# STIX Use Case Examples

**Sean Barnum, Bryan Worrell, John Mazella, John Wunder**

**February 20, 2014**

**Version 1.1, Revision 1**

MITRE

# Abstract

The Structured Threat Information eXpression (STIX™) provides a structured language for the expression of cyber threat information. This document walks through example use cases demonstrating how they might leverage STIX.

# Trademark Information



This technical data was produced for the U. S. Government under Contract No. HSHQDC-11-J-00221, and is subject to the Rights in Technical Data-Noncommercial Items clause at DFARS 252.227-7013 (NOV 1995)



# Feedback

Community input is necessary for the success of STIX. Feedback on this or any of the other STIX work product is welcome and can be sent to stix@mitre.org. Comments, questions, suggestions, and concerns are all appreciated.

# Record of Changes [delete if not used]

| No. | Date | Reference | A=Add M=Modify D=Delete | Description of Change |
|---|---|---|---|---|
| 1 | 18 Feb 2014 | N/A | A | Created reformatted version |
| 2 | 19 Feb 2014 | N/A | M | Updated to STIX Version 1.1 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

# 1 Use Cases

This document provides use case-centric demonstrative examples for how the STIX language may be used to support various use cases within the cyber threat intelligence and information sharing context. These examples are typically simple in nature and do not convey the full expressivity or flexibility of the STIX language. The examples demonstrate only a single way to express the information in each example. Due to the inherent flexibility of the STIX language, there are often other ways to express the information as well. The examples typically include some prose describing use case activities, XML snippets of STIX content, and fully validated STIX content documents (included in the Appendices).

This document currently outlines the Phishing use case but will evolve going forward to include other relevant use cases.

## 1.1 Phishing

### 1.1.1 Premise

Phishing is an attempt by an individual or group to solicit personal information from or otherwise compromise unsuspecting users by employing social engineering techniques typically via email. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate or an unknowingly compromised legitimate site, or to open a malicious attachment. The user then may be asked to provide personal information such as account usernames and passwords that can further expose them to future compromises or may be directly compromised via malware on the site or within a malicious attachment. Phishing is one of the most common forms of malicious cyber attack and is of great concern to all organizations.

### 1.1.2 Current Practice

Current practice for phishing management is typically something like:

- Individual receives an email that they consider suspicious
- The email recipient forwards the email (typically with original email attached) to some sort of suspicious@XXX.YYY email address for their organization.
- A threat analyst comes in each morning to an inbox full of reported emails and must go through them to determine if they are malicious and then determine and carry out appropriate courses of action for recovery, cleaning up and blocking future attacks. This typically involves a lengthy list of analysis activities (outlined below) that are very manual and time consuming. This leads to a limitation on the volume of suspicious emails that can be analyzed, the depth of rigor that can often be applied and means that they are often evaluated without a meaningfully prioritized order.
- Appropriate recovery, cleanup and blocking courses of action are determined and executed.

#### 1.1.2.1 Analysis

The following flow of activity describes a typical current-practice process for analyzing and managing reported suspicious email for phishing attempts. Analyst activities would typically include but not be limited to things like:

- Look to see if the email is the same as malicious emails seen before. This may be some sort of query against a repository or simply the memory of the analyst.
- Look to see if the email contains any attachments or embedded URLs
- Open the raw email to analyze the structure for things like To, From, Subject, Date, Message ID, Content Type, MIME Version, X-Mailer, etc. looking for anything phishy.
- Compute characteristics for any attached files (file type, size, hashes, etc.).
- Run file hashes against reputation services.
- Run files through static triage tools looking for suspicious or known bad characteristics
- Run files through dynamic sandbox tools for suspicious or known bad behaviors
- Copy URLs out of email body and run them against URL reputation services (maybe even google them).
- Examine the URLs to extract the relevant domain name
- Run domain name against reputation services
- Run WHOIS on the domain name
- Research to see if registrant info for domain name is known bad actor
- Run DNS Query on domain name to determine resolved IP address
- Run IP address against reputation services
- Search to determine if domain names or IP addresses were involved in past known bad activity

If an email is determined by the analyst to be malicious they will typically:

- Investigate to see if the recipient opened the attachments or clicked on the URLs
- Search for other instances where such emails were received in their organization.
- Search for similar emails received in their organization (including historical)
- Determine and execute the appropriate recovery and cleanup courses of action
- Determine and execute the appropriate blocking courses of action

#### 1.1.2.2 Sharing

Current sharing of phishing threat information is most typically in the form of short textual messages describing what email characteristics were observed and often conveyed to sharing partners via person-to-person email or via some form of portal. In some cases, structured representations may be used but they are typically very limited in expressivity and localized exclusively to only the phishing context limiting their value within broader cyber threat intelligence. The format of the shared data is typically such that it cannot be automatically ingested, analyzed or acted on.

### 1.1.3 Potential STIX-enabled Practice

The basic flow of activity for STIX-enabled phishing management is very similar to the current practice flow but far more time-effective, productive, efficient, automated, consistent and structured. A large majority of the analysis activities performed manually by the analyst can be performed in an automated and apriori/background fashion utilizing STIX. This means that the analyst can be presented with reported suspicious emails that have already undergone automated first-order and potentially second-order analysis from the start giving the analyst a risk-prioritized list of analysis targets and lets the analyst's time be focused on more meaningful and relevant analysis activities. The information is all captured in a consistently structured fashion that significantly improves the ease of capturing, analyzing, storing, querying and sharing such information. The structured representations of the information are also consistent with structured threat information from many other use cases enabling analysis and correlation of information beyond the context of phishing analysis and across the broad scope of cyber threat intelligence and information sharing. The structured representations of the information also enable much more powerful automated sharing of threat information among chosen partners in a secure fashion.

NOTE: ID fields in STIX and CybOX are represented as Qualified Names (QNames) which are composed of a namespace prefix followed by a colon followed by a postfix string. For STIX and CybOX the prefix namespace should be a value unique to the producer of the identified content. For STIX and CybOX the postfix string should contain a globally unique identifier (GUID) beginning with an alphabetic character. For the ID fields in this example STIX and CybOX XML content, prefix and postfix naming conventions were arbitrarily chosen and do not indicate that these values or conventions must be used by any entity leveraging STIX or CybOX.

#### 1.1.1.1 Analysis

The following flow of activity describes a typical potential STIX-enabled process for analyzing and managing reported suspicious email for phishing attempts. This flow of activity is adorned throughout with actual STIX and CybOX snippets of XML content intended to demonstrate how STIX can be leveraged to support the phishing analysis use case. For fully validated content that integrates the various snippets from this activity flow see Appendix A.

##### *1.1.3.1.1 Suspicious e-mail is received*

A suspicious email is received by an individual within organization XXX.

##### *1.1.3.1.2 E-mail recipient forwards e-mail to suspicious@XXX.YYY*

The email recipient decides that the email is suspicious and forwards it to suspicious@XXX.YYY for analysis by the XXX.YYY threat analysis cell. A text file version of the example email is provided below. The email for this example is a standard email with a single file attachment and with two URLs in the body. In this case, one of the URLs is an active link (href) and the other is a valid URL but only used as the label for the active URL. The bulk of the encoded content for the attached file has been cut out for space purposes.

```
Delivered-To: jsmith@gmail.com
Received: by 10.236.111.46 with SMTP id v34cs581528yhg;
        Wed, 5 Jan 2011 12:48:37 -0800 (PST)
```

```
Received: by 10.142.11.2 with SMTP id 2mr253515wfk.275.1294232332935;
        Wed, 05 Jan 2011 12:48:35 -0800 (PST)
Received: from ccccc-ddddd ([113.28.117.3])
        by mx.google.com with ESMTP id p7si32937473wfl.41.2011.01.05.04.58.51;
        Wed, 05 Jan 2011 12:48:37 -0800 (PST)
Received-SPF: neutral (google.com: 113.28.117.3 is neither permitted nor denied by best guess
record for domain of jdoe@state.gov) client-ip=113.28.117.3;
Authentication-Results: mx.google.com; spf=neutral (google.com: 113.28.117.3 is neither
permitted nor denied by best guess record for domain of jdoe@state.gov)
smtp.mail=jdoe@state.gov
Received: from mail pickup service by ccccc-ddddd with Microsoft SMTPSVC;
        Wed, 5 Jan 2011 12:48:30 +0800
Thread-Topic: Draft US-China Joint Statement
From: "Jane Doe" <jdoe@state.gov>
To: "Joe Smith" <jsmith@gmail.com>
Subject: Fw:Draft US-China Joint Statement
Date: Wed, 5 Jan 2011 12:48:50 +0800
Message-ID: <CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com>
X-Mailer: Microsoft CDO for Windows 2000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4721
X-OriginalArrivalTime: 05 Jan 2011 12:48:37 (UTC) FILETIME=[ED3C28C0:01CBACD7]
Content-Type: multipart/mixed; boundary=90e6ba10b0e7fbf25104cdd9ad08
MIME-Version: 1.0

--90e6ba10b0e7fbf25104cdd9ad08
Content-Type: multipart/alternative; boundary=90e6ba10b0e7fbf24904cdd9ad06

--90e6ba10b0e7fbf24904cdd9ad06
Content-Type: text/plain; charset=ISO-8859-1

This is the latest version of State's joint statement. My understanding is
that State put in placeholder econ language and am happy to have us fill in
but in their rush to get a cleared version from the WH, they sent the
attached to Mike. If the attachment doesn't go through, download it here:
http://www.state.gov/public/01aff0dc/Joint_Statement.pdf<http://bhsxeozfiwqj.net/links/p2ioda
jfpoajsfafh.php>

Regards,
Jane Doe

--90e6ba10b0e7fbf24904cdd9ad06
Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

<div>This is the latest version of State&#39;s joint statement. My understa=
nding=A0is that State put in placeholder econ language and am happy to have=
 us=A0fill in but in their rush to get a cleared version from the WH, they=
=A0sent the attached to Mike. If the attachment doesn&#39;t go through, dow=
nload it here: <a href=3D"http://bhsxeozfiwqj.net/links/p2iodajfpoajsfafh.p=
hp">http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</a></div>
<div><br></div><div>Regards,</div><div>Jane Doe</div><div><br></div>

--90e6ba10b0e7fbf24904cdd9ad06--
--90e6ba10b0e7fbf25104cdd9ad08
Content-Type: application/pdf; name="Joint_Statement.pdf"
Content-Disposition: attachment; filename="Joint_Statement.pdf"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_h97hmd9k0

JVBERi0xLjMKJcTl8uXrp/Og0MTGCjQgMCBvYmoKPDwgL0xlbmd0aCA1IDAgUiAvRmlsdGVyIC9G
bGF0ZURlY29kZSA+PgpzdHJlYW0KeAG9ndmuLMtxnu/7KdrzObbVrHm4NAkRhgEDFrjvLF/I25YH
```

```
                                                …
PGQ1NmRiZmU5NzBhNzdhODMyZDUyMTc5NzUwNGI3YTZmPgo8ZDU2ZGJmZTk3MGE3N2E4MzJkNTIx
Nzk3NTA0YjdhNmY+IF0gPj4Kc3RhcnR4cmVmCjg1NTA0CiUlRU9GCg==
--90e6ba10b0e7fbf25104cdd9ad08--
```

#### 1.1.3.1.3 The suspicious e-mail is processed with Email_to_CybOX

The suspicious email received in the suspicious@XXX.YYY Inbox is automatically processed with the Email_to_CybOX utility in the background. A comprehensive package of structured CybOX content is generated which characterizes the suspicious email including some derivative automated background analysis.

The package includes the following Observable Objects with all of the appropriate defined relationships between them:

- a fully structured representation of the email itself (CybOX Email_Message object)
- for each attachment:
  - a structured capture of the raw file itself (CybOX Artifact object)
  - a structured characterization of the properties of the file (CybOX File object)
- for each URL/link embedded in the email itself:
  - a structured capture of the URL (CybOX URI object)
  - a structured capture of the domain name of the URL (CybOX Domain object)
  - a structured capture of the results of a WHOIS lookup performed on the domain name (CybOX WHOIS object)
  - a structured capture of a DNS Query (Type A Record) run on the domain name (CybOX DNSQuery object)
  - a structured capture of the DNS Record (Type A Record) resulting from the DNS Query run on the domain name (CybOX DNSRecord object)
  - a structured capture of the resolving IP address for the domain name resulting from the (Type A Record) DNS Query (CybOX Address object) a structured capture of a DNS Query (Type AAAA Record) run on the domain name (CybOX DNSQuery object)
  - a structured capture of the DNS Record (Type AAAA Record) resulting from the DNS Query run on the domain name (CybOX DNSRecord object)
  - a structured capture of the resolving IP address for the domain name resulting from the (Type AAAA Record) DNS Query (CybOX Address object)

1. Structured CybOX Email Message Object

Note the relationships (within the Related_Objects construct near the end) with the objects representing the attached file and the embedded URLs. Similar relationships between objects can be observed throughout the example content.

```
<cybox:Observable id="cybox:observable-6f45ce72-30c8-11e2-8011-000c291a73d5">
    <cybox:Object id="cybox:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
        <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
            <EmailMessageObj:Header>
```

```
                <EmailMessageObj:To>
                    <EmailMessageObj:Recipient category="e-mail">
                        <AddressObj:Address_Value>jsmith@gmail.com</AddressObj:Address_Value>
                    </EmailMessageObj:Recipient>
                </EmailMessageObj:To>
                <EmailMessageObj:From category="e-mail">
                    <AddressObj:Address_Value>jdoe@state.gov</AddressObj:Address_Value>
                </EmailMessageObj:From>
                <EmailMessageObj:Subject>Fw:Draft US-China Joint
Statement</EmailMessageObj:Subject>
                <EmailMessageObj:Date>2011-01-05T12:48:50+08:00</EmailMessageObj:Date>

<EmailMessageObj:Message_ID>CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.co
m</EmailMessageObj:Message_ID>
                <EmailMessageObj:Content_Type>multipart/mixed;
boundary=90e6ba10b0e7fbf25104cdd9ad08</EmailMessageObj:Content_Type>
                <EmailMessageObj:MIME_Version>1.0</EmailMessageObj:MIME_Version>
                <EmailMessageObj:X_Mailer>Microsoft CDO for Windows
2000</EmailMessageObj:X_Mailer>
            </EmailMessageObj:Header>
            <EmailMessageObj:Raw_Body><![CDATA[ This is the latest version of State's joint
statement. My understanding is that State put in placeholder econ language and am happy to
have us fill in but in their rush to get a cleared version from the WH, they sent the
attached to Mike. If the attachment doesn't go through, download it here:

       http://www.state.gov/public/01aff0dc/Joint_Statement.pdf<http://bhsxeozfiwqj.net/links
/p2iodajfpoajsfafh.php>

Regards,
Jane Doe

<div>This is the latest version of State&#39;s joint statement. My understa=
nding=A0is that State put in placeholder econ language and am happy to have=
us=A0fill in but in their rush to get a cleared version from the WH, they=
=A0sent the attached to Mike. If the attachment doesn&#39;t go through, dow=
nload it here: <a
href=3D"http://bhsxeozfiwqj.net/links/p2iodajfpoajsfafh.p=hp">http://www.state.gov/public/01a
ff0dc/Joint_Statement.pdf</a></div>
       <div><br></div><div>Regards,</div><div>Jane Doe</div><div><br></div>
]]></EmailMessageObj:Raw_Body>
            <EmailMessageObj:Raw_Header><![CDATA[ Delivered-To: jsmith@gmail.com
Received: by 10.236.111.46 with SMTP id v34cs581528yhg;
Wed, 5 Jan 2011 12:48:37 -0800 (PST)
Received: by 10.142.11.2 with SMTP id 2mr253515wfk.275.1294232332935;
Wed, 05 Jan 2011 12:48:35 -0800 (PST)
Received: from ccccc-ddddd ([113.28.117.3])
by mx.google.com with ESMTP id p7si32937473wfl.41.2011.01.05.04.58.51;
Wed, 05 Jan 2011 12:48:37 -0800 (PST)
Received-SPF: neutral (google.com: 113.28.117.3 is neither permitted nor denied by best guess
record for domain of jdoe@state.gov) client-ip=113.28.117.3;
Authentication-Results: mx.google.com; spf=neutral (google.com: 113.28.117.3 is neither
permitted nor denied by best guess record for domain of jdoe@state.gov)
smtp.mail=jdoe@state.gov
Received: from mail pickup service by ccccc-ddddd with Microsoft SMTPSVC;
Wed, 5 Jan 2011 12:48:30 +0800
Thread-Topic: Draft US-China Joint Statement
From: "Jane Doe" <jdoe@state.gov>
To: "Joe Smith" <jsmith@gmail.com>
Subject: Fw:Draft US-China Joint Statement
Date: Wed, 5 Jan 2011 12:48:50 +0800
Message-ID: <CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com>
```

```
X-Mailer: Microsoft CDO for Windows 2000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4721
X-OriginalArrivalTime: 05 Jan 2011 12:48:37 (UTC) FILETIME=[ED3C28C0:01CBACD7]
Content-Type: multipart/mixed; boundary=90e6ba10b0e7fbf25104cdd9ad08
MIME-Version: 1.0
]]></EmailMessageObj:Raw_Header>
            <EmailMessageObj:Attachments>
                <EmailMessageObj:File  object_reference="cybox:object-6dcae276-30c8-11e2-
8011-000c291a73d5"/>
            </EmailMessageObj:Attachments>
            <EmailMessageObj:Links>
                <EmailMessageObj:Link object_reference="cybox:object-6dcb5fda-30c8-11e2-8011-
000c291a73d5"/>
                <EmailMessageObj:Link object_reference="cybox:object-6ec9050e-30c8-11e2-8011-
000c291a73d5"/>
            </EmailMessageObj:Links>
        </cybox:Properties>
        <cybox:Related_Objects>
            <cybox:Related_Object idref="cybox:object-cb0ec4ad-4a39-4d4b-934b-72ff0563476f">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object><!-- File  -->
            <cybox:Related_Object idref="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object><!-- Artifact  -->
            <cybox:Related_Object idref="cybox:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object><!-- URL  -->
            <cybox:Related_Object idref="cybox:object-fa7efe7f-e1b4-45de-ba7e-c6a7d625c9d8">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object><!-- URL  -->
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

2. File attachments
    a. File object for the single attached file

```
<cybox:Observable id="cybox:observable-0a41ab04-f6ca-4bc7-93e1-0efbad2119da">
    <cybox:Object id="cybox:object-cb0ec4ad-4a39-4d4b-934b-72ff0563476f">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
            <FileObj:File_Name>Joint_Statement.pdf</FileObj:File_Name>
            <FileObj:File_Extension>pdf</FileObj:File_Extension>
            <FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
            <FileObj:Hashes>
                <cyboxCommon:Hash>
                    <cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Hash_Valu
e>
                </cyboxCommon:Hash>
            </FileObj:Hashes>
        </cybox:Properties>
        <cybox:Related_Objects>
```

```
            <!-- Email Message  -->
            <cybox:Related_Object idref="cybox:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
            </cybox:Related_Object>

            <!-- Artifact  -->
            <cybox:Related_Object idref="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Characterizes</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

3. Artifact object for single attached file.

Artifact objects are for conveying raw chunks of bits like files. They enable the raw content to be conveyed in a structured fashion including characterization of packaging applied such as compression, encryption and encoding.

```
<cybox:Observable id="cybox:observable-14ee6790-b83d-44f1-8604-92271efac9bf">
    <cybox:Object id="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
        <cybox:Properties xsi:type="Artifact:ArtifactObjectType" type="File"
content_type="application/pdf">
            <Artifact:Hashes>
                <cyboxCommon:Hash>
                    <cyboxCommon:Type>MD5</cyboxCommon:Type>
                        <cyboxCommon:Simple_Hash_Value>

                            cf2b3ad32a8a4cfb05e9dfc45875bd70

                        </cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
            </Artifact:Hashes>
            <Artifact:Packaging is_compressed="false" is_encrypted="false">
                <Artifact:Encoding algorithm="Base64" character_set=""/>
            </Artifact:Packaging>
<Artifact:Raw_Artifact>JVBERi0xLjUNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIF
IvTGFuZyhlbi1VUykgL1N0cnVjdFRyZWVSb290IDEwNyAwIFIvTWFya0luZm88PC9NYXJrZWQgdHJ1ZT4+Pj4NCmVuZG9
iag0KMiAwIG9iag0KPDwvVHlwZS9QYWdlcy9Db3VudCAyM
                <!-- The rest of the base64 encoded file content is not included within this
document for space concerns. The full content is available in the example file. -->
            </Artifact:Raw_Artifact>
        </cybox:Properties>
        <cybox:Related_Objects>

            <!-- File  -->
            <cybox:Related_Object idref="cybox:object-cb0ec4ad-4a39-4d4b-934b-72ff0563476f">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Characterized_By</cybox:Relationship>
            </cybox:Related_Object>

            <!-- Email  -->
            <cybox:Related_Object idref="cybox:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
```

```
    </cybox:Object>
</cybox:Observable>
```

a. Potential capability to add to Email_to_CybOX utility: Automated static triage or dynamic sandbox execution of attached files resulting in:
   1. Potentially enriched File objects
   2. Potential for TTP entries with MAEC packages

4. Embedded URLs

The following example snippets present the produced content for only one of the URLs for demonstrative purposes. The produced content for the other URL is available in the full package in Appendix A.

a. URI object for one of the embedded URLs

```
<cybox:Observable id="cybox:observable-524048ee-9af0-4bb7-824e-52e1ce71ebd3">
    <cybox:Object id="cybox:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
        <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">

<URIObj:Value>http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</URIObj:Value>
        </cybox:Properties>
        <cybox:Related_Objects>
            <!-- URI  -->
            <cybox:Related_Object idref="cybox:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object>
            <!-- Email Message  -->
            <cybox:Related_Object idref="cybox:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

b. URI object for the domain name extracted from one of the embedded URLs

```
<cybox:Observable id="cybox:observable-6e98b56a-41b8-4c52-b5ae-6ac86e968b93">
    <cybox:Object id="cybox:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">
        <cybox:Properties xsi:type="DomainNameObj:DomainObjectType" type="FQDN">
            <DomainNameObj:Value>state.gov</URIObj:Value>
        </cybox:Properties>
        <cybox:Related_Objects>
            <!-- WHOIS  -->
            <cybox:Related_Object idref="cybox:object-03d041dd-21f7-4b70-a2be-d4abedf2503b">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Resolved_To</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Query  -->
            <cybox:Related_Object idref="cybox:object-bea8273c-3b4d-409f-880e-c53c64f8a05c">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Properties_Queried_By</cybox:Relationship>
```

```
            </cybox:Related_Object>
            <!-- DNS Record  -->
            <cybox:Related_Object idref="cybox:object-4c9bad1b-e4ac-4b3e-9e28-fbf03b73613c">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Characterized_By</cybox:Relationship>
            </cybox:Related_Object>
            <!-- IP Address  -->
            <cybox:Related_Object idref="cybox:object-f686e94e-d7ff-48b1-a1c3-0f5e8b8d59c1">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Resolved_To</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Query  -->
            <cybox:Related_Object idref="cybox:object-c1849f06-d433-4ef8-bcfa-a516a008c8d4">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Properties_Queried_By</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Record -->
            <cybox:Related_Object idref="cybox:object-1f68760e-fa04-4730-936d-d3abcc4b365b">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Characterized_By</cybox:Relationship>
            </cybox:Related_Object>
            <!-- IP Address  -->
            <cybox:Related_Object idref="cybox:object-428679c7-89c4-4d3a-9693-dd2beb617fb7">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Resolved_To</cybox:Relationship>
            </cybox:Related_Object>
            <!-- URL  -->
            <cybox:Related_Object idref="cybox:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Extracted_From</cybox:Relationship>
            </cybox:Related_Object>
            <!-- URL  -->
            <cybox:Related_Object idref="cybox:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0">Sub-
domain_Of</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

c. DNS resolution

i. DNS Query & DNS Record objects for the domain name extracted from one of the embedded URLs

Two DNS Queries (one for Type A Record and one for Type AAAA Record) are executed by the Email_to_CybOX utility for the domain name within each embedded URL in the email. The DNSQuery object captures the details of the DNS Query executed. The example snippets below show the DNSQuery, DNSRecord and Address objects for the Type AAAA Record query.

```
<cybox:Observable id="cybox:observable-fbd84ce1-fb99-4c6c-8617-5f2b4179da64">
    <cybox:Object id="cybox:object-c1849f06-d433-4ef8-bcfa-a516a008c8d4">
        <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType" successful="true">
            <DNSQueryObj:Question>
                <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
```

```
                    <URIObj:Value>state.gov</URIObj:Value>
                </DNSQueryObj:QName>
                <DNSQueryObj:QType>AAAA</DNSQueryObj:QType>
                <DNSQueryObj:QClass>IN</DNSQueryObj:QClass>
            </DNSQueryObj:Question>
            <DNSQueryObj:Answer_Resource_Records>
                <DNSQueryObj:Resource_Record xsi:type="DNSRecordObj:DNSRecordObjectType"
object_reference="cybox:object-6ec8ffaa-30c8-11e2-8011-000c291a73d5"/>
            </DNSQueryObj:Answer_Resource_Records>
        </cybox:Properties>
        <cybox:Related_Objects>
            <!-- URI  -->
            <cybox:Related_Object idref="cybox:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Properties_Queried</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Record  -->
            <cybox:Related_Object idref="cybox:object-1f68760e-fa04-4730-936d-d3abcc4b365b">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Searched_For</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

The DNS Record object captures the resulting DNS resource record from the executed DNS Query.

```
<cybox:Observable id="cybox:observable-66d0ee64-2412-4af4-82b5-9e5b20e7deda">
    <cybox:Object id="cybox:object-1f68760e-fa04-4730-936d-d3abcc4b365b">
        <cybox:Properties xsi:type="DNSRecordObj:DNSRecordObjectType">
            <DNSRecordObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
                <URIObj:Value>state.gov</URIObj:Value>
            </DNSRecordObj:Domain_Name>
            <DNSRecordObj:IP_Address xsi:type="AddressObj:AddressObjectType" category="ipv6-
addr">

<AddressObj:Address_Value>2001:428:d400:4:72:166:186:151</AddressObj:Address_Value>
            </DNSRecordObj:IP_Address>
            <DNSRecordObj:Entry_Type>AAAA</DNSRecordObj:Entry_Type>
            <DNSRecordObj:Flags>8180</DNSRecordObj:Flags>
            <DNSRecordObj:Record_Data>id 10546
                opcode QUERY
                rcode NOERROR
                flags QR RD RA
                ;QUESTION
                state.gov. IN AAAA
                ;ANSWER
                state.gov. 5 IN AAAA 2001:428:d400:4:72:166:186:151
                ;AUTHORITY
                ;ADDITIONAL</DNSRecordObj:Record_Data>
        </cybox:Properties>
        <cybox:Related_Objects>
            <!-- DNS Query  -->
            <cybox:Related_Object idref="cybox:object-c1849f06-d433-4ef8-bcfa-a516a008c8d4">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Searched_For_By</cybox:Relationship>
            </cybox:Related_Object>
```

```
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

ii. A separate Address object is created from the resulting DNS Record which contains the IP address resolved from the domain name. This information is contained within the DNS record object but giving it its own Observable and Object enables more flexible reuse and pivoting for analysis.

```
<cybox:Observable id="cybox:observable-d701dba9-9325-4d6b-a2d5-3927a9ffd4f5">
    <cybox:Object id="cybox:object-428679c7-89c4-4d3a-9693-dd2beb617fb7">
        <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv6-addr">
            <AddressObj:Address_Value>
                2001:428:d400:4:72:166:186:151
            </AddressObj:Address_Value>
        </cybox:Properties>
        <cybox:Related_Objects>
            <!-- URI  -->
            <cybox:Related_Object idref="cybox:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Resolved_To</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Query  -->
            <cybox:Related_Object idref="cybox:object-c1849f06-d433-4ef8-bcfa-a516a008c8d4">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
            </cybox:Related_Object>
            <!-- DNS Record  -->
            <cybox:Related_Object idref="cybox:object-1f68760e-fa04-4730-936d-d3abcc4b365b">
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

iii. Potential capability to add to Email_to_CybOX utility: Historical DNS lookup

iv. Potential capability to add to Email_to_CybOX utility: Reverse DNS lookup on resolved IP addresses to discover other domains resolving to those IPs

d. WHOIS lookup

A WHOIS lookup is executed for the domain name.

i. For this example, the WHOIS query simply returned a Status statement that the Domain is registered but gave no registrant info. Typically, the WHOIS would also return registrant info for Technical, Billing, Admin, etc.

```
 <cybox:Observable id="cybox:observable-e43863e6-8c28-479d-a8cb-714521750365">
    <cybox:Object id="cybox:object-03d041dd-21f7-4b70-a2be-d4abedf2503b">
        <cybox:Properties xsi:type="WhoisObj:WhoisObjectType">
```

```
            <WhoisObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
                <URIObj:Value>state.gov</URIObj:Value>
            </WhoisObj:Domain_Name>
            <WhoisObj:Status><WhoisObj:Status>OK</WhoisObj:Status></WhoisObj:Status>
        </cybox:Properties>
        <cybox:Related_Objects>

            <!-- URI  -->
            <cybox:Related_Object idref="cybox:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">

                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Resolved_To</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

ii. Potential capability to add to Email_to_CybOX utility: WHOIS lookup by the resolved IP address

iii. Potential capability to add to Email_to_CybOX utility: Query for other domains and IP addresses registered to the same registrant

***Potential capabilities to add to Email_to_CybOX utility***

- Reputation analysis (Query reputation sources for malicious intent)
- Query File hashes from the File/Artifact objects for attachments against file hash reputation sources. If hits found set Artifact object suspected_malicious=true.
- Query Domain names against domain name reputation sources. If hits found create STIX-TTP Resource-Infrastructure entries to characterize the malicious domains and IP addresses, and create STIX ThreatActor entries for registrant info returned in the WHOIS object.
- Query IP addresses against IP reputation sources. . If hits found create STIX-TTP Resource-Infrastructure entries to characterize the malicious domains and IP addresses, and create STIX ThreatActor entries for registrant info returned in the WHOIS object.

#### *1.1.3.1.4 List of e-mails are structured and prioritized*

List of emails submitted to suspicious@XXX.YYY are structured and prioritized (based on reputation analysis or other policy-driven maliciousness characterization) analysis results of the email are presented to the analyst. This basically saves the analyst a significant amount of time by automating the first steps of analysis that must be performed on each email and shortens response time for real threats by enabling the analyst to work on likely malicious issues first.

#### *1.1.3.1.5 Analyst uses structured representation to query for similar e-mails*

Analyst can leverage structured representations to quickly query if this email or similar have been seen before or sent to others within XXX.

1. Query email servers and logs for other identical (other than targeted recipient) emails
2. Query email servers and logs for other similar emails
3. Query shared indicators from sharing partners for similar indicators

#### 1.1.3.1.6 Analyst reviews e-mails and creates generalized pattern

Analyst reviews suspicious email and any related emails (including shared Indicators), identifies unique characteristics, and captures them in an appropriate Observables (CybOX) pattern.

In this example, the analyst creates a pattern for any email from an email address with the domain name "state.gov" and with a PDF file attached that has a size of 87022 bytes and an MD5 hash= cf2b3ad32a8a4cfb05e9dfc45875bd70.

```
<cybox:Observable id="cybox:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
    <cybox:Object id="cybox:object-3a7aa9db-d082-447c-a422-293b78e24238">
        <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
            <EmailMessageObj:Header>
                <EmailMessageObj:From category="e-mail">
                    <AddressObj:Address_Value
condition="Contains">@state.gov</AddressObj:Address_Value>
                </EmailMessageObj:From>
            </EmailMessageObj:Header>
        </cybox:Properties>
        <cybox:Related_Objects>
            <cybox:Related_Object>
                <cybox:Properties xsi:type="FileObj:FileObjectType">
                    <FileObj:File_Extension>pdf</FileObj:File_Extension>
                    <FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
                    <FileObj:Hashes>
                        <cyboxCommon:Hash>
                            <cyboxCommon:Type>MD5</cyboxCommon:Type>
                            <cyboxCommon:Simple_Hash_Value>

                                cf2b3ad32a8a4cfb05e9dfc45875bd70

                            </cyboxCommon:Simple_Hash_Value>
                        </cyboxCommon:Hash>
                    </FileObj:Hashes>
                </cybox:Properties>
                <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
            </cybox:Related_Object>
        </cybox:Related_Objects>
    </cybox:Object>
</cybox:Observable>
```

#### 1.1.3.1.7 Analyst creates STIX Indicator

Analyst creates a STIX Indicator to identify similar emails and to carry out a range of courses of action (COAs) including to filter out future occurrences before they are delivered.

The analyst sets the Indicator's Type to "Malicious E-mail" to express that this Indicator characterizes information regarding a phishing attempt. The Indicator Type field is optional so

the analyst may choose to not create one but it is strongly recommended that they do so. The use of the xsi:type attribute indicates that the Type is from the STIX default vocabulary for indicator types.

```
<indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Malicious E-
mail</indicator:Type>
```

The analyst sets the Indicator's Title to a value they determine relevant to this particular case. In the example here, the value is set to ""US-China" Phishing Indicator". The Indicator Title field is optional so the analyst may choose to not create one but it is recommended that they do so.

```
<indicator:Title>"US-China" Phishing Indicator</indicator:Title>
```

The analyst provides a Description for the Indicator. This description can be as simple or comprehensive as the analyst determines is appropriate. The Description field is optional so the analyst may choose to not create one.

```
<indicator:Description>This is a cyber threat indicator for instances of "US-China" phishing
attempts.</indicator:Description>
```

The analyst defines a Valid Time Position window to specify how long the Indicator should be considered relevant. The Valid Time Position field is optional so the analyst may choose to not create one but it is recommended that they do so.

```
<indicator:Valid_Time_Position>
    <indicator:Start_Time>2012-12-01T09:30:47Z</indicator:Start_Time>
    <indicator:End_Time>2013-02-01T09:30:47Z</indicator:End_Time>
</indicator:Valid_Time_Position>
```

The analyst sets the Indicator Observable field to the CybOX Observable pattern they defined in step 6 above. The defined Observable pattern can be defined inline within the Indicator or defined separately and included by reference (idref). For the example here, the pattern has been defined separately and included by reference (`idref="cybox:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474"`). The Observable field is optional so the analyst may choose to not create one but it is strongly recommended that they do so as an Indicator without a defined pattern of what is relevant does not really make much sense.

```
<indicator:Observable idref="cybox:observable-pattern-5f1dedd3-ece3-4007-94cd-
7d52784c1474"></indicator:Observable>
```

The analyst specifies Indicated TTP content to provide suspected malicious context for instances of the pattern defined in the Observables section. This could be specifying particular attack patterns, malware, exploits, attack tools or infrastructure, etc. The TTP content can be defined

inline within the Indicator or defined separately and included by reference. For this example, a very simple Indicated TTP entry is included inline specifying that instances of the Observable defined in the CybOX pattern indicate the presence of a phishing attack as described in CAPEC-98 "Phishing". The Indicated TTP field is optional so the analyst may choose to not create one but it is recommended that they do so if possible.

```
<indicator:Indicated_TTP>
    <stixCommon:TTP xsi:type="TTP:TTPType">
        <TTP:Behavior>
            <TTP:Attack_Patterns>
                <TTP:Attack_Pattern capec_id="CAPEC-98">
                    <TTP:Description>Phishing</TTP:Description>
                </TTP:Attack_Pattern>
            </TTP:Attack_Patterns>
        </TTP:Behavior>
    </stixCommon:TTP>
</indicator:Indicated_TTP>
```

The analyst may specify particular phases of particular kill chains that are relevant for this Indicator. The Kill_Chain_Phases field is optional so the analyst may choose to not create one.

Before you can reference specific kill chain phases relevant to the Indicator, you must first have a kill chain specification defined somewhere using the STIX-TTP Kill_Chains construct. The snippet below contains a kill chain specification for the Lockheed Martin (LMCO) kill chain. While other kill chains exist, the LMCO kill chain is considered by many the seminal kill chain. The Kill_Chain_Phases entries for this Indicator example will leverage this kill chain specification.

```
<stix:TTPs>
    <stix:Kill_Chains>
        <stixCommon:Kill_Chain id="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff" name="LM
Cyber Kill Chain" definer="LMCO"
reference="http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-
White-Paper-Intel-Driven-Defense.pdf" number_of_phases="7">
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-af1016d6-a744-4ed7-ac91-
00fe2272185a" name="Reconnaissance" ordinality="1"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-445b4827-3cca-42bd-8421-
f2e947133c16" name="Weaponization" ordinality="2"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-79a0e041-9d5f-49bb-ada4-
8322622b162d" name="Delivery" ordinality="3"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-f706e4e7-53d8-44ef-967f-
81535c9db7d0" name="Exploitation" ordinality="4"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-e1e4e3f7-be3b-4b39-b80a-
a593cfd99a4f" name="Installation" ordinality="5"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-d6dc32b9-2538-4951-8733-
3cb9ef1daae2" name="Command and Control" ordinality="6"/>
            <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-786ca8f9-2d9a-4213-b38e-
399af4a2e5d6" name="Actions on Objectives" ordinality="7"/>
        </stixCommon:Kill_Chain>
    </stix:Kill_Chains>
</stix:TTPs>
```

The snippet below specifies that this Indicator is relevant to the "Delivery" phase of the LMCO kill chain.

```
<indicator:Kill_Chain_Phases>
    <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-79a0e041-9d5f-49bb-ada4-8322622b162d"
name="Delivery" ordinality="3" kill_chain_id="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff"
kill_chain_name="LM Cyber Kill Chain"/>
</indicator:Kill_Chain_Phases>
```

The analyst specifies suggested courses of action to take if instances of the pattern defined for this Indicator are observed. Suggested courses of action could be a wide range of possible actions but typically fall into one of two "Stage" types, Remedy or Response where remedies imply apriori actions to mitigate particular malicious actions before they have occurred and responses imply actions taken to recover or clean up after malicious actions have occurred. Suggested courses of action may be defined inline within the Indicator or defined separately and included by reference. For this example, the suggested courses of action are defined inline and consist of several simple descriptions of recommended actions including both remedies and responses. The last entry here with the Type "Super Secret Proprietary Response" contains obviously unrealistic content but is included here to demonstrate the capabilities of the Handling structure described below. The Suggested_COAs field is optional so the analyst may choose to not create one but it is typically recommended to do so in at least a minimal fashion.

```
<indicator:Suggested_COAs>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
346075c3-f3a4-48db-8e71-31b053f7838a" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Email Block</COA:Type>
            <COA:Description>Redirect and quarantine new matching email</COA:Description>
            <COA:Objective>
                <COA:Description>Prevent future instances of similar phishing attempts from
reaching targeted recipients in order to eliminate possibility of compromise from targeted
recipient falling for phishing lure.</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
a157f596-e1bf-4599-9dad-748511d68c3a" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Web Link Block</COA:Type>
            <COA:Description>Block malicous links on web proxies</COA:Description>
            <COA:Objective>
                <COA:Description>Prevent execution/navigation to known malicious web
URLs.</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
0ac78ae1-661d-4845-ace1-a460c6075080" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Domain Traffic Block</COA:Type>
```

```
            <COA:Description>Block traffic to/from malicous domains via firewalls and DNS
servers.</COA:Description>
            <COA:Objective>
                <COA:Description>Prevent any traffic (potentially containing malicious logic,
data exfil, C2, etc.) to or from known malicious domains.</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
a09c17a4-d05e-48f3-b629-7de9a8c42162" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Malicous Email Cleanup</COA:Type>
            <COA:Description>Remove existing matching email from the mail
servers</COA:Description>
            <COA:Objective>
                <COA:Description>Cleanup any known malicious emails from mail servers
(potentially in Inboxes, Sent folders, Deleted folders, etc.) to prevent any future
exploitation from those particular emails.</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
98cf40a2-e2be-448e-8474-c6e8c02628ef" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Phishing Target Identification</COA:Type>
            <COA:Description>Review mail logs to identify other targeted
recipients</COA:Description>
            <COA:Objective>
                <COA:Description>Identify all targeted victims of a particular phishing
campaign in order to enable notification and to support more strategic cyber threat
intelligence activities (TTP characterization, Campaign analysis, ThreatActor attribution,
etc.).</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
d470b8d7-3717-4a42-a3bc-3b57f1b2c300" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Phishing Target Notification</COA:Type>
            <COA:Description>Notify targeted recipients</COA:Description>
            <COA:Objective>
                <COA:Description>Notify all targeted victims of a particular phishing campaign
to ensure they are aware they have been targeted and to help them understand how to avoid
falling for phishing attacks.</COA:Description>
            </COA:Objective>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
    <indicator:Suggested_COA>
        <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType" id="example:COA-
e46d2565-754e-4ac3-9f44-2de1bfb1e71d" timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Super Secret Proprietary Response</COA:Type>
            <COA:Description>Carry out some sensitive action that is applicable only within
the environment of the affected organization.</COA:Description>
        </stixCommon:Course_Of_Action>
    </indicator:Suggested_COA>
</indicator:Suggested_COAs>
```

The analyst specifies guidance on how the content within this Indicator should be handled, especially when sharing with others. The Handling structure within Indicators leverages the separately defined Data_Marking schema. The Data_Marking schema employs a flexible structure enabling the specification of any relevant structure portion (Controlled_Structure) within the defined context (in this case the Indicator) utilizing XPATH and the specification of any set of defined data markings (Marking_Structure) to apply to that specific relevant structure portion. Controlled_Structure entries specify the XPATH of some node in the XML document and imply that any related Marking_Structure entries apply to that node and its descendent children unless overridden by another Marking entry. The Marking_Structure entries can be very flexible in that they are of defined types derived from a single abstract type defined within the Data_Marking schema. This enables a wide range of data marking models to be defined and leveraged in any combination within the same STIX document. The STIX v1.1 language currently includes data marking extensions to do Traffic Light Protocol (TLP), a simple prose marking statement, and terms of use markings. Other data marking models will be added in the future but any STIX user is also free to define and use their own data marking models. For this example, the TLP data marking model is used in two separate "Marking" entries to specify first that the entire Indicator structure should be considered TLP Green and then that one particular SuggestedCOA entry (with id="example:COA-e46d2565-754e-4ac3-9f44-2de1bfb1e71d") should be TLP Red overriding the previous TLP Green marking only for that localized construct. Any number of other "Marking" entries could be specified here if appropriate including other TLP entries or entries utilizing any combination of other data marking models. This enables the same STIX data to be marked with various different marking models to be applied for differing sharing/usage contexts. The Handling field is optional so the analyst may choose to not create one but it is typically recommended to do so to give some guidance on how the information should be handled.

```
<indicator:Handling>
    <marking:Marking id="example:Marking-88501eee-135a-429b-9848-9a992456bd91">
        <marking:Controlled_Structure>ancestor-or-
self::stix:Indicator//node()</marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType"
marking_model_name="TLP" marking_model_ref="http://www.us-cert.gov/tlp/" color="GREEN"/>
    </marking:Marking>
    <marking:Marking id="example:Marking-d50a3e6b-142e-4b8e-92ab-2bb61a273d61">
        <marking:Controlled_Structure>ancestor-or-
self::stix:Indicator//indicator:Suggested_COAs/indicator:Suggested_COA/stixCommon:Course_Of_Ac
tion[@id="example:COA-e46d2565-754e-4ac3-9f44-
2de1bfb1e71d"]//node()</marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType"
marking_model_name="TLP" marking_model_ref="http://www.us-cert.gov/tlp/" color="RED"/>
    </marking:Marking>
</indicator:Handling>
```

The analyst asserts a level of confidence in the aggregate accuracy and relevance of the information contained in this Indicator (in this case basically that the Observables pattern defined truly does represent a phishing attempt). The confidence value field is simply a string and can contain any confidence model value desired. The "vocab_reference" field enables the specification of a reference characterizing the confidence model value specified in the value field. For this example, a simple value of "High" is asserted coming from "MITRE". The

Confidence field is optional so the analyst may choose to not create one but it is typically recommended to do so.

```
<indicator:Confidence timestamp="2012-12-01T09:30:47Z">
    <stixCommon:Value
vocab_reference="someURLtoConfidenceModelDescription.foo.com">High</stixCommon:Value>
    <stixCommon:Source>MITRE</stixCommon:Source>
</indicator:Confidence>
```

The analyst specifies any sighting reports for this particular Indicator or its relevant Observable pattern. For this example, there is only a single sighting specified as this is a new Indicator created for phishing attempts within XXX and has yet to be shared. Other entries could be added if similar Indicators were discovered during the query for similar shared Indicators as described above in Step 5.c or if this new Indicator was shared and others reported seeing it as well. The Confidence field is optional so the analyst may choose to not create one.

```
<indicator:Sightings sightings_count="1">
    <indicator:Sighting timestamp="2012-12-01T09:30:47Z">
        <indicator:Source>MITRE</indicator:Source>
    </indicator:Sighting>
</indicator:Sightings>
```

If this Indicator were reported as seen by others the Sightings structure could be revised to something like the following snippet.

```
<indicator:Sightings sightings_count="3">
    <indicator:Sighting><indicator:Source>MITRE</indicator:Source></indicator:Sighting>
    <indicator:Sighting><indicator:Source>ACME</indicator:Source></indicator:Sighting>
    <indicator:Sighting><indicator:Source>FooBar</indicator:Source></indicator:Sighting>
</indicator:Sightings>
```

The analyst specifies information characterizing the producer of this Indicator. For this example, a very minimal producing organization name is specified but significantly more information could be provided if appropriate. The Producer field is optional so the analyst may choose to not create one but it is strongly recommended to do so.

```
<indicator:Producer>
    <stixCommon:Identity id="example:Org-ba680284-6865-44b4-ba36-dd48d402a589">
        <stixCommon:Name>MITRE</stixCommon:Name>
    </stixCommon:Identity>
    <stixCommon:Time>
        <cyboxCommon:Produced_Time>2012-12-01T09:30:47Z</cyboxCommon:Produced_Time>
    </stixCommon:Time>
</indicator:Producer>
```

#### 1.1.1.2 Sharing

This STIX Indicator and any related STIX content can then be easily shared in an automated fashion with threat information sharing partners as desired utilizing a Trusted Automated eXchange of Indicator Information (TAXII) agent in support of a variety of sharing models. For detailed example information of how to leverage TAXII for sharing STIX content see the TAXII Overview, Version 1.1 document at http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

# Appendix A Phishing Example Detailed Content

## A.1 Full Package of Phishing Observables Autogenerated by the Email_to_CybOX Script (XML Content)

```
<cybox:Observables xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
    xmlns:Artifact="http://cybox.mitre.org/objects#ArtifactObject-2"
    xmlns:WhoisObj="http://cybox.mitre.org/objects#WhoisObject-2"
    xmlns:DNSRecordObj="http://cybox.mitre.org/objects#DNSRecordObject-2"
    xmlns:DNSQueryObj="http://cybox.mitre.org/objects#DNSQueryObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:example="http://example.com"
    xsi:schemaLocation="
http://cybox.mitre.org/cybox-2 ../../../cybox/cybox_core.xsd
http://cybox.mitre.org/common-2 ../../../cybox/cybox_common.xsd
http://cybox.mitre.org/objects#AddressObject-2 ../../../cybox/objects/Address_Object.xsd
http://cybox.mitre.org/objects#FileObject-2 ../../../cybox/objects/File_Object.xsd
http://cybox.mitre.org/objects#URIObject-2 ../../../cybox/objects/URI_Object.xsd
http://cybox.mitre.org/objects#DomainNameObject-1
../../../cybox/objects/Domain_Name_Object.xsd
http://cybox.mitre.org/objects#EmailMessageObject-2
../../../cybox/objects/Email_Message_Object.xsd
http://cybox.mitre.org/objects#ArtifactObject-2 ../../../cybox/objects/Artifact_Object.xsd
http://cybox.mitre.org/objects#WhoisObject-2 ../../../cybox/objects/Whois_Object.xsd
http://cybox.mitre.org/objects#DNSRecordObject-2 ../../../cybox/objects/DNS_Record_Object.xsd
http://cybox.mitre.org/objects#DNSQueryObject-2 ../../../cybox/objects/DNS_Query_Object.xsd
http://cybox.mitre.org/default_vocabularies-2 ../../../cybox/cybox_default_vocabularies.xsd
"
    cybox_major_version="2" cybox_minor_version="1">
    <cybox:Observable id="example:observable-6f45ce72-30c8-11e2-8011-000c291a73d5">
        <cybox:Object id="example:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
            <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
                <EmailMessageObj:Header>
                    <EmailMessageObj:To>
                        <EmailMessageObj:Recipient category="e-mail">

<AddressObj:Address_Value>jsmith@gmail.com</AddressObj:Address_Value>
                        </EmailMessageObj:Recipient>
                    </EmailMessageObj:To>
                    <EmailMessageObj:From category="e-mail">
                        <AddressObj:Address_Value>jdoe@state.gov</AddressObj:Address_Value>
                    </EmailMessageObj:From>
                    <EmailMessageObj:Subject>Fw:Draft US-China Joint
                        Statement</EmailMessageObj:Subject>
                    <EmailMessageObj:Date>2011-01-05T12:48:50+08:00</EmailMessageObj:Date>

<EmailMessageObj:Message_ID>CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com
</EmailMessageObj:Message_ID>
                    <EmailMessageObj:Content_Type>multipart/mixed;
                        boundary=90e6ba10b0e7fbf25104cdd9ad08</EmailMessageObj:Content_Type>
                    <EmailMessageObj:MIME_Version>1.0</EmailMessageObj:MIME_Version>
                    <EmailMessageObj:X_Mailer>Microsoft CDO for Windows
```

```
                        2000</EmailMessageObj:X_Mailer>
                </EmailMessageObj:Header>
                <EmailMessageObj:Raw_Body><![CDATA[ This is the latest version of State's
joint statement. My understanding is
that State put in placeholder econ language and am happy to have us fill in
but in their rush to get a cleared version from the WH, they sent the
attached to Mike. If the attachment doesn't go through, download it here:
http://www.state.gov/public/01aff0dc/Joint_Statement.pdf<http://bhsxeozfiwqj.net/links/p2iodaj
fpoajsfafh.php>

Regards,
Jane Doe

<div>This is the latest version of State&#39;s joint statement. My understa=
nding=A0is that State put in placeholder econ language and am happy to have=
us=A0fill in but in their rush to get a cleared version from the WH, they=
=A0sent the attached to Mike. If the attachment doesn&#39;t go through, dow=
nload it here: <a href=3D"http://bhsxeozfiwqj.net/links/p2iodajfpoajsfafh.p=
hp">http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</a></div>
<div><br></div><div>Regards,</div><div>Jane Doe</div><div><br></div>
]]></EmailMessageObj:Raw_Body>
                <EmailMessageObj:Raw_Header><![CDATA[ Delivered-To: jsmith@gmail.com
Received: by 10.236.111.46 with SMTP id v34cs581528yhg;
Wed, 5 Jan 2011 12:48:37 -0800 (PST)
Received: by 10.142.11.2 with SMTP id 2mr253515wfk.275.1294232332935;
Wed, 05 Jan 2011 12:48:35 -0800 (PST)
Received: from ccccc-ddddd ([113.28.117.3])
by mx.google.com with ESMTP id p7si32937473wfl.41.2011.01.05.04.58.51;
Wed, 05 Jan 2011 12:48:37 -0800 (PST)
Received-SPF: neutral (google.com: 113.28.117.3 is neither permitted nor denied by best guess
record for domain of jdoe@state.gov) client-ip=113.28.117.3;
Authentication-Results: mx.google.com; spf=neutral (google.com: 113.28.117.3 is neither
permitted nor denied by best guess record for domain of jdoe@state.gov)
smtp.mail=jdoe@state.gov
Received: from mail pickup service by ccccc-ddddd with Microsoft SMTPSVC;
Wed, 5 Jan 2011 12:48:30 +0800
Thread-Topic: Draft US-China Joint Statement
From: "Jane Doe" <jdoe@state.gov>
To: "Joe Smith" <jsmith@gmail.com>
Subject: Fw:Draft US-China Joint Statement
Date: Wed, 5 Jan 2011 12:48:50 +0800
Message-ID: <CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com>
X-Mailer: Microsoft CDO for Windows 2000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4721
X-OriginalArrivalTime: 05 Jan 2011 12:48:37 (UTC) FILETIME=[ED3C28C0:01CBACD7]
Content-Type: multipart/mixed; boundary=90e6ba10b0e7fbf25104cdd9ad08
MIME-Version: 1.0
]]></EmailMessageObj:Raw_Header>
                <EmailMessageObj:Attachments>
                    <EmailMessageObj:File
                        object_reference="example:object-6dcae276-30c8-11e2-8011-
000c291a73d5"/>
                </EmailMessageObj:Attachments>
                <EmailMessageObj:Links>
                    <EmailMessageObj:Link
                        object_reference="example:object-6dcb5fda-30c8-11e2-8011-
000c291a73d5"/>
                    <EmailMessageObj:Link
                        object_reference="example:object-6ec9050e-30c8-11e2-8011-
000c291a73d5"/>
                </EmailMessageObj:Links>
```

```
            </cybox:Properties>

            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-cb0ec4ad-4a39-4d4b-934b-
72ff0563476f">
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
                <!-- File  -->
                <cybox:Related_Object idref="example:object-afb6205d-4db6-44de-98d7-
37a32ee4b012">
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
                <!-- Artifact  -->
                <cybox:Related_Object idref="example:object-1ba9f939-0c5a-421e-b59d-
f8a6517f9018">
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
                <!-- URL  -->
                <cybox:Related_Object idref="example:object-fa7efe7f-e1b4-45de-ba7e-
c6a7d625c9d8">
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
                <!-- URL  -->
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Artifact (raw attachment)-->
    <cybox:Observable id="example:observable-14ee6790-b83d-44f1-8604-92271efac9bf">
        <cybox:Object id="example:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
            <cybox:Properties xsi:type="Artifact:ArtifactObjectType" type="File"
                content_type="application/pdf">
                <Artifact:Hashes>
                    <cyboxCommon:Hash>
                        <cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Hash_Value
>
                    </cyboxCommon:Hash>
                </Artifact:Hashes>
                <Artifact:Packaging is_compressed="false" is_encrypted="false">
                    <Artifact:Encoding algorithm="Base64" character_set=""/>
                </Artifact:Packaging>
                <Artifact:Raw_Artifact>
                    <!-- Not wanting to use actual malicious content, the Raw content included
here is actually derived from the STIX whitepaper just for example purposes. -->

JVBERi0xLjUNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFuZyhlbi1VUykgL1N0cn
VjdFRyZWVSb290IDEwNyAwIFIvTWFya0luZm88PC9NYXJrZWQgdHJ1ZT4+Pj4NCmVuZG9iag0KMiAwIG9iag0KPDwvVHlw
ZS9QYWdl
                    <!-- The full artifact content is omitted for space reasons, but can be
found in the Github repository or in the full downloads available on the samples page -->
                </Artifact:Raw_Artifact>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-cb0ec4ad-4a39-4d4b-934b-
72ff0563476f">
```

```
                    <!-- File  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Characterized_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-
68eb0ea12ef0">
                    <!-- Email  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- FIle Attachment  -->
    <cybox:Observable id="example:observable-0a41ab04-f6ca-4bc7-93e1-0efbad2119da">
        <cybox:Object id="example:object-cb0ec4ad-4a39-4d4b-934b-72ff0563476f">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
                <FileObj:File_Name>Joint_Statement.pdf</FileObj:File_Name>
                <FileObj:File_Extension>pdf</FileObj:File_Extension>
                <FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
                <FileObj:Hashes>
                    <cyboxCommon:Hash>
                        <cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Hash_Value
>
                    </cyboxCommon:Hash>
                </FileObj:Hashes>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-
68eb0ea12ef0">
                    <!-- Email Message  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-afb6205d-4db6-44de-98d7-
37a32ee4b012">
                    <!-- Artifact  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Characterizes</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Link URL (http://www.state.gov/public/01aff0dc/Joint_Statement.pdf)  -->
    <cybox:Observable id="example:observable-524048ee-9af0-4bb7-824e-52e1ce71ebd3">
        <cybox:Object id="example:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">

<URIObj:Value>http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</URIObj:Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
```

```
                <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-
68eb0ea12ef0">
                    <!-- Email Message  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Extracted Domain from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-6e98b56a-41b8-4c52-b5ae-6ac86e968b93">
        <cybox:Object id="example:object-45ed3e11-5be1-4a7e-8f02-25b8f74196d3">
            <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
                <DomainNameObj:Value>state.gov</DomainNameObj:Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-03d041dd-21f7-4b70-a2be-
d4abedf2503b">
                    <!-- WHOIS  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-bea8273c-3b4d-409f-880e-
c53c64f8a05c">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-4c9bad1b-e4ac-4b3e-9e28-
fbf03b73613c">
                    <!-- DNS Record  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Characterized_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-f686e94e-d7ff-48b1-a1c3-
0f5e8b8d59c1">
                    <!-- IP Address  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-c1849f06-d433-4ef8-bcfa-
a516a008c8d4">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-1f68760e-fa04-4730-936d-
d3abcc4b365b">
                    <!-- DNS Record -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Characterized_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-428679c7-89c4-4d3a-9693-
dd2beb617fb7">
                    <!-- IP Address  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-1ba9f939-0c5a-421e-b59d-
f8a6517f9018">
```

```
                    <!-- URL  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Extracted_From</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-1ba9f939-0c5a-421e-b59d-
f8a6517f9018">
                    <!-- URL  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Sub-domain_Of</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- WHOIS for extracted Domain from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-e43863e6-8c28-479d-a8cb-714521750365">
        <cybox:Object id="example:object-03d041dd-21f7-4b70-a2be-d4abedf2503b">
            <cybox:Properties xsi:type="WhoisObj:WhoisObjectType">
                <WhoisObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
                    <URIObj:Value>state.gov</URIObj:Value>
                </WhoisObj:Domain_Name>
                <WhoisObj:Status>
                    <WhoisObj:Status>OK</WhoisObj:Status>
                </WhoisObj:Status>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Type A DNS Query of extracted Domain from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-58c11cce-aef1-467c-b2bf-051407a0c2ba">
        <cybox:Object id="example:object-bea8273c-3b4d-409f-880e-c53c64f8a05c">
            <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType" successful="true">
                <DNSQueryObj:Question>
                    <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
                        <URIObj:Value>state.gov</URIObj:Value>
                    </DNSQueryObj:QName>
                    <DNSQueryObj:QType>A</DNSQueryObj:QType>
                    <DNSQueryObj:QClass>IN</DNSQueryObj:QClass>
                </DNSQueryObj:Question>
                <DNSQueryObj:Answer_Resource_Records>
                    <DNSQueryObj:Resource_Record xsi:type="DNSRecordObj:DNSRecordObjectType"
                        object_reference="example:object-6ec1cb36-30c8-11e2-8011-
000c291a73d5"/>
                </DNSQueryObj:Answer_Resource_Records>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-4c9bad1b-e4ac-4b3e-9e28-
```

```
fbf03b73613c">
                    <!-- DNS Record  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Searched_For</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Returned DNS Record for Type A DNS Query of extracted Domain from link URL
(state.gov)  -->
    <cybox:Observable id="example:observable-8239d3ba-5f4e-4d3d-99cf-cc17ae99f9b5">
        <cybox:Object id="example:object-4c9bad1b-e4ac-4b3e-9e28-fbf03b73613c">
            <cybox:Properties xsi:type="DNSRecordObj:DNSRecordObjectType">
                <DNSRecordObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
                    <URIObj:Value>state.gov</URIObj:Value>
                </DNSRecordObj:Domain_Name>
                <DNSRecordObj:IP_Address xsi:type="AddressObj:AddressObjectType"
                    category="ipv4-addr">
                    <AddressObj:Address_Value>72.166.186.151</AddressObj:Address_Value>
                </DNSRecordObj:IP_Address>
                <DNSRecordObj:Entry_Type>A</DNSRecordObj:Entry_Type>
                <DNSRecordObj:Flags>8180</DNSRecordObj:Flags>
                <DNSRecordObj:Record_Data>id 48924 opcode QUERY rcode NOERROR flags QR RD RA
                    ;QUESTION state.gov. IN A ;ANSWER state.gov. 5 IN A 72.166.186.151
;AUTHORITY
                    ;ADDITIONAL</DNSRecordObj:Record_Data>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Characterizes</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-bea8273c-3b4d-409f-880e-
c53c64f8a05c">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Searched_For_By</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Resolved IP Address from Returned DNS Record for Type A DNS Query of extracted Domain
from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-2b2b84e1-2d10-46d7-ab4a-6f71d33f2b0b">
        <cybox:Object id="example:object-f686e94e-d7ff-48b1-a1c3-0f5e8b8d59c1">
            <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
                <AddressObj:Address_Value>72.166.186.151</AddressObj:Address_Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-bea8273c-3b4d-409f-880e-
c53c64f8a05c">
```

```
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-4c9bad1b-e4ac-4b3e-9e28-
fbf03b73613c">
                    <!-- DNS Record  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Type AAAA DNS Query of extracted Domain from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-fbd84ce1-fb99-4c6c-8617-5f2b4179da64">
        <cybox:Object id="example:object-c1849f06-d433-4ef8-bcfa-a516a008c8d4">
            <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType" successful="true">
                <DNSQueryObj:Question>
                    <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
                        <URIObj:Value>state.gov</URIObj:Value>
                    </DNSQueryObj:QName>
                    <DNSQueryObj:QType>AAAA</DNSQueryObj:QType>
                    <DNSQueryObj:QClass>IN</DNSQueryObj:QClass>
                </DNSQueryObj:Question>
                <DNSQueryObj:Answer_Resource_Records>
                    <DNSQueryObj:Resource_Record xsi:type="DNSRecordObj:DNSRecordObjectType"
                        object_reference="example:object-6ec8ffaa-30c8-11e2-8011-
000c291a73d5"/>
                </DNSQueryObj:Answer_Resource_Records>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-1f68760e-fa04-4730-936d-
d3abcc4b365b">
                    <!-- DNS Record  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Searched_For</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Returned DNS Record for Type AAAA DNS Query of extracted Domain from link URL
(state.gov)  -->
    <cybox:Observable id="example:observable-66d0ee64-2412-4af4-82b5-9e5b20e7deda">
        <cybox:Object id="example:object-1f68760e-fa04-4730-936d-d3abcc4b365b">
            <cybox:Properties xsi:type="DNSRecordObj:DNSRecordObjectType">
                <DNSRecordObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
                    <URIObj:Value>state.gov</URIObj:Value>
                </DNSRecordObj:Domain_Name>
                <DNSRecordObj:IP_Address xsi:type="AddressObj:AddressObjectType"
                    category="ipv6-addr">

<AddressObj:Address_Value>2001:428:d400:4:72:166:186:151</AddressObj:Address_Value>
                </DNSRecordObj:IP_Address>
```

```
                <DNSRecordObj:Entry_Type>AAAA</DNSRecordObj:Entry_Type>
                <DNSRecordObj:Flags>8180</DNSRecordObj:Flags>
                <DNSRecordObj:Record_Data>id 10546 opcode QUERY rcode NOERROR flags QR RD RA
                    ;QUESTION state.gov. IN AAAA ;ANSWER state.gov. 5 IN AAAA
                    2001:428:d400:4:72:166:186:151 ;AUTHORITY
;ADDITIONAL</DNSRecordObj:Record_Data>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-c1849f06-d433-4ef8-bcfa-
a516a008c8d4">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Searched_For_By</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Resolved IP Address from Returned DNS Record for Type AAAA DNS Query of extracted
Domain from link URL (state.gov)  -->
    <cybox:Observable id="example:observable-d701dba9-9325-4d6b-a2d5-3927a9ffd4f5">
        <cybox:Object id="example:object-428679c7-89c4-4d3a-9693-dd2beb617fb7">
            <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv6-addr">

<AddressObj:Address_Value>2001:428:d400:4:72:166:186:151</AddressObj:Address_Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Resolved_To</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-c1849f06-d433-4ef8-bcfa-
a516a008c8d4">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-1f68760e-fa04-4730-936d-
d3abcc4b365b">
                    <!-- DNS Record  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Link URL (http://bhsxeozfiwqj.net/links/p2iodajfpoajsfafh.php)  -->
    <cybox:Observable id="example:observable-bcb595f7-2d67-4ef2-883e-5cca47e336ce">
        <cybox:Object id="example:object-fa7efe7f-e1b4-45de-ba7e-c6a7d625c9d8">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">

<URIObj:Value>http://bhsxeozfiwqj.net/links/p2iodajfpoajsfafh.php</URIObj:Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-486b9846-ced7-49d3-ae92-
7845f06b6557">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
```

```
                        >Contains</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-
68eb0ea12ef0">
                    <!-- Email Message  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Extracted Domain from link URL (bhsxeozfiwqj.net)  -->
    <cybox:Observable id="example:observable-542405ea-3a77-4490-b37d-c1a555f2d7be">
        <cybox:Object id="example:object-486b9846-ced7-49d3-ae92-7845f06b6557">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="Domain Name">
                <URIObj:Value>bhsxeozfiwqj.net</URIObj:Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-79a3f502-478d-4c0c-a97f-
d10d69658b4c">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-b7edd88e-5b47-42a6-a5be-
ab87d8d8d1ba">
                    <!-- DNS Query  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried_By</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-fa7efe7f-e1b4-45de-ba7e-
c6a7d625c9d8">
                    <!-- URL  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Extracted_From</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-fa7efe7f-e1b4-45de-ba7e-
c6a7d625c9d8">
                    <!-- URL  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >FQDN_Of</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Type A DNS Query of extracted Domain from link URL (bhsxeozfiwqj.net)  -->
    <cybox:Observable id="example:observable-86edf6eb-e67f-47c4-96ed-1f5b3eb5fa44">
        <cybox:Object id="example:object-79a3f502-478d-4c0c-a97f-d10d69658b4c">
            <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType" successful="false">
                <DNSQueryObj:Question>
                    <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
                        <URIObj:Value>bhsxeozfiwqj.net</URIObj:Value>
                    </DNSQueryObj:QName>
                    <DNSQueryObj:QType>A</DNSQueryObj:QType>
                    <DNSQueryObj:QClass>IN</DNSQueryObj:QClass>
                </DNSQueryObj:Question>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-486b9846-ced7-49d3-ae92-
```

```
7845f06b6557">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>

    <!-- Type AAAA DNS Query of extracted Domain from link URL (bhsxeozfiwqj.net)  -->
    <cybox:Observable id="example:observable-a044709c-8d83-406c-8cc9-73cd16c62718">
        <cybox:Object id="example:object-b7edd88e-5b47-42a6-a5be-ab87d8d8d1ba">
            <cybox:Properties xsi:type="DNSQueryObj:DNSQueryObjectType" successful="false">
                <DNSQueryObj:Question>
                    <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
                        <URIObj:Value>bhsxeozfiwqj.net</URIObj:Value>
                    </DNSQueryObj:QName>
                    <DNSQueryObj:QType>AAAA</DNSQueryObj:QType>
                    <DNSQueryObj:QClass>IN</DNSQueryObj:QClass>
                </DNSQueryObj:Question>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-486b9846-ced7-49d3-ae92-
7845f06b6557">
                    <!-- URI  -->
                    <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
                        >Properties_Queried</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Observable>
</cybox:Observables>
```

## A.2 Phishing Email Attachment Artifact Object (XML Content)

```
<cybox:Observables
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:Artifact="http://cybox.mitre.org/objects#ArtifactObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:example="http://example.com"
  xsi:schemaLocation="
http://cybox.mitre.org/cybox-2 http://cybox.mitre.org/XMLSchema/core/2.1/cybox_core.xsd
http://cybox.mitre.org/common-2 http://cybox.mitre.org/XMLSchema/common/2.1/cybox_common.xsd
http://cybox.mitre.org/objects#ArtifactObject-2
http://cybox.mitre.org/XMLSchema/objects/Artifact/2.1/Artifact_Object.xsd
http://cybox.mitre.org/default_vocabularies-2
http://cybox.mitre.org/XMLSchema/default_vocabularies/2.1/cybox_default_vocabularies.xsd
"
  cybox_major_version="2" cybox_minor_version="1">

  <!-- Artifact object -->
  <cybox:Observable id="example:observable-14ee6790-b83d-44f1-8604-92271efac9bf">
    <cybox:Object id="example:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
      <cybox:Properties xsi:type="Artifact:ArtifactObjectType" type="File"
        content_type="application/pdf">
        <Artifact:Hashes>
```

```
          <cyboxCommon:Hash>
            <cyboxCommon:Type>MD5</cyboxCommon:Type>

<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Hash_Value
>
          </cyboxCommon:Hash>
        </Artifact:Hashes>
        <Artifact:Packaging is_compressed="false" is_encrypted="false">
          <Artifact:Encoding algorithm="Base64" character_set=""/>
        </Artifact:Packaging>
        <Artifact:Raw_Artifact>
          <!-- Not wanting to use actual malicious content, the Raw content included here is
actually derived from the STIX whitepaper just for example purposes. -->
JVBERi0xLjUNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFuZyhlbi1VUykgL1N0cn
VjdFRyZWVSb290IDEwNyAwIFIvTWFya0luZm88PC9NYXJrZWQgdH
          <!--The rest of the base64 encoded file content is not included within this document
for space concerns. The full content is available in the example file. -->
        </Artifact:Raw_Artifact>
      </cybox:Properties>
      <cybox:Related_Objects>
        <cybox:Related_Object idref="example:object-cb0ec4ad-4a39-4d4b-934b-72ff0563476f">
          <!-- File  -->
          <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
            >Characterized_By</cybox:Relationship>
        </cybox:Related_Object>
        <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-68eb0ea12ef0">
          <!-- Email  -->
          <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
            >Contained_Within</cybox:Relationship>
        </cybox:Related_Object>
      </cybox:Related_Objects>
    </cybox:Object>
  </cybox:Observable>
</cybox:Observables>
```

## A.3 LMCO Kill Chain Specification (XML Content)

```
<?xml version="1.0" encoding="UTF-8"?>
<TTP:TTP xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:TTP="http://stix.mitre.org/TTP-1"
xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
version="1.1"
xsi:schemaLocation="http://stix.mitre.org/TTP-1
http://stix.mitre.org/XMLSchema/ttp/1.1/ttp.xsd" >
  <TTP:Kill_Chains>
    <stixCommon:Kill_Chain id="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff" name="LM Cyber
Kill Chain" definer="LMCO"
reference="http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-
White-Paper-Intel-Driven-Defense.pdf" number_of_phases="7">
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-af1016d6-a744-4ed7-ac91-00fe2272185a"
name="Reconnaissance" ordinality="1"/>
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-445b4827-3cca-42bd-8421-f2e947133c16"
name="Weaponization" ordinality="2"/>
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-79a0e041-9d5f-49bb-ada4-8322622b162d"
name="Delivery" ordinality="3"/>
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-f706e4e7-53d8-44ef-967f-81535c9db7d0"
name="Exploitation" ordinality="4"/>
```

```
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-e1e4e3f7-be3b-4b39-b80a-a593cfd99a4f"
name="Installation" ordinality="5"/>
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-d6dc32b9-2538-4951-8733-3cb9ef1daae2"
name="Command and Control" ordinality="6"/>
      <stixCommon:Kill_Chain_Phase phase_id="stix:TTP-786ca8f9-2d9a-4213-b38e-399af4a2e5d6"
name="Actions on Objectives" ordinality="7"/>
    </stixCommon:Kill_Chain>
  </TTP:Kill_Chains>
</TTP:TTP>
```

## A.4 CybOX Pattern for Phishing Instance Characterization (XML Content)

```
<cybox:Observables xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
  xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:example="http://example.com"
  xsi:schemaLocation="
http://cybox.mitre.org/cybox-2 http://cybox.mitre.org/XMLSchema/core/2.1/cybox_core.xsd
http://cybox.mitre.org/common-2 http://cybox.mitre.org/XMLSchema/common/2.1/cybox_common.xsd
http://cybox.mitre.org/objects#AddressObject-2
http://cybox.mitre.org/XMLSchema/objects/Address/2.1/Address_Object.xsd
http://cybox.mitre.org/objects#FileObject-2
http://cybox.mitre.org/XMLSchema/objects/File/2.1/File_Object.xsd
http://cybox.mitre.org/objects#EmailMessageObject-2
http://cybox.mitre.org/XMLSchema/objects/Email_Message/2.1/Email_Message_Object.xsd
http://cybox.mitre.org/default_vocabularies-2
http://cybox.mitre.org/XMLSchema/default_vocabularies/2.1/cybox_default_vocabularies.xsd"
  cybox_major_version="2" cybox_minor_version="1">
  <cybox:Observable id="example:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
    <cybox:Object id="example:object-3a7aa9db-d082-447c-a422-293b78e24238">
      <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
        <EmailMessageObj:Header>
          <EmailMessageObj:From category="e-mail">
            <AddressObj:Address_Value condition="Contains"
              >@state.gov</AddressObj:Address_Value>
          </EmailMessageObj:From>
        </EmailMessageObj:Header>
      </cybox:Properties>
      <cybox:Related_Objects>
        <cybox:Related_Object>
          <cybox:Properties xsi:type="FileObj:FileObjectType">
            <FileObj:File_Extension>pdf</FileObj:File_Extension>
            <FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
            <FileObj:Hashes>
              <cyboxCommon:Hash>
                <cyboxCommon:Type>MD5</cyboxCommon:Type>
<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Hash_Value
>
              </cyboxCommon:Hash>
            </FileObj:Hashes>
          </cybox:Properties>
          <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0"
            >Contains</cybox:Relationship>
        </cybox:Related_Object>
```

```
      </cybox:Related_Objects>
    </cybox:Object>
  </cybox:Observable>
</cybox:Observables>
```

## A.5 STIX Indicator for Phishing with Observables Included by Reference (XML Content)

```
<stix:STIX_Package xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1" xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:TTP="http://stix.mitre.org/TTP-1"
  xmlns:COA="http://stix.mitre.org/CourseOfAction-1" xmlns:ciq="urn:oasis:names:tc:ciq:xpil:3"
  xmlns:n="urn:oasis:names:tc:ciq:xnl:3"
  xmlns:capec="http://stix.mitre.org/extensions/AP#CAPEC2.5-1"
  xmlns:marking="http://data-marking.mitre.org/Marking-1"
  xmlns:tlpMarking="http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.1/stix_core.xsd
http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1/stix_common.xsd
http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.1/indicator.xsd
http://stix.mitre.org/TTP-1 http://stix.mitre.org/XMLSchema/ttp/1.1/ttp.xsd
http://stix.mitre.org/CourseOfAction-1
http://stix.mitre.org/XMLSchema/course_of_action/1.1/course_of_action.xsd
http://data-marking.mitre.org/Marking-1
http://stix.mitre.org/XMLSchema/data_marking/1.1/data_marking.xsd
http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1
http://stix.mitre.org/XMLSchema/extensions/marking/tlp/1.1/tlp_marking.xsd
http://stix.mitre.org/default_vocabularies-1
http://stix.mitre.org/XMLSchema/default_vocabularies/1.1.0/stix_default_vocabularies.xsd
"
  id="example:package-ba1d406e-937c-414f-9231-6e1dbe64fe8b" version="1.1">
  <stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType"
      id="example:Indicator-19e5d914-cc0e-478f-a523-b099a34383f7"
      timestamp="2014-02-20T09:00:00.000000Z">
      <indicator:Title>"US-China" Phishing Indicator</indicator:Title>
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Malicious
        E-mail</indicator:Type>
      <indicator:Description>This is a cyber threat indicator for instances of "US-China"
        phishing attempts.</indicator:Description>
      <indicator:Valid_Time_Position>
        <indicator:Start_Time>2012-12-01T09:30:47Z</indicator:Start_Time>
        <indicator:End_Time>2013-02-01T09:30:47Z</indicator:End_Time>
      </indicator:Valid_Time_Position>

      <!-- The CybOX observable pattern is defined in a separate file and included here by
reference for space reasons. It could just as easily be included here inline. -->
      <indicator:Observable
        idref="example:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474"/>

      <indicator:Indicated_TTP>
```

```
        <stixCommon:TTP xsi:type="TTP:TTPType">
          <TTP:Behavior>
            <TTP:Attack_Patterns>
              <TTP:Attack_Pattern capec_id="CAPEC-98">
                <TTP:Description>Phishing</TTP:Description>
              </TTP:Attack_Pattern>
            </TTP:Attack_Patterns>
          </TTP:Behavior>
        </stixCommon:TTP>
      </indicator:Indicated_TTP>
      <indicator:Kill_Chain_Phases>
        <stixCommon:Kill_Chain_Phase
          phase_id="stix:TTP-79a0e041-9d5f-49bb-ada4-8322622b162d" name="Delivery"
          ordinality="3" kill_chain_id="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff"
          kill_chain_name="LM Cyber Kill Chain"/>
      </indicator:Kill_Chain_Phases>
      <indicator:Suggested_COAs>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-346075c3-f3a4-48db-8e71-31b053f7838a">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Email Block</COA:Type>
            <COA:Description>Redirect and quarantine new matching
              email</COA:Description>
            <COA:Objective>
              <COA:Description>Prevent future instances of similar phishing attempts
                from reaching targeted recipients in order to eliminate possibility
                of compromise from targeted recipient falling for phishing
                lure.</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-a157f596-e1bf-4599-9dad-748511d68c3a"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Web Link Block</COA:Type>
            <COA:Description>Block malicous links on web proxies</COA:Description>
            <COA:Objective>
              <COA:Description>Prevent execution/navigation to known malicious web
                URLs.</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-0ac78ae1-661d-4845-ace1-a460c6075080"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Remedy</COA:Stage>
            <COA:Type>Domain Traffic Block</COA:Type>
            <COA:Description>Block traffic to/from malicous domains via firewalls and
              DNS servers.</COA:Description>
            <COA:Objective>
              <COA:Description>Prevent any traffic (potentially containing malicious
                logic, data exfil, C2, etc.) to or from known malicious
                domains.</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
```

```
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-a09c17a4-d05e-48f3-b629-7de9a8c42162"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Malicous Email Cleanup</COA:Type>
            <COA:Description>Remove existing matching email from the mail
              servers</COA:Description>
            <COA:Objective>
              <COA:Description>Cleanup any known malicious emails from mail servers
                (potentially in Inboxes, Sent folders, Deleted folders, etc.) to
                prevent any future exploitation from those particular
                emails.</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-98cf40a2-e2be-448e-8474-c6e8c02628ef"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Phishing Target Identification</COA:Type>
            <COA:Description>Review mail logs to identify other targeted
              recipients</COA:Description>
            <COA:Objective>
              <COA:Description>Identify all targeted victims of a particular phishing
                campaign in order to enable notification and to support more
                strategic cyber threat intelligence activities (TTP
                characterization, Campaign analysis, ThreatActor attribution,
                etc.).</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-d470b8d7-3717-4a42-a3bc-3b57f1b2c300"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Phishing Target Notification</COA:Type>
            <COA:Description>Notify targeted recipients</COA:Description>
            <COA:Objective>
              <COA:Description>Notify all targeted victims of a particular phishing
                campaign to ensure they are aware they have been targeted and to
                help them understand how to avoid falling for phishing
                attacks.</COA:Description>
            </COA:Objective>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
        <indicator:Suggested_COA>
          <stixCommon:Course_Of_Action xsi:type="COA:CourseOfActionType"
            id="example:COA-e46d2565-754e-4ac3-9f44-2de1bfb1e71d"
            timestamp="2014-02-20T09:00:00.000000Z">
            <COA:Stage>Response</COA:Stage>
            <COA:Type>Super Secret Proprietary Response</COA:Type>
            <COA:Description>Carry out some sensitive action that is applicable only
              within the environment of the affected organization.</COA:Description>
          </stixCommon:Course_Of_Action>
        </indicator:Suggested_COA>
      </indicator:Suggested_COAs>
      <indicator:Handling>
        <marking:Marking id="example:Marking-88501eee-135a-429b-9848-9a992456bd91">
          <marking:Controlled_Structure>ancestor-or-
```

```
self::stix:Indicator//node()</marking:Controlled_Structure>
          <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType"
            marking_model_name="TLP" marking_model_ref="http://www.us-cert.gov/tlp/"
            color="GREEN"/>
        </marking:Marking>
        <marking:Marking id="example:Marking-d50a3e6b-142e-4b8e-92ab-2bb61a273d61">
          <marking:Controlled_Structure>ancestor-or-
self::stix:Indicator//indicator:Suggested_COAs/indicator:Suggested_COA/stixCommon:Course_Of_Ac
tion[@id="example:COA-e46d2565-754e-4ac3-9f44-
2de1bfb1e71d"]//node()</marking:Controlled_Structure>
          <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType"
            marking_model_name="TLP" marking_model_ref="http://www.us-cert.gov/tlp/"
            color="RED"/>
        </marking:Marking>
      </indicator:Handling>
      <indicator:Confidence timestamp="2012-12-01T09:30:47Z">
        <stixCommon:Value vocab_reference="someURLtoConfidenceModelDescription.foo.com"
          >High</stixCommon:Value>
        <stixCommon:Source>MITRE</stixCommon:Source>
      </indicator:Confidence>
      <indicator:Sightings sightings_count="1">
        <indicator:Sighting timestamp="2012-12-01T09:30:47Z">
          <indicator:Source>MITRE</indicator:Source>
        </indicator:Sighting>
      </indicator:Sightings>
      <indicator:Producer>
        <stixCommon:Identity id="example:Org-ba680284-6865-44b4-ba36-dd48d402a589">
          <stixCommon:Name>MITRE</stixCommon:Name>
        </stixCommon:Identity>
        <stixCommon:Time>
          <cyboxCommon:Produced_Time>2012-12-01T09:30:47Z</cyboxCommon:Produced_Time>
        </stixCommon:Time>
      </indicator:Producer>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```