CybOX v1.0 Release Notes

The Version 1.0 release of CybOX is a stabilization of the Version 1.0 (Draft) release intended as an initial major version of the CybOX language that can be utilized for practical operational use and integration into other standards efforts. This release includes several refinements, simplifications, fixes and additions in response to stakeholder feedback on Version 1.0 (Draft) from initial use and review. This release consists primarily of updates to the schemas from Version 1.0 (Draft) and six new defined object schemas along with updated Python bindings compliant with the new schemas. The formal language specifications for the core language content and defined objects content will be updated within the coming month to be aligned with the details of the Version 1.0 schemas.

The CybOX v1.0 XML schemas include a number of changes from v1.0 (Draft):

- Various localized restructuring and renaming for consistency and simplicity
- Numerous refinements and additions to the ObjectTypeEnum, ObjectRelationshipEnum, ActionTypeEnum, ActionRelationshipTypeEnum, DefinedArgumentNameEnum, and DefinedActionNameEnum
- Addition of several attributes to BaseObjectAttributesType to enable specification of obfuscation and defanging/refanging on any CybOX defined object field.
- 6 new defined object schemas added (Artifact, Network Connection, HTTP_Session, DNS_Query, WHOIS, Win_Memory_Page_Region)

Summary of changes from CybOX_v1.0 (Draft) to CybOX_v1.0:

CybOX Core:

- Modified
  - cybox::ActionType
    - Removed Action_Name structuree
    - Added "name" attribute which utilizes the cybox::DefinedActionNameEnum to replace the Action_Name structure and flatten the schema
    - Added "undefined_name" attribute
  - cybox::ActionRelationshipTypeEnum
    - Changed restriction base from cybox::RelationshipTypeEnum to xs:string
    - Added Initiated_By value
  - cybox::ActionTypeEnum
    - Added Inject value
    - Added Add value
    - Added Shutdown value
    - Added Sleep value

    - Added Revert value
    - Added Extract value
    - Added Uninstall value
    - Added Protect value
    - Added Change value
    - Added Check value

- cybox::ActionArgumentType
    - Changed Argument_Name_Defined element to @action_argument_defined attribute
    - Changed Argument_Name_Undefined element to @action_argument_undefined attribute
    - Changed Argument_Value element to @action_value attribute

- cybox::DefinedArgumentNameEnum
    - Added Protection value
    - Added Target PID value
    - Added Mapping Offset value
    - Added File Information Class value
    - Added Function Ordinal value
    - Added Function Name value
    - Added Hook Type value
    - Added Request Size value
    - Added Service Type value
    - Added Service State value
    - Added Group Name value
    - Added Hostname value
    - Added Shutdown Flag value
    - Added Sleep Time (ms) value
    - Added Code Address value
    - Added Parameter Address value
    - Added Server value

- cybox::DefinedActionNameEnum
    - Added Add Connection to Network Share value
    - Added Add Network Share value
    - Added Add System Call Hook value
    - Added Add User value
    - Added Add Windows Hook value
    - Added Connect to IP value
    - Added Connect to Network Share value
    - Added Connect to URL value
    - Added Create File Mapping value
    - Added Delete Network Share value
    - Added Delete User value
    - Added Disconnect from Network Share value

    - Added Download File value
    - Added Enumerate DLLs value
    - Added Enumerate Network Shares value
    - Added Enumerate System Handles value
    - Added Enumerate System Modules value
    - Added Enumerate Users value
    - Added Get Registry Key Attributes value
    - Added Get System Global Flags value
    - Added Get System Local Time value
    - Added Get System NetBIOS Name value
    - Added Get User Attributes value
    - Added Get Username value
    - Added Impersonate Thread value
    - Added Inject Memory Page value
    - Added Load and Call Driver value
    - Added Load Module value
    - Added Logon as User value
    - Added Map Library value
    - Added Map View of File value

- cybox::ObjectTypeEnum
    - Removed SQL Query value
    - Removed Role value
    - Removed Signature value
    - Removed Malware value
    - Removed Media value
    - Removed Named Pipe value
    - Removed Network value
    - Modified Registry Key/Key Group value
    - Modified Registry Hive value
    - Modified GUI Window value
    - Modified GUI Dialogbox value
    - Modified HTTP Session value
    - Modified Domain Name value
    - Added Address value
    - Added Artifact value
    - Added Code value
    - Added DNS Cache value
    - Added DNS Query value
    - Added Memory value
    - Added Product value
    - Added User Account value
    - Added Computer Account value
    - Added Driver value
    - Added Event value
    - Added Kernel value

        - Added Kernel Hook value
        - Added Prefetch value
        - Added Certificate value
        - Added URL value

- cybox::ObjectRelationshipEnum
    - Removed the following values
        - Decompressed_From
        - Decompressed_Into
        - Decrypted_From
        - Decrypted_Into
        - Joined_From
        - Joined_Into
        - Merged_From
        - Merged_Into
        - Sent_From
    - Added the following values
        - Allocated
        - Bound
        - Closed
        - Compressed
        - Compressed_From
        - Connected_From
        - Contains
        - Copied
        - Created
        - Decoded
        - Decompressed
        - Decrypted
        - Deleted
        - Downloaded
        - Dropped
        - Encoded
        - Encrypted
        - Encrypted_From
        - Freed
        - Hooked
        - Injected
        - Installed
        - Joined
        - Killed
        - Locked
        - Merged
        - Modified_Properties_Of
        - Monitored
        - Moved
        - Opened
        - Packed
        - Paused
        - Received
        - Renamed
        - Resumed
        - Sent
        - Set_From
        - Suspended
        - Unhooked
        - Unlocked
        - Unpacked
        - Received_Via_Upload
        - Uploaded_From
        - Uploaded
        - Wrote_To
        - Sub-domain_Of
        - Root_Domain_Of
        - FQDN_Of
        - Packed_From
        - Extracted_From
        - Previously_Contained
        - Sent_Via_Upload
        - Supra-domain_Of

        - Packed_Into

- Removed
    - cybox::ActionNameType
    - cybox::RelationshipTypeEnum

CybOX Common:

- Added
    - common::DigitalSignaturesType

- Modified
    - common::BaseObjectAttributeType
        - Added is_obfuscated attribute
        - Added obfuscation_algorithm_ref attribute
        - Added is_defanged attribute
        - Added defanging_algorithm_ref attribute
        - Added refanging_transformation_type attribute
        - Added reganging_transform attribute

    - common::MeasureSourceType
        - Removed Indicators element
        - Removed analysisMethod and analysisType attributes

    - common::RangeValueType
        - Added datatypes to union which defines how ranges are represented
            - xs:Name
            - xs:string
            - xs:hexBinary
            - xs:anyURI
            - xs:duration
            - xs:time
            - xs:base64Binary

- Removed/Renamed/Replaced datatypes or document-level elements
    - Removed common::IndicatorType
    - Removed common::IndicatorsType

CybOX Objects:

- New Objects:
    - Artifact_Object (created 2012-10-15)
    - Whois_Object (created 2012-09-12)
    - HTTP_Session_Object (initially created on 2012-09-14 as HTTP_Connection_Object)

- DNS_Query_Object (created 2012-09-17)
- Network_Connection_Object (created 2012-09-21)
- Win_Memory_Page_Region_Object (created 2012-10-12)

- Modified Objects
  - Process_Object
    - Removed Path element from ProcessObj::ProcessObjectType
    - Removed Current_Working_Directory element from ProcessObj::ProcessObjectType
    - Added File_Name element to ProcessObj::ImageInfoType
  - Email_Message_Object
    - Added Links element to EmailMessageObj::EmailMessageObjectType
  - Win_Event_Object
    - Renamed WinEventObj::EventType to WinEventObj::WinEventType
    - Renamed WinEventObj::EventTypeEnum to WinEventObk::WinEventTypeEnum
  - Win_Executable_File_Object
    - Removed CharacterEncodingObject (already defined in Common)
    - Encoding element references common::CharacterEncoding
    - Added VersionInfo resource type through resource substitution group
  - Win_Driver_Object
    - Renamed WinDriverObj::Device_Object to WinDriverObj::Device_Object_Struct
    - Renamed WinDriverObj::DeviceObjectType to WinDriverObj::DeviceObjectStructType to avoid conflict with cybox::DeviceObjectType
  - Unix_Process_object
    - Renamed UnixProcessObj::ProcessStatusType to UnixProcessObj::ProcessStateType
    - Renamed UnixProcessObj::ProcessStatusEnum to UnixProcessObj::ProcessStateEnum
  - File_Object
    - Removed FileObj::DigitalSignaturesType
    - Changed type of Digitial_Signatures to common::DigitalSignaturesType
    - Changed the type for File_Attributes_List in FileObj::FileObjectType
      - to the abstract FileObj::FileAttributeType directly and removed the
      - FileObj::FileAttributeListType.
    - Renamed FileObj::PackerAttributesType to FileObj::PackerType
    - Renamed FileObj::PackerType to FileObj::PackerClassType
    - Renamed FileObj::PackerTypeEnum to FileObj::PackerClassEnum
    - Added Magic_Number element to FileObj::FileObjectType
    - Added File_Format element to FileObj::FileObjectType
  - User_Account_Object

        - Removed User_ID field from UserAccountObj::UserAccountObjectType
    - Win_Task_Object:
        - Changed WinTaskObj::ActionType to WinTaskObj::ActionTaskTypeType to deconflict with cybox::ActionType
    - X509_Certificate_Object
        - Broke out inline complextypes into global complextypes
            - Created X509CertificateObj::RSAPublicKeyType

Detailed changes from CybOX_v1.0 (Draft) to CybOX_v1.0:

- Detailed difference reports are available for each individual schema at http://cybox.mitre.org/XMLSchema/release_notes/cybox_v1.0_diff_reports.zip