document that describes the Observable class).

[2] Conformant implementations are free to ignore normative structural specifications of the UML model or additional normative statements within this document that do not apply to the portions of CybOX they implement (e.g., non-implementers of any particular properties of the Observable class are free to ignore all normative structural specifications of the UML model regarding those properties of the Observable class or additional normative statements contained in the document that describes the Observable class).

The conformance section of this document is intentionally broad and attempts to reiterate what already exists in this document.

Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Dean Thompson, Australia and New Zealand Banking Group (ANZ Bank)

Bret Jordan, Blue Coat Systems, Inc.

Adnan Baykal, Center for Internet Security (CIS)

Liron Schiff, Comilion (mobile) Ltd.

Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)

Richard Struse, DHS Office of Cybersecurity and Communications (CS&C)

Ryusuke Masuoka, Fujitsu Limited

Eric Burger, Georgetown University

Jason Keirstead, IBM

Paul Martini, iboss, Inc.

Jerome Athias, Individual

Sanjiv Kalkar, Individual

Terry MacDonald, Individual

Alex Pinto, Individual

Patrick Maroney, Integrated Networking Technologies, Inc.

Wouter Bolsterlee, Intelworks BV

Joep Gommers, Intelworks BV

Sergey Polzunov, Intelworks BV

Rutger Prins, Intelworks BV

Andrei Sîrghi, Intelworks BV

Jonathan Baker, MITRE Corporation

Sean Barnum, MITRE Corporation

Mark Davidson, MITRE Corporation

Ivan Kirillov, MITRE Corporation

John Wunder, MITRE Corporation

Mike Boyle, National Security Agency

Jessica Fitzgerald-McKay, National Security Agency

Takahiro Kakumaru, NEC Corporation

John-Mark Gurney, New Context Services, Inc.

Christian Hunt, New Context Services, Inc.

Andrew Storms, New Context Services, Inc.

Igor Baikalov, Securonix

Bernd Grobauer, Siemens AG

John Anderson, Soltra

Trey Darley, Soltra

Paul Dion, Soltra

Brandon Hanes, Soltra

Ali Khan, Soltra

The authors would also like to thank the larger CybOX Community for its input and help in reviewing this document.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| wd01 | 15 December 2015 | Desiree Beck Trey Darley Ivan Kirillov Rich Piazza | Initial transfer to OASIS template |