XML Examples for DHZM

DHZM-Examples

Version 2021-JAN

January 15, 2021

Table of Contents

Chapter 1 - Introduction 1
1.1 - Purpose 1
Chapter 2 - Example Files 2
2.1 - DHZM_TDO_commercial.xml 2

Chapter 1 - Introduction

1.1 - Purpose

This is an informative supplement for DHZM. This document provides concrete examples of XML files implementing DHZM elements and attributes.

Chapter 2 - Example Files

2.1 - DHZM_TDO_commercial.xml

```
<?xml-model href="../../Schematron/DHZM/DHZM_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?>
<?xml-model href="../../Schematron/DHZMC-TDF/DHZMC-TDF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?>
<?xml-model href="../../Schematron/BASE-TDF/BASE-TDF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?>
<?xml-model href="../../Schematron/IC-SF/IC-SF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?>
<tdf:TrustedDataObject xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                    xmlns:tdf="urn:us:gov:ic:tdf"
                                    xmlns:dhzm="urn:us:gov:ic:digitalhazmat"
                                    xmlns:sign="http://www.w3.org/2000/09/xmldsig#"
                                    xmlns:icsfhashv="urn:us:gov:ic:sf:hashverification"
                                    xmlns:icsf="urn:us:gov:ic:sf"
                                    xmlns="urn:us:gov:ic:tdf"
                                    xsi:schemaLocation="urn:us:gov:ic:tdf ../../Schema/DHZMC-TDF/DHZMC-TDF.xsd                                    urn:us:gov:ic:digitalhazmat ../../
Schema/DHZM/DHZM.xsd                                    urn:us:gov:ic:sf:hashverification ../../Schema/IC-SF/HashVerification.xsd"
                                    tdf:version="202101-DHZMC-TDF.202101">
                  <tdf:Assertion tdf:scope="PAYL">
                     <tdf:StructuredStatement>
                        <dhzm:ProvenanceAssertion dhzm:DESVersion="202101" icsf:DESVersion="202101">
                           <dhzm:DigitalHazMat>This element describes an obfuscated payload which is either known or suspected to
         contain software or similar data which could cause harm to information processing systems.
         It has been encapsulated to render it inert. Any attempt to decode this payload outside a safe
         analysis environment may pose a danger to your system.</dhzm:DigitalHazMat>
                           <dhzm:ContentCollectionTimestamp>2019-01-17T09:00:00Z</dhzm:ContentCollectionTimestamp>
                           <dhzm:ContentSize>100</dhzm:ContentSize>
                           <icsfhashv:ContentDecodedHashVerification icsfhashv:hashType="SHA-256">
                              <icsfhashv:PayloadHash>4355a46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865</icsfhashv:PayloadHash>
                           </icsfhashv:ContentDecodedHashVerification>
                           <dhzm:ContentEncodedSize>100</dhzm:ContentEncodedSize>
                           <dhzm:ContentEncodingMethod>XOR</dhzm:ContentEncodingMethod>
                           <icsfhashv:ContentEncodedHashVerification icsfhashv:hashType="SHA-256">
                              <icsfhashv:TotalHash icsfhashv:blockSize="134217728" icsfhashv:totalBlocks="2">53c234e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3</
icsfhashv:TotalHash>
                              <icsfhashv:BlockHash icsfhashv:block="1">e0642c608aa3e28350cebc98e47dfe784f966bd027ea376b7d4700fe6b07ea3d</icsfhashv:BlockHash>
                              <icsfhashv:BlockHash icsfhashv:block="2">e6b98e46bd027ea376b7d47dc0758a48a4f96e68fe78e064700f700fe6b07ea3</icsfhashv:BlockHash>
                           </icsfhashv:ContentEncodedHashVerification>
                        </dhzm:ProvenanceAssertion>
                     </tdf:StructuredStatement>
                  </tdf:Assertion>
                  <tdf:Assertion tdf:scope="PAYL">
                     <tdf:StructuredStatement>
                        <dhzm:AnalysisAssertion dhzm:DESVersion="202101" icsf:DESVersion="202101">
                           <dhzm:DigitalHazMat>This element describes an obfuscated payload which is either known or suspected to
         contain software or similar data which could cause harm to information processing systems.
         It has been encapsulated to render it inert. Any attempt to decode this payload outside a safe
         analysis environment may pose a danger to your system.</dhzm:DigitalHazMat>
                           <dhzm:OriginContentFilename>SuperBadDigitalHazMat</dhzm:OriginContentFilename>
                           <icsfhashv:ContentDecodedHashVerification icsfhashv:hashType="SHA-256">
                              <icsfhashv:PayloadHash>839ba46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865</icsfhashv:PayloadHash>
                           </icsfhashv:ContentDecodedHashVerification>
```

```
            <dhzm:KnownMalicious>true</dhzm:KnownMalicious>
            <dhzm:AnalysisMethod>Virus_Scan</dhzm:AnalysisMethod>
            <dhzm:AnalysisMethodToolList>
               <dhzm:AnalysisMethodTool>
                  <dhzm:AnalysisMethodToolName>ManualAnalysis</dhzm:AnalysisMethodToolName>
               </dhzm:AnalysisMethodTool>
               <dhzm:AnalysisMethodTool>
                  <dhzm:AnalysisMethodToolName>cpe:/a:nsa:ghidra:9.0</dhzm:AnalysisMethodToolName>
               </dhzm:AnalysisMethodTool>
               <dhzm:AnalysisMethodTool>
                  <dhzm:AnalysisMethodToolName>Other:cpe:/a:nsa:superghidra:10.0</dhzm:AnalysisMethodToolName>
               </dhzm:AnalysisMethodTool>
            </dhzm:AnalysisMethodToolList>
         </dhzm:AnalysisAssertion>
      </tdf:StructuredStatement>
   </tdf:Assertion>
   <tdf:EncryptionInformation>
      <tdf:KeyAccess>
         <tdf:AttachedKey>
            <tdf:KeyValue>abcdefghijklmnop</tdf:KeyValue>
         </tdf:AttachedKey>
      </tdf:KeyAccess>
      <tdf:EncryptionMethod tdf:algorithm="SHA-256"/>
   </tdf:EncryptionInformation>
   <tdf:ReferenceValuePayload tdf:uri="bitcionstealer.gz.enc"
                              tdf:mediaType="application/octet-stream"
                              tdf:isEncrypted="true">
      <ReferenceValueBlock tdf:uri="bitcionstealer.gz.enc.p01" icsfhashv:block="1"/>
      <ReferenceValueBlock tdf:uri="bitcionstealer.gz.enc.p02" icsfhashv:block="2"/>
      <icsfhashv:ContentEncodedHashVerification icsfhashv:hashType="SHA-256">
         <icsfhashv:TotalHash icsfhashv:blockSize="134217728" icsfhashv:totalBlocks="2">a8cd34e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3</icsfhashv:TotalHash>
         <icsfhashv:BlockHash icsfhashv:block="1">e1232c608aa3e28350cebc98e47dfe784f966bd027ea376b7d4700fe6b07ea3d</icsfhashv:BlockHash>
         <icsfhashv:BlockHash icsfhashv:block="2">f9fa8e46bd027ea376b7d47dc0758a48a4f96e68fe78e064700f700fe6b07ea3</icsfhashv:BlockHash>
      </icsfhashv:ContentEncodedHashVerification>
      <icsfhashv:ContentDecodedHashVerification icsfhashv:hashType="SHA-256">
         <icsfhashv:TotalHash icsfhashv:blockSize="134217728" icsfhashv:totalBlocks="2">1e9e34e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3</icsfhashv:TotalHash>
         <icsfhashv:BlockHash icsfhashv:block="1">4e5e608aa3e28350cebc98e47dfe784f966bd027ea376b7d4700fe6b07ea3d</icsfhashv:BlockHash>
         <icsfhashv:BlockHash icsfhashv:block="2">2e3e8e46bd027ea376b7d47dc0758a48a4f96e68fe78e064700f700fe6b07ea3</icsfhashv:BlockHash>
      </icsfhashv:ContentDecodedHashVerification>
   </tdf:ReferenceValuePayload>
</tdf:TrustedDataObject>
```