International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1215

(01/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Use cases for structured threat information expression

Recommendation ITU-T X.1215

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1215

Use cases for structured threat information expression

Summary

Recommendation ITU-T X.1215 provides various use cases for how the structured threat information expression (STIX) language may be used to support cyber threat intelligence (CTI) and information sharing.

This Recommendation also describes concepts and functionality of the STIX language. It is targeted to support a range of use cases involved in cyber threat management, including analysing cyber threats, specifying indicator patterns for cyber threats, managing response activities and sharing cyber threat information. With this kind of information, a security decision can be made on how to best defend against the threat. It is intended to support both more effective analysis and the continued exchange of cyber threat information. The STIX suite of specifications [b-STIX2.0] is maintained under the responsibility of the Organization for the Advancement of Structured Information Standards (OASIS).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1215	2019-01-30	17	11.1002/1000/13849

Keywords

Cyber threat intelligence, information sharing, security, STIX.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1215

Use cases for structured threat information expression

1 Scope

This Recommendation aims to provide various use cases for structured threat information expression (STIX), which is a structured language for describing cyber threat information. It is targeted to support a range of use cases involved in cyber threat management, including analysing cyber threats, specifying indicator patterns for cyber threats, managing response activities and sharing cyber threat information. These use cases are typically simple in nature and do not convey the full expressivity or flexibility of the STIX language. The use cases typically include some prose describing use case activities, representations of STIX content and fully validated STIX content documents. An implementation of the use cases in the extensible markup language (XML) is presented as version 1.2 of STIX released in 2016 uses XML schema, while version 2.0 employs JavaScript Object Notation (JSON). It is recommended to use requirements described in STIX 2.0.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 entity [b-STIX2.0-Part 1]: Anything that has a separately identifiable existence (e.g., organization, person, group, etc.).

3.1.2 STIX object [b-STIX2.0-Part 1]: A STIX domain object (SDO) or a STIX relationship object (SRO).

3.1.3 structured threat information expression (STIX) [b-STIX2.0-Part 1]: A language and serialization format used to exchange cyber threat intelligence (CTI).

3.1.4 trusted automated exchange of indicator information (TAXII) [b-STIX2.0-Part 1]: An application layer protocol for the communication of cyber threat information.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAPEC	Common Attack Pattern Enumeration and Classification
COA	Course Of Action
CnC	Command and Control
CTI	Cyber Threat Intelligence
CVE	Common Vulnerability and Exposures
C2	Command and Control
DLL	Dynamic Link Library
EDR	Event Data Recorder
JSON	JavaScript Object Notation
OS	Operating System
SDO	STIX Domain Object (a "node" in a graph)
SMBv2	Server Message Block version 2
SRO	STIX Relationship Object (one mechanism to represent an "edge" in a graph)
STIX	Structured Threat Information Expression
TAXII	Trusted Automated exchange of Indicator Information
TTP	Tactics, Technique, and Procedure
TLP	Traffic Light Protocol
XML	Extensible Markup Language

5 Conventions

None.

6 Overview of STIX

6.1 Concepts of STIX

For real-time response to cyber threats, not only an individual security system, but also a global cooperative security management system should be provided since there are global problems which cannot be solved by any single entity as well as single domain [b-STIX2.0]. Therefore, global cyber threat intelligence (CTI) is an important component of an organization's security program and can be obtained internally and from external sources. One of solutions for cyber threat intelligence and information sharing is structured threat information expression (STIX) which is a structured language for describing cyber threat information. STIX provides structured representations of cyber threat information that is expressive, flexible, extensible, automatable and readable.

6.2 Objects in STIX

6.2.1 Objects in STIX 1.2

This Recommendation should adopt seven STIX domain objects (SDOs) defined in [b-STIX1.2.1-Part 1] as follows:

1) Campaign: A STIX campaign represents a set of tactics, technique, and procedures (TTPs), incidents, or threat actors that together express a common intent or desired effect.

2) Course of action: A STIX course of action component is used to convey information about courses of action that may be taken either in response to an attack or as a preventative measure prior to an attack.

3) Exploit target: A STIX exploit target conveys information about a technical vulnerability, weakness, or misconfiguration in software, systems, or networks that may be targeted for exploitation by an adversary.

4) Incident: A STIX incident conveys information about a cybersecurity incident.

5) Indicator: A STIX indicator conveys specific observable patterns combined with contextual information.

6) Threat actor: A STIX threat actor conveys information that characterizes or identifies (or both) an adversary.

7) TTP: TTP is a military term that means "tactics, techniques, and procedures".

6.2.2 STIX objects

This Recommendation should adopt the set of STIX domain objects (SDOs) and STIX relationship objects (SROs) defined in [b-STIX2.0-Part 2] to represent cyber threat information.

Twelve SDOs are defined in [b-STIX2.0-Part 2] as follows:

1) Attack pattern: Attack patterns are a type of TTP that describe ways that adversaries attempt to compromise targets.

2) Campaign: A campaign is a grouping of adversarial behaviours that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets.

3) Course of action: A course of action is an action taken either to prevent an attack or to respond to an attack that is in progress.

4) Identity: Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, or groups (e.g., the finance sector).

5) Indicator: Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.

6) Intrusion set: An intrusion set is a grouped set of adversarial behaviours and resources with common properties that is believed to be orchestrated by a single organization.

7) Malware: Malware is a type of TTP that is also known as malicious code and malicious software, and refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.

8) Observed data: Observed data conveys information that was observed on systems and networks using the cyber observable specification defined in parts 3 and 4 of this specification.

9) Report: Reports are collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.

10) Threat actor: Threat actors are actual individuals, groups, or organizations believed to be operating with malicious intent.

11) Tool: Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed.

12) Vulnerability: A vulnerability is "a mistake in software that can be directly used by a hacker to gain access to a system or network".

Two SROs are defined in [b-STIX2.0-Part 2] as follows:

1) Relationship: The relationship object is used to link together two SDOs in order to describe how they are related to each other.

2) Sighting: A sighting denotes the belief that something in CTI (e.g., an indicator, malware, tool, threat actor) was seen.

6.3 STIX characteristics and tools

This Recommendation should consider the following characteristics defined in [b-STIX2.0] (and/or [b-STIX1.2.1]):

– JSON/XML schemas: [b-STIX2.0] uses JSON schema [b-RFC7159] to represent the six objects and properties. In addition, [b-STIX1.2.1] uses XML schema.

– STIX domain object: All objects in STIX are at the top-level. These objects are called STIX SDO. Some object properties use a reference to another object's id directly (e.g., created_by_ref), but most relationships are expressed using the top-level relationship object.

– STIX relationship object: [b-STIX2.0-Part 2] introduces a top-level relationship object, which links two other top-level objects via a named relationship type.

This Recommendation should use the following set of tools defined in [b-STIX2.0 tool]:

– STIX validator: The STIX validator tool is a useful resource for validating that STIX JSON content conforms to the 2.0 specification.

– Pattern validator: STIX patterns are expressions that represent cyber observable objects within a STIX indicator SDO. They are helpful for modelling intelligence that indicates cyber activity. This tool simply makes sure patterning syntax adheres to the patterning expression.

– STIX visualization: The STIX visualization tool helps to convert JSON into a more concise, legible diagram.

– STIX elevator: The elevator tool helps to serve as the tool to convert STIX 1.x to STIX 2.0 and will provide a best-effort conversion from 1.x to 2.0, where x = 1,2.

– STIX pattern matcher: The pattern matching tool provides a way to compare STIX observed data against STIX indicator patterns.

7 Use cases for STIX 2.0

This Recommendation provides various use cases for how the STIX language may be used to support cyber threat intelligence and information sharing context. It is targeted to support a range of use cases (UCs) involved in cyber threat management, including: analysing cyber threats (UC1, clause 7.2.1), specifying indicator patterns for cyber threats (UC2, clause 7.2.2), and managing cyber threat response activities (UC3, clause 7.2.3). Sharing cyber threat information (UC4) is not addressed in this Recommendation. An overview of an example STIX use case is depicted in Figure 1. A use case for STIX 1.2 is provided in Annex A.

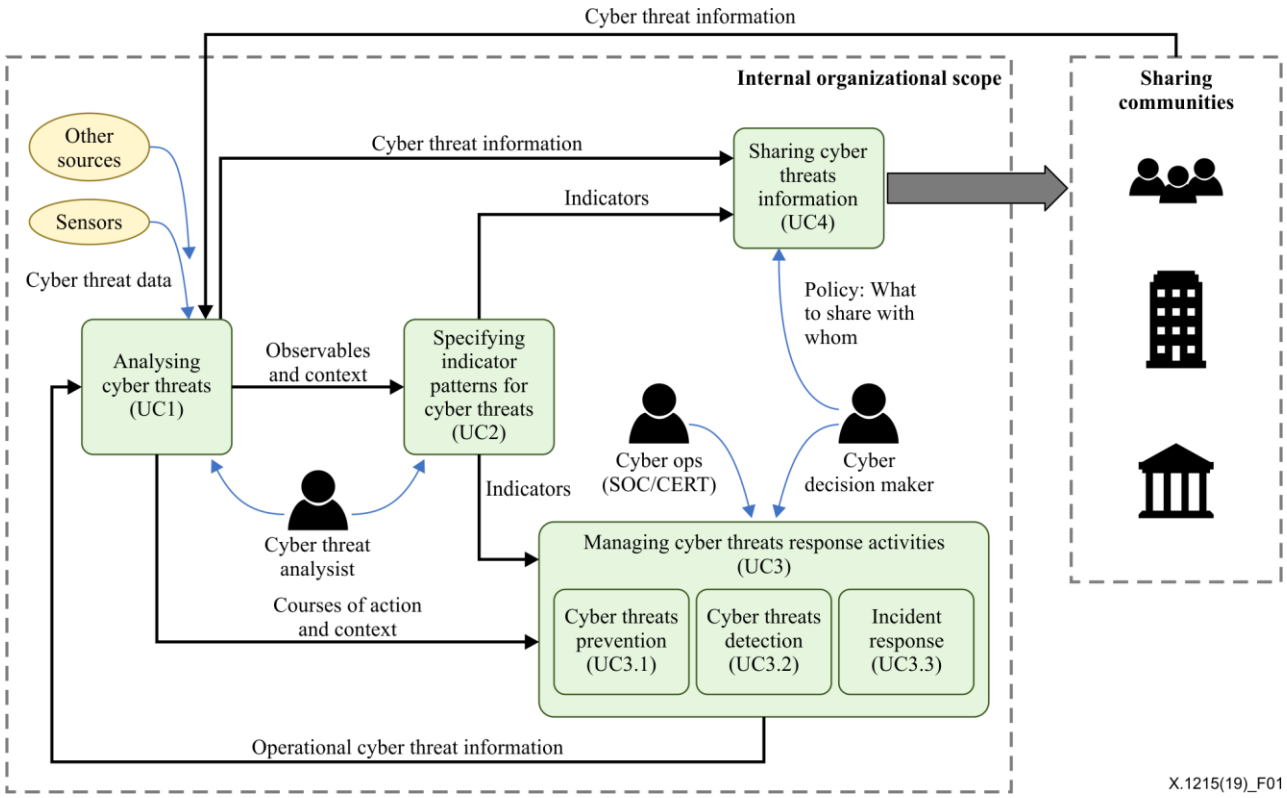

Figure 1 – Overview of STIX use case

7.1 Ransomware use case with STIX 2.0

Ransomware is a kind of malicious software that infects computer systems, restricts access to the victim's data and requires a ransom. Because access to the computer is limited, a victim will be forced to pay the entity who developed the malicious program in order to remove the restriction. Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading, or opening when it arrives as an e-mail attachment.

Recently, WannaCry ransomware began affecting computers worldwide; it propagated automatically between computers without user interaction. Unlike ordinary ransomware, which is spread via e-mail attachments, the WannaCry infection vector only required vulnerable systems to be connected to the Internet. WannaCry ransomware encrypts various files such as document files, compressed files, database files and virtual machine files.

This clause outlines the ransomware use case for how the STIX 2.0 language may be used to support the cyber threat management against WannaCry ransomware.

7.1.1 Analysing cyber threats

This clause provides the analysed information of ransomware (WannaCrypt) that has been reported by malicious code attacks worldwide using server message block version 2 (SMBv2) remote code execution vulnerability ransomware.

7.1.1.1 Identity

The information of an observer could be defined as an identity object.

7.1.1.2 Observed data

It is observed that an e-mail for a shipping notification was received with an archive of egg files and 52 command and control (CnC) server domains (only two CnC server domains in this example) had been observed.

```
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
     "0": {
     "type": "email-addr",
     "value": john@mail.com,
     "display_name" : "john"
     }
    }
}
{
   "type": "observed-data",
   "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb2",
   "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2017-04-14T19:37:11.213Z",
   "modified": "2017-04-14T19:37:11.213Z",
   "first_observed": "2017-04-14T21:37:11.213Z",
   "last_observed": "2017-04-14T21:37:11.213Z",
   "number_observed": 1,
   "objects": {
    "0: {
    "type": "email-message",
    "to_refs" : "0",
    "is_multipart": false,
    "subject" : "FedEx Shipping Information",
    "body_multipart": [
      {
      "content_type": "application/zip",
      "content_disposition": "attachment; filename=\" ipa_email_attachment_zip\"",
      "body_raw_ref": "5"
      }
    ]
   }
   }
}
{
   "type": "observed-data",
```

```
    "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb3,
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-04-14T19:37:11.213Z",
    "modified": "2017-04-14T19:37:11.213Z",
    "first_observed": "2017-04-14T21:37:11.213Z",
    "last_observed": "2017-04-14T21:37:11.213Z",
    "number_observed": 1,
    "objects": {
      "0": {
      "type":"domain-name",
      "value":" 43bwabxrduicndiocpo.net",
      "description" : "CnC server"
       }
    }
},
{
    "type": "observed-data",
    "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb4",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-04-14T19:37:11.213Z",
    "modified": "2017-04-14T19:37:11.213Z",
    "first_observed": "2017-04-14T21:37:11.213Z",
    "last_observed": "2017-04-14T21:37:11.213Z",
    "number_observed": 1,
    "objects": {
    "0": {
      "type":"domain-name",
      "value":" dyc5m6xx36kxj.net",
      "description" : "CnC server"
       }
    }
}
```

7.1.1.3 TTP

It is reported that a ransomware attack targeting an individual computer was observed; the attack pattern is the activity of a targeted attack using malware and a relationship object that uses malware can be created as an attack pattern.

```
{
    "type": "attack-pattern",
    "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": " Targeted Malware ",
```

```
   "external_references": [
     {
       "source_name": "capec",
       "id": "CAPEC-542"
     }
   ]
 }

{
   "type": "malware",
   "id": "malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
   "created_by_ref" : "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2014-02-20T09:16:08.989000Z",
   "modified": "2014-02-20T09:16:08.989000Z",
   "name": "WannaCry",
   "labels": [
     "Ransomware"
   ]
}

{
   "type": "relationship",
   "id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "relationship_type": "uses",
   "source_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 },
```

7.1.1.4 Vulnerability

It is reported that the vulnerability is related to common vulnerability and exposures CVE-2017-0147 and CVE-2017-0143, which is ransomware that exploited the SMBv2 remote code execution vulnerability (17.3.14 patch release, MS17-010) on Microsoft Windows. A relationship object that uses malware targeting this vulnerability can be created.

```
{
 "type": "vulnerability",
 "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
 "created": "2016-05-12T08:17:27.000Z",
 "modified": "2016-05-12T08:17:27.000Z",
 "name": "Related CVE Information"
 "external_references": [
   {
```

```
      "source_name": "cve",
      "external_id": "CVE-2017-0147"
    },
   {
      "source_name": "cve",
      "external_id": "CVE-2017-0143"
    }
   ]
}


{
  "type": "relationship",
  "id": "relationship--6ce78886-1027-4800-9301-40c274fd472f",
  "created": "2014-06-30T09:15:17.182Z",
  "modified": "2014-06-30T09:15:17.182Z",
  "relationship_type": "targets",
  "source_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
  "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
}
```


7.1.1.5 Campaign and threat actor

It is reported that two objects are defined as campaign and threat-actor for the information about the ransomware attack. It is defined that the 'attributed-to' relationship can be created for campaign and threat-actor, the 'uses' relationship for campaign and attack pattern and the 'targets' relationship for campaign and vulnerability.


```
{
       "type": "campaign",
       "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
       "created": "2017-05-12T15:50:10.983Z",
       "modified": "2017-05-13T08:33:39.001Z",
       "name": "Ransomware (WannaCrypt) Attack",
       "description": "May 12-13, 2017 infected more than 120,000 computers worldwide. Damage caused by WannaCrypt, a variant of WannaCry, which is distributed via networks in about 100 countries, including Europe and Asia.
The spread of malware is assumed by the hacker group 'Shadow Brokers' who claimed to have stolen hacking tools developed by the US National Security Agency (NSA). The attacker type is Malware Developer motivated by financial (Financial or Economic). Proficiency is Expert. The intruder's intention is Theft",
       "aliases": ["WannaCry"],
       "first_seen": "2017-05-12T04:50:40.123Z",
       "objective": "Theft"
}
{
```

```
      "type": "threat-actor",
      "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
      "created": "2017-05-08T15:50:10.983Z",
      "modified": "2017-05-08T15:50:10.983Z",
      "labels": ["hacker"],
      "roles": ["malware-author"],
     "sophistication": "expert",
     "resource_level": "team",
      "goals": ["Theft the development Tools"],
      "primary_motivation": "organizational-gain",
      "name": "Shadow Brokers”
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "attributed-to",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "uses",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5923",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "targets",
      "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
      "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5924",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
```

```
      "relationship_type": "uses",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
}
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5925",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "attributed-to",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e"
},
{
      "type": "relationship",
      "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5926",
      "created": "2017-08-08T15:50:10.983Z",
      "modified": "2017-08-08T15:50:10.983Z",
      "relationship_type": "targets",
      "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
      "target_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
}
```

7.1.2 Specifying indicator patterns for cyber threats

7.1.2.1 Indicator

It is reported that the malware distribution site URL is defined as an indicator type of URL watch and the relationship object that represents the malware can be created.

```
{
      "type": "indicator",
      "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
      "created": "2017-02-29T13:49:37.079000Z",
      "modified": "2017-06-29T13:49:37.079000Z",
      "labels": [
        "malicious-activity"
      ],
      "name": " Malware distribution site URL",
      "pattern":   "[url:value   =   '43bwabxrduicndiocpo.net']   OR   [url:value   =
'dyc5m6xx36kxj.net']",
      "valid_from": "2017-06-29T13:49:37.079000Z"
},
{
      "type": "relationship",
      "id": "relationship--6ce78886-1027-4800-9301-40c274fd473g",
```

```
      "created": "2017-06-30T09:15:17.182Z",
      "modified": "2017-06-30T09:15:17.182Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
      "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
}
{
   "type": "relationship",
   "id": "relationship--6ce78886-1027-4800-9301-40c274fd473h",
   "created": "2017-06-30T09:15:17.182Z",
   "modified": "2017-06-30T09:15:17.182Z",
   "relationship_type": "indicates",
   "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
   "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
}
```

7.1.3 Managing response activities

7.1.3.1 Course of action

It is noted that there are remedy methods of 'disabling the SMB protocol' and 'software vulnerability patching', which can be defined as course of action (COA) objects. A relationship object that mitigates malware for each object can be created.

```
{
   "type": "course-of-action",
   "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2016-04-06T20:03:48.000Z",
   "modified": "2016-04-06T20:03:48.000Z",
   "name": " Disable the SMB protocol ",
   "description": " Block SMB-related ports (TCP 139, TCP 445) using network firewalls and Windows Firewall"
 }
{
   "type": "course-of-action",
   "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g",
   "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2016-04-06T20:03:48.000Z",
   "modified": "2016-04-06T20:03:48.000Z",
   "name": " Latest Windows Updates ",
   "description": " Download and apply version upgrades and latest security patches through MS update catalog site ",
"external_references": [
       {
       "url": " http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598",
       }
]
```

```
}
{
 "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
   "created": "2016-04-06T20:07:10.000Z",
   "modified": "2016-04-06T20:07:10.000Z",
   "relationship_type": "mitigates",
   "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 }
{
 "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fae",
   "created": "2016-04-06T20:07:10.000Z",
   "modified": "2016-04-06T20:07:10.000Z",
   "relationship_type": "mitigates",
   "source_ref": " course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g ",
   "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
 }
```


7.1.4 Overview of attack scenario using a relationship diagram

Figure 2 shows the relationship between all STIX objects used to describe the use case.

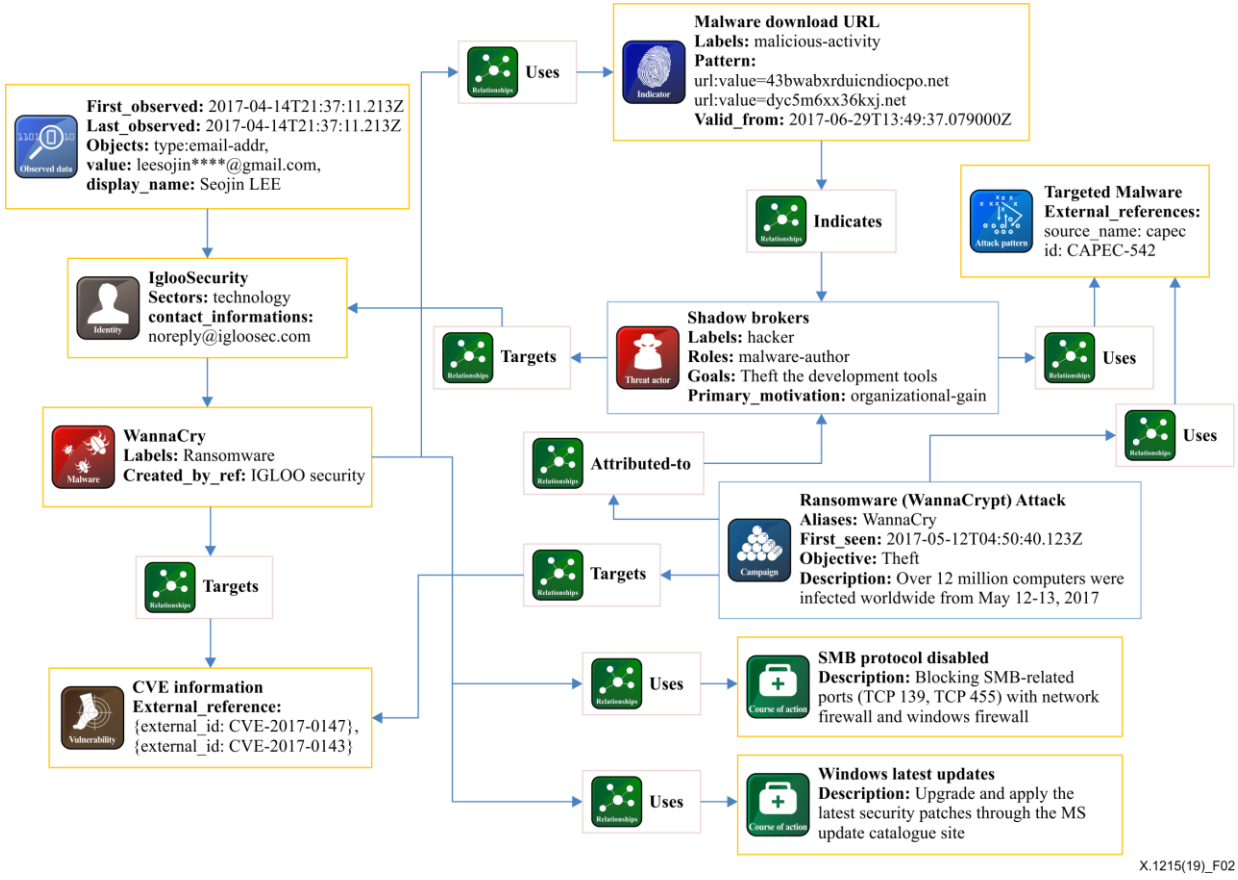

Figure 2 – Relationship between STIX objects for describing the use case

To summarize, the following describes STIX bundle objects incorporating all objects to detect, analyse and respond to the malicious attacks carried out by the so-called WannaCry ransomware.


```
{
   "type": "bundle",
   "id": "bundle--44af6c39-c09b-49c5-9de2-394224b04982",
   "spec_version": "2.0",
   "objects": [
    {
     "type": "identity",
     "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
     "created": "2017-04-14T13:07:49.812Z",
     "modified": "2017-04-14T13:07:49.812Z",
     "name": "IglooSecurity”
     "identity_class": "organization",
     "contact_information": "noreply@igloosec.com",
     "sectors": [
     "technology"
     ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
      "number_observed": 1,
      "objects": {
        “0”: {
          “type”: “email-addr”,
          “value”: john@mail.com,
          “display_name” : “john”
        }
      }
    },
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb2",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
```

```
      "number_observed": 1,
      "objects": {
      "0: {
        "type": "email-message",
        “to_refs” : “0”,
        “is_multipart”: false,
        “subject” : “FedEx Shipping Information”,
        "body_multipart": [
        {
          "content_type": "application/zip",
          "content_disposition":          "attachment;          filename=\₩          "
ipa_email_attachment_zip₩ \"",
          "body_raw_ref": "5"
        }
        ]
        }
      }
    }
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb3,
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
      "number_observed": 1,
      "objects": {
        “0”: {
        “type”:”domain-name”,
        “value”:” 43bwabxrduicndiocpo.net”,
        “description” : “CnC server”
        }
      }
    }
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb4",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T19:37:11.213Z",
      "modified": "2017-04-14T19:37:11.213Z",
      "first_observed": "2017-04-14T21:37:11.213Z",
      "last_observed": "2017-04-14T21:37:11.213Z",
```

```
    "number_observed": 1,
    "objects": {
    "0": {
    "type":"domain-name",
    "value":" dyc5m6xx36kxj.net",
    "description" : "CnC server"
    }
    }
  },
  {
   "type": "attack-pattern",
   "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "name": " Targeted Malware ",
   "external_references": [
   {
    "source_name": "capec",
    "id": "CAPEC-542"
   }
   ]
  },
  {
   "type": "malware",
   "id": "malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
   "created_by_ref" : "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
   "created": "2014-02-20T09:16:08.989000Z",
   "modified": "2014-02-20T09:16:08.989000Z",
   "name": " WannaCry ",
   "labels": [
    " Ransomware "
   ]
  },
  {
   "type": "vulnerability",
   "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
   "created": "2016-05-12T08:17:27.000Z",
   "modified": "2016-05-12T08:17:27.000Z",
   "name": " Related CVE Information"
   "external_references": [
    {
    "source_name": "cve",
    "external_id": "CVE-2017-0147"
    },
```

```
      {
      "source_name": "cve",
      "external_id": "CVE-2017-0143"
      }
     ]
    },
    {
     "type": "campaign",
     "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
     "created": "2017-05-12T15:50:10.983Z",
     "modified": "2017-05-13T08:33:39.001Z",
     "name": " Ransomware (WannaCrypt) Attack ",
    "description": "May 12-13, 2017 infected more than 120,000 computers worldwide. Damage caused by WannaCrypt, a variant of WannaCry, which is distributed via networks in about 100 countries, including Europe and Asia.
     The spread of malware is assumed by the hacker group 'Shadow Brokers' who claimed to have stolen hacking tools developed by the US National Security Agency (NSA). The at tacker type is Malware Developer motivated by financial (Financial or Economic). Profic iency is Expert. The intruder's intention is Theft ",
     "aliases": ["WannaCry"],
     "first_seen": "2017-05-12T04:50:40.123Z",
     "objective": "Theft"
    }
    {
     "type": "threat-actor",
     "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
     "created": "2017-05-08T15:50:10.983Z",
     "modified": "2017-05-08T15:50:10.983Z",
     "labels": ["hacker"],
     "roles": ["malware-author"],
     "sophistication": "expert",
     "resource_level": "team",
     "goals": ["Theft the development Tools"],
     "primary_motivation": "organizational-gain",
     "name": "Shadow Brokers”
    },
    {
     "type": "indicator",
     "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
     "created": "2017-02-29T13:49:37.079000Z",
     "modified": "2017-06-29T13:49:37.079000Z",
     "labels": [
     "malicious-activity"
     ],
     "name": " Malware distribution site URL ",
     "pattern":    "[url:value    =    ‘43bwabxrduicndiocpo.net']    OR    [url:value    =
```

```
'dyc5m6xx36kxj.net']",
     "valid_from": "2017-06-29T13:49:37.079000Z"
    },
    {
      "type": "course-of-action",
      "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "name": " Disable the SMB protocol ",
      "description": " Block SMB-related ports (TCP 139, TCP 445) using network
firewalls and Windows Firewall "
    },
    {
     "type": "course-of-action",
     "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g",
     "created_by_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
     "created": "2016-04-06T20:03:48.000Z",
     "modified": "2016-04-06T20:03:48.000Z",
     "name": " Latest Windows Updates ",
     "description": " Download and apply version upgrades and latest security patches
through MS update catalog site ",
     "external_references": [
     {
      "url": " http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598"
     }
     ]
    },
    {
     "type": "relationship",
     "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
     "created": "2017-08-08T15:50:10.983Z",
     "modified": "2017-08-08T15:50:10.983Z",
     "relationship_type": "uses",
     "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
     "target_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
    },
    {
     "type": "relationship",
     "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5923",
     "created": "2017-08-08T15:50:10.983Z",
     "modified": "2017-08-08T15:50:10.983Z",
     "relationship_type": "targets",
     "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
     "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
    },
```

```
{
 "type": "relationship",
 "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5924",
 "created": "2017-08-08T15:50:10.983Z",
 "modified": "2017-08-08T15:50:10.983Z",
 "relationship_type": "uses",
 "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
 "target_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
},
{
 "type": "relationship",
 "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5925",
 "created": "2017-08-08T15:50:10.983Z",
 "modified": "2017-08-08T15:50:10.983Z",
 "relationship_type": "attributed-to",
 "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e"
 "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
},
{
  "type": "relationship",
  "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5926",
  "created": "2017-08-08T15:50:10.983Z",
  "modified": "2017-08-08T15:50:10.983Z",
  "relationship_type": "targets",
  "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
  "target_ref": " identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
 "type": "relationship",
 "id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",
 "created": "2016-05-12T08:17:27.000Z",
 "modified": "2016-05-12T08:17:27.000Z",
 "relationship_type": "uses",
 "source_ref": " attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
 "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
},
{
 "type": "relationship",
 "id": "relationship--6ce78886-1027-4800-9301-40c274fd472f",
 "created": "2014-06-30T09:15:17.182Z",
 "modified": "2014-06-30T09:15:17.182Z",
 "relationship_type": "targets",
 "source_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
 "target_ref": " vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061"
```

```
    },
    {
     "type": "relationship",
     "id": "relationship--6ce78886-1027-4800-9301-40c274fd473g",
     "created": "2017-06-30T09:15:17.182Z",
     "modified": "2017-06-30T09:15:17.182Z",
     "relationship_type": "indicates",
     "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
     "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
    },
    {
     "type": "relationship",
     "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
     "created": "2016-04-06T20:07:10.000Z",
     "modified": "2016-04-06T20:07:10.000Z",
     "relationship_type": "mitigates",
     "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
     "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
    },
    {
     "type": "relationship",
     "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fae",
     "created": "2016-04-06T20:07:10.000Z",
     "modified": "2016-04-06T20:07:10.000Z",
     "relationship_type": "mitigates",
     "source_ref": " course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3ef3g ",
     "target_ref": " malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111"
    },
    {
     "type": "relationship",
     "id": "relationship--6ce78886-1027-4800-9301-40c274fd473h",
     "created": "2017-06-30T09:15:17.182Z",
     "modified": "2017-06-30T09:15:17.182Z",
     "relationship_type": "indicates",
     "source_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
     "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"
    }
   ]
}
```


7.2 Use case for cyberattack on a cryptocurrency exchange

This clause describes a use case for the attack carried out by the so-called "Lazarus APT group", the threat actor, on June 20, 2018, against the cryptocurrency exchange in Korea.

In this scenario, the threat actor sent a phishing e-mail with malicious code to the cryptocurrency exchange staff. The phishing e-mail was accompanied by a malicious postscript hidden-document

file that can download malicious dynamic link libraries (DLLs) later. The document file exploited the vulnerability of the Hangul word processor to execute the postscript and as a result, the malicious DLL file was installed on a user's PC. The malicious DLL file captured the control of the user's PC and accessed the servers which were accessible to the inside of the exchange. As a result, the attacker was able to accesses to the exchange's cryptocurrency wallet and withdrew a substantial amount of money from that wallet.

7.2.1 UC1: Analysing cyber threats

Attacks on cryptocurrency exchanges have been reported several times, happening between June and July 2018. In this scenario, the hacking incident against so-called company, "BC-Company" cryptocurrency exchange is analysed.

7.2.1.1 Identity

Basic identifying information of the observer can be modelled with the identity object. The organization that observed the incident and the place where the incident occurred can be modelled as identity objects.

To identify the originator for the STIX report object, the security monitoring companies, WINS and IGLOO security, are represented as the identity objects. The target of the incident is modelled as an identity object with the property named "BC-Company.com", which is a pseudonymous name. This object is specified in the where_sighted_refs of the sighting object to be discussed later and is used as an attack target for attack patterns and malware.

```
{
"type": "identity",
"id": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
"created": "2018-07-20T10:03:57.843Z",
"modified": "2018-07-20T10:03:57.843Z",
"name": "WINS",
"identity_class": "organization",
"sectors": [
"technology"
],
"contact_information": "sangpil@wins21.co.kr"
},
{
"type": "identity",
"id": "identity--650de76c-7638-4026-8900-ec7de2fc757f",
"created": "2018-07-20T10:03:57.886Z",
"modified": "2018-07-20T10:03:57.886Z",
"name": "BC-Company.com – pseudonymous URL",
"identity_class": "organization"
},
```

7.2.1.2 Observed data

Observed data represents machine-generated raw information and are different from indicators which dictate more of an intelligence assertion. Observed data object contains cyber-observable information that was captured on systems and networks such as IP addresses, files, and URL's. In this scenario, a file was observed. Another reference, sighting_of_ref, contains the ID of the SDO

that was sighted, which in this case is the observed-data object.

The cryptocurrency exchange observed a file delivered via an e-mail. The file name and the sender's e-mail address are represented by the observed data object. Observed data objects that are observed elsewhere are represented as sighting objects. The observed location is represented by the where_sighted_rerfs property.


```
{
    "type": "observed-data",
    "id": "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
    "created": "2018-07-20T10:03:57.887Z",
    "modified": "2018-07-20T10:03:57.887Z",
    "first_observed": "2018-07-20T10:03:57.887095Z",
    "last_observed": "2018-07-20T10:03:57.887101Z",
    "number_observed": 1,
    "objects": {
        "0": {
            "type": "email-addr",
            "value": "****@hanmail.net"
        },
        "1": {
            "type": "file",
            "name": "ICT staff profile.hwp"
        }
    }
},
{
    "type": "sighting",
    "id": "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21",
    "created": "2018-07-20T10:03:57.896Z",
    "modified": "2018-07-20T10:03:57.896Z",
    "count": 1,
    "sighting_of_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "observed_data_refs": [
        "observed-data--45eeee3b-a455-404e-8612-613168eeb693"
    ],
    "where_sighted_refs": [
        "identity--650de76c-7638-4026-8900-ec7de2fc757f"
    ]
}
```


7.2.1.3 Tactics, techniques and procedures

This clause describes the nature to characterize how and what adversary behaviour is.

The attack originated from the attachment in a phishing e-mail, where two types of malicious codes used were used in the attack. Phishing attacks are specified as common attack pattern enumeration and classification (CAPEC)-163 through the attack pattern object. The malicious code delivered from the phishing e-mail downloads the malicious DLL exploiting the CVE-2015-2545

vulnerability. Therefore, the labels of malware objects are marked as exploit and dropper. In the case of malicious DLLs received later, the remote-access-trojan is labeled as a malicious code that takes control of the user's PC.

The relation between two malicious codes was specified as a 'related-to' type, indicating that there is a relationship between the malicious document and the malicious DLL.

When the spear phishing occurred, the attacker used a highly disguised document. Since the attack is aimed at the cryptocurrency exchange, a relationship object of type 'target' is used.


```
{
    "type": "attack-pattern",
    "id": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
    "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
    "created": "2018-07-20T10:03:57.851Z",
    "modified": "2018-07-20T10:03:57.851Z",
    "name": "Sphere Phishing",
    "external_references": [
{
    "source_name": "capec",
    "external_id": "CAPEC-163"
}
    ]
},
{
    "type": "malware",
    "id": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.845Z",
    "modified": "2018-07-20T10:03:57.845Z",
    "name": " malicious document (HWP file)",
    "description": "A purpose for downloading the RAT in the document file that contains the postscript in the attachment of the spear fishing e-mail",
    "labels": [
"exploit",
"dropper"
    ]
},
{
    "type": "malware",
    "id": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.847Z",
    "modified": "2018-07-20T10:03:57.847Z",
    "name": "Malicious DLL (C2 communication)",
    "description": " A tool for remote control of the attacker controls to steal the bit coin.",
    "labels": [
```

```
"exploit",
"dropper"
    ]
},
{
    "type": "relationship",
    "id": "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "targets",
    "source_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
    "target_ref": "identity--650de76c-7638-4026-8900-ec7de2fc757f"
},
{
    "type": "relationship",
    "id": "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
    "created": "2018-07-20T10:03:57.889Z",
    "modified": "2018-07-20T10:03:57.889Z",
    "relationship_type": "related-to",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "targets",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
},
```


7.2.1.4 Vulnerability

Here, CVE-2015-2545, a vulnerability that hides malicious postscript in a Hangul word processor document and makes it run, is used. Vulnerability object is used to model this vulnerability. The relationship object also indicates the relationship between malicious code and vulnerability.


```
{
    "type": "vulnerability",
    "id": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
    "created": "2018-07-20T10:03:57.885Z",
    "modified": "2018-07-20T10:03:57.885Z",
    "name": " CVE information",
    "external_references": [
{
```

```
    "source_name": "cve",
    "external_id": "CVE-2015-2545"
}
    ]
},
{
    "type": "relationship",
    "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "targets",
    "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
    "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
}
```

7.2.1.5 Campaign and threat actor

Since Lazarus APT Group has spread spear phishing e-mails embedded with malicious code in order to steal the cryptocurrency stored in the cryptocurrency exchange.

The goal of the threat-actor object is represented as "Steal cryptographic currency" in the 'goals' property. Since a malicious document was created, the 'roles' property is set to as 'malware-author' in the role property. Since it was used to commit a crime, the 'label' property is set to 'crime-syndicate'.

The attack on the cryptocurrency exchange is represented through the campaign object and the 'objective' property is set to 'Theft'.

Attack techniques and malicious code objects used in attack campaigns are represented by relationship objects using 'use' type.

```
        {
            "type": "campaign",
            "id": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.850Z",
            "modified": "2018-07-20T10:03:57.850Z",
            "name": " Hacking incident for the BC-Company on June 20, 2018",
            "description": "The Lazarus APT group launched a campaign to hack the BC-
Company cryptocurrency exchange. The attack method was to send the malicious code to
the target through the spear phishing technique, and then installed the DLL file which
was able to communicate with the C2 server and use them to steal the Bit coin.",
            "objective": "Theft"
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.848Z",
            "modified": "2018-07-20T10:03:57.848Z",
```

```
            "name": "Lazarus APT Group",
            "description": "The Lazarus APT group has been known to use spear phishing techniques to disguise social issues as document files and use them. Also, it is widely known in Korea as an example of exploiting a vulnerability that implements postscript in a Hangul document.",
            "roles": [
                "malware-author"
            ],
            "goals": [
                "Steal cryptographic currency"
            ],
            "primary_motivation": "organizational-gain",
            "labels": [
                "crime-syndicate"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692"
        },
        {
            "type": "relationship",
            "id": "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "attribute-to",
            "source_ref": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "target_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3"
        },
        {
            "type": "relationship",
            "id": "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        }
```

7.2.2 UC2: Specifying indicator patterns for cyber threats

7.2.2.1 Indicator

Indicator objects identify malicious documents and malicious DLLs. The pattern property in the indicator object for malicious documents represents either URLs or file hash values for downloading malicious DLLs. In this scenario, the malicious DLL patterns in the indicator object represent the command and control (C2) URL and the file's hash value. This makes it possible to register as a policy. Several relationship objects with type 'indicates' indicate the relationship between two malicious codes.


```
{
    "type": "indicator",
    "id": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.875Z",
    "modified": "2018-07-20T10:03:57.875Z",
    "name": "C2 URL",
    "pattern": "[url:value = 'https://tpddata.com/skin/skin-6.html' OR url:value = 'https://tpddata.com/skin/skin-8.html']",
    "valid_from": "2018-07-20T10:03:57.875238Z",
    "labels": [
"malicious-activity"
    ]
},
{
    "type": "indicator",
    "id": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
    "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
    "created": "2018-07-20T10:03:57.853Z",
    "modified": "2018-07-20T10:03:57.853Z",
    "name": " Hash value of malicious document",
    "pattern": "[file:hashes.'SHA-256' = 'e498630abe9a91485ba42698a35c2a0d8e13fe5cccde65479bf3033c45e7d431']",
    "valid_from": "2018-07-20T10:03:57.853427Z",
    "labels": [
"malicious-activity"
    ]
},
{
    "type": "indicator",
    "id": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
    "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
    "created": "2018-07-20T10:47:50.715Z",
    "modified": "2018-07-20T10:47:50.715Z",
    "name": "Hash value of malicious DLL",
    "pattern": "[file:hashes.'SHA-256' =
```

```
'5b1663d5eb565caccca188b6ff8a36291da32f368211e6437db2dc2e9cd']",
    "valid_from": "2018-07-20T10:47:50.71577Z",
    "labels": [
"malicious-activity"
    ]
},
{
    "type": "indicator",
    "id": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
    "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
    "created": "2018-07-20T10:47:50.719Z",
    "modified": "2018-07-20T10:47:50.719Z",
    "name": " a list of C2 URLs",
    "pattern": "[url:value = 'www.51up.com/ace/main.asp' OR url:value =
'paulkaren.com/synthpop/main.asp' OR url:value = 'shieldonline.co.za/sitemap.asp']",
    "valid_from": "2018-07-20T10:47:50.719761Z",
    "labels": [
"malicious-activity"
    ]
}
{
    "type": "relationship",
    "id": "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
    "created": "2018-07-20T10:03:57.887Z",
    "modified": "2018-07-20T10:03:57.887Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
},
{
    "type": "relationship",
    "id": "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
    "created": "2018-07-20T10:47:50.725Z",
    "modified": "2018-07-20T10:47:50.725Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
    "created": "2018-07-20T10:47:50.726Z",
    "modified": "2018-07-20T10:47:50.726Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
```

```
    "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
},
{
    "type": "relationship",
    "id": "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
    "created": "2018-07-20T10:03:57.887Z",
    "modified": "2018-07-20T10:03:57.887Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
}
```


7.2.3 UC3: Managing cyber threat response activities

7.2.3.1 Course of action

In this attack scenario, course of action by the response team is divided into detection and response. First, the malicious document is executed and then the attack begins.

The hash value of the malicious document is registered with the security policy in the malware analyzing tool, such as YARA. The event data recorder (EDR) can detect the attack when the file with the hash value is executed. In addition, the network security device responds by blocking the traffic to the download URL of the malicious DLL so that the downloading of the malicious DLL is blocked so the control rights of the PC are not stolen. If a malicious DLL has been hijacked, the network device can block malicious activity by blocking traffic to the C2 URL.


```
{
    "type": "course-of-action",
    "id": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
    "created": "2018-07-20T10:03:57.884Z",
    "modified": "2018-07-20T10:03:57.884Z",
    "name": "Establishment of EDR policy",
    "description": " Registration of DLL downloading URL and a list of C2 URLs as a reputation policy"
},
{
    "type": "course-of-action",
    "id": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
    "created": "2018-07-20T10:03:57.883Z",
    "modified": "2018-07-20T10:03:57.883Z",
    "name": "EDR policy establishment",
    "description": "Registration of SHA256 hash values for malicious documents and malicious DLLs as blocking policies "
},
{
    "type": "relationship",
    "id": "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
```

```
    "relationship_type": "mitigates",
    "source_ref": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
},
{
    "type": "relationship",
    "id": "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
    "created": "2018-07-20T10:03:57.888Z",
    "modified": "2018-07-20T10:03:57.888Z",
    "relationship_type": "mitigates",
    "source_ref": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
    "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
}
```


7.2.4 Relationship diagram and bundle object

Figure 3 shows the relationship between all objects to describe the use case.

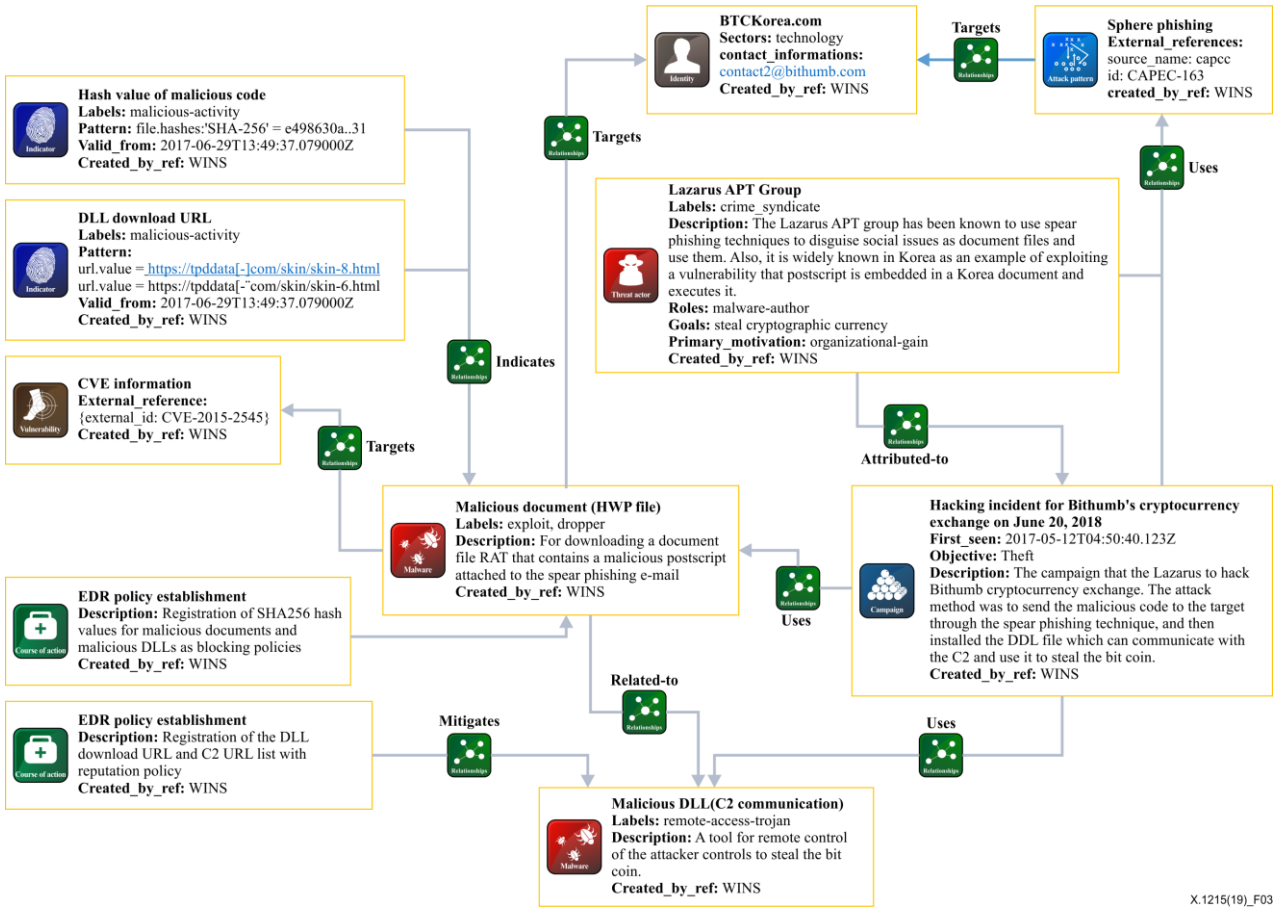

Figure 3 – Relationship between STIX objects for describing the use case

To summarize, the following describes a STIX bundle object incorporating all objects to detect, analyse and respond to the malicious attacks carried out by the so-called Lazarus.

```
{
    "type": "bundle",
    "id": "bundle--42d953f0-0a5c-4b82-b223-b22ec85da222",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "campaign",
            "id": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.850Z",
            "modified": "2018-07-20T10:03:57.850Z",
            "name": "Hacking incident for BC-Company on June 20, 2018",
            "description": "The Lazarus APT group launched a campaign to hack the BC-
Company cryptocurrency exchange. The attack method was to send the malicious code to
the target through the spear phishing technique, and then installed the DLL file which
was able to communicate with the C2 server and use them to steal the Bit coin.",
            "objective": "Theft"
        },
        {
            "type": "relationship",
            "id": "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692"
        },
        {
            "type": "course-of-action",
            "id": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "created": "2018-07-20T10:03:57.883Z",
            "modified": "2018-07-20T10:03:57.883Z",
            "name": "Establishment of EDR policy ",
            "description": "Registration of DLL downloading URL and a list of C2 URLs
as a reputation policy"
        },
        {
            "type": "relationship",
            "id": "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "related-to",
            "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
```

```
            "type": "malware",
            "id": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.847Z",
            "modified": "2018-07-20T10:03:57.847Z",
            "name": "Malicious DLL (C2 communication)",
            "description": "A tool for remote control of the attacker controls to steal
the bit coin.",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
            "created": "2018-07-20T10:47:50.725Z",
            "modified": "2018-07-20T10:47:50.725Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "relationship",
            "id": "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
            "created": "2018-07-20T10:47:50.726Z",
            "modified": "2018-07-20T10:47:50.726Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "report",
            "id": "report--91ed4b5a-5375-42cf-be5c-5fecff6d6da6",
            "created": "2018-07-20T10:03:57.897Z",
            "modified": "2018-07-20T10:03:57.897Z",
            "name": "Report on hacking incident for crypto currency exchange on
2018/06/20.",
            "published": "2018-07-20T10:03:57.897114Z",
            "object_refs": [
                "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
                "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
                "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
                "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
                "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
```

```
            "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
            "identity--650de76c-7638-4026-8900-ec7de2fc757f",
            "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
            "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
            "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
            "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
            "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
            "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
            "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
            "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
            "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
            "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
            "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21"
        ],
        "labels": [
            "threat-report"
        ]
    },
    {
        "type": "identity",
        "id": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
        "created": "2018-07-20T10:03:57.843Z",
        "modified": "2018-07-20T10:03:57.843Z",
        "name": "WINS",
        "identity_class": "organization",
        "sectors": [
            "technology"
        ],
        "contact_information": "sangpil@wins21.co.kr"
    },
    {
        "type": "relationship",
        "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
```

```
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "targets",
            "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
        },
        {
            "type": "course-of-action",
            "id": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "created": "2018-07-20T10:03:57.884Z",
            "modified": "2018-07-20T10:03:57.884Z",
            "name": "EDR policy establishment”,
            "description": "Registration of DLL downloading URL and a list of C2 URLs
as a reputation policy"
        },
        {
            "type": "relationship",
            "id": "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "mitigates",
            "source_ref": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "relationship",
            "id": "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "vulnerability",
            "id": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
            "created": "2018-07-20T10:03:57.885Z",
            "modified": "2018-07-20T10:03:57.885Z",
            "name": "CVE information",
            "external_references": [
                {
                    "source_name": "cve",
                    "external_id": "CVE-2015-2545"
                }
            ]
```

```
        },
        {
            "type": "relationship",
            "id": "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "mitigates",
            "source_ref": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "indicator",
            "id": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.875Z",
            "modified": "2018-07-20T10:03:57.875Z",
            "name": "C2 URL",
            "pattern":   "[url:value   =   'https://tpddata.com/skin/skin-6.html'   OR
url:value = 'https://tpddata.com/skin/skin-8.html']",
            "valid_from": "2018-07-20T10:03:57.875238Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "attack-pattern",
            "id": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.851Z",
            "modified": "2018-07-20T10:03:57.851Z",
            "name": "Sphere Phishing",
            "external_references": [
                {
                    "source_name": "capec",
                    "external_id": "CAPEC-163"
                }
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "attribute-to",
            "source_ref": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
```

```
            "target_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3"
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.848Z",
            "modified": "2018-07-20T10:03:57.848Z",
            "name": "Lazarus APT Group",
            "description": "The Lazarus APT group has been known to use spear phishing
techniques to disguise social issues as document files and use them. Also, it is widely
known in Korea as an example of exploiting a vulnerability that implements postscript
in a Hangul document.",
            "roles": [
                "malware-author"
            ],
            "goals": [
                "Steal cryptographic currency"
            ],
            "primary_motivation": "organizational-gain",
            "labels": [
                "crime-syndicate"
            ]
        },
        {
            "type": "identity",
            "id": "identity--650de76c-7638-4026-8900-ec7de2fc757f",
            "created": "2018-07-20T10:03:57.886Z",
            "modified": "2018-07-20T10:03:57.886Z",
            "name": "BC-Company.com",
            "identity_class": "organization"
        },
        {
            "type": "malware",
            "id": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.845Z",
            "modified": "2018-07-20T10:03:57.845Z",
            "name": "Malicious document(HWPfile)",
            "description": "A purpose for downloading the RAT in the document file that
contains the postscript in the attachment of the spear fishing e-mail ",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
```

```
        {
            "type": "identity",
            "id": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.844Z",
            "modified": "2018-07-20T10:03:57.844Z",
            "name": "IGLOO Security",
            "identity_class": "organization",
            "sectors": [
                "technology"
            ],
            "contact_information": "noreply@igloosec.co.kr"
        },
        {
            "type": "relationship",
            "id": "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "target_ref": "identity--650de76c-7638-4026-8900-ec7de2fc757f"
        },
        {
            "type": "observed-data",
            "id": "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
"first_observed": "2018-07-20T10:03:57.887095Z",
            "last_observed": "2018-07-20T10:03:57.887101Z",
            "number_observed": 1,
            "objects": {
                "0": {
                    "type": "email-addr",
                    "value": "****@hanmail.net"
                },
                "1": {
                    "type": "file",
                    "name": " ICT staff profile.hwp"
                }
            }
        },
        {
            "type": "sighting",
            "id": "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21",
            "created": "2018-07-20T10:03:57.896Z",
```

```
            "modified": "2018-07-20T10:03:57.896Z",
            "count": 1,
            "sighting_of_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "observed_data_refs": [
                "observed-data--45eeee3b-a455-404e-8612-613168eeb693"
            ],
            "where_sighted_refs": [
                "identity--650de76c-7638-4026-8900-ec7de2fc757f"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "relationship",
            "id": "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "indicator",
            "id": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.853Z",
            "modified": "2018-07-20T10:03:57.853Z",
            "name": "Hash value of malicious document",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'e498630abe9a91485ba42698a35c2a0d8e13fe5cccde65479bf3033c45e7d431']",
            "valid_from": "2018-07-20T10:03:57.853427Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
```

```
            "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
                    "created": "2018-07-20T10:47:50.715Z",
            "modified": "2018-07-20T10:47:50.715Z",
            "name": "Hash value of malicious DLL",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'5b1663d5eb565caccca188b6ff8a36291da32f368211e6437db2dc2e9cd']",
            "valid_from": "2018-07-20T10:47:50.71577Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
            "created": "2018-07-20T10:47:50.719Z",
            "modified": "2018-07-20T10:47:50.719Z",
            "name": "a List of C2 URLs",
            "pattern":  "[url:value  =  'www.51up.com/ace/main.asp'  OR  url:value  =
'paulkaren.com/synthpop/main.asp' OR url:value = 'shieldonline.co.za/sitemap.asp']",
            "valid_from": "2018-07-20T10:47:50.719761Z",
            "labels": [
                "malicious-activity"
            ]
        }
    ]
}
```

Annex A

Ransomware use case with STIX 1.2

(This annex forms an integral part of this Recommendation.)

This annex outlines the ransomware use case for how the STIX 1.2 language may be used to support the cyber threat management against WannaCry ransomware.

A.1 Analysing cyber threats

This clause provides the analysed information of ransomware (WannaCrypt) which has been reported by malicious code attacks worldwide using SMBv2 remote code execution vulnerability ransomware.

A.1.1 Observable

It is observed that an e-mail for a shipping notification was received with an archive of egg files and 52 CnC server domains had been observed.

```
<stix:Observables xsi:type="cybox:ObservablesType" cybox_major_version="2"
cybox_minor_version="1">
    <cybox:Observable id="IGL:observable_000009392_01">
      <cybox:Event>
        <cybox:Type xsi:type="cyboxVocabs:EventTypeVocab-1.0.1">Email Ops</cybox:Type>
        <cybox:Description>Mail title: FedEx Shipping Information, Sender: john@mail,
Attachment: Before decompression HBDIN_386572.egg (MD5: 447282e7c0ef3b830128476648015831)
After decompression FedEx branch Information.doc (MD5: aa083dde6b58ec6e22a1dafea36f96f8),
Access URL: icanhazip.com (Infection signal transmission) voh2in67mks5uygu.tor2web.cf
(Ransomware private key transmission) </cybox:Description>
        <cybox:Actions>
          <cybox:Action>
            <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Receive</cybox:Type>
            <cybox:Associated_Objects>
              <cybox:Associated_Object id="IGL:object_igloo_email_000009392">
                <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
                  <EmailMessageObj:Header>
                    <EmailMessageObj:To>
                      <EmailMessageObj:Recipient category="e-mail">

<AddressObj:Address_Value>john@mail.com</AddressObj:Address_Value>
                      </EmailMessageObj:Recipient>
                    </EmailMessageObj:To>
                    <EmailMessageObj:Subject>FedEx Shipping
Information</EmailMessageObj:Subject>
                  </EmailMessageObj:Header>
                  <EmailMessageObj:Attachments>
                    <EmailMessageObj:File
object_reference="IGL:object_igloo_email_attachment_zip_000009392"/>
                  </EmailMessageObj:Attachments>
                </cybox:Properties>
                <cybox:Association_Type
xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-
```

```
1.0">Returned</cybox:Association_Type>
              </cybox:Associated_Object>
            </cybox:Associated_Objects>
          </cybox:Action>
        </cybox:Actions>
      </cybox:Event>
    </cybox:Observable>
    <cybox:Observable id="IGL:observable_000009392_02">
      <cybox:Description> CnC Server </cybox:Description>
      <cybox:Object id="IGL:Object-37be6630-b2df-4bf9-8750-3f45ca9e19cf">
        <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
          <URIObj:Value condition="Equals">43bwabxrduicndiocpo.net</URIObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
    <cybox:Observable id="IGL:observable_000009392_03">
      <cybox:Description> CnC Server </cybox:Description>
      <cybox:Object id="IGL:Object-827A13A8-7C90-4A6C-9FEF-F5734BE693F1">
        <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
          <URIObj:Value condition="Equals">dyc5m6xx36kxj.net</URIObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
  </stix:Observables>
```

A.1.2 TTP

It is reported that a ransomware attack targeting an individual computer was observed. The attack pattern is the activity of a targeted attack using malware, and the attack target is information properties in the organization.

```
<stix:TTPs>
    <stix:TTP xsi:type="ttp:TTPType" id="IGL:ttp_000009392">
      <ttp:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </ttp:Intended_Effect>
      <ttp:Behavior>
        <ttp:Attack_Patterns>
          <ttp:Attack_Pattern capec_id="CAPEC-542">
            <ttp:Title>Targeted Malware</ttp:Title>
          </ttp:Attack_Pattern>
        </ttp:Attack_Patterns>
        <ttp:Malware>
          <ttp:Malware_Instance>
            <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Ransomware</ttp:Type>
```

```
            <ttp:Title>WannaCry</ttp:Title>
          </ttp:Malware_Instance>
        </ttp:Malware>
     </ttp:Behavior>
      <ttp:Resources>
        <ttp:Tools>
          <ttp:Tool>
            <cyboxCommon:Type                xsi:type="stixVocabs:AttackerToolTypeVocab-
1.0">Malware</cyboxCommon:Type>
          </ttp:Tool>
        </ttp:Tools>
      </ttp:Resources>
      <ttp:Victim_Targeting>
        <ttp:Targeted_Systems       xsi:type="stixVocabs:SystemTypeVocab-1.0">Enterprise
Systems</ttp:Targeted_Systems>
        <ttp:Targeted_Information            xsi:type="stixVocabs:InformationTypeVocab-
1.0">Information Assets</ttp:Targeted_Information>
      </ttp:Victim_Targeting>
      <ttp:Exploit_Targets>
        <ttp:Exploit_Target>
          <stixCommon:Exploit_Target idref="IGL:et_000009392"/>
        </ttp:Exploit_Target>
      </ttp:Exploit_Targets>
    </stix:TTP>
  </stix:TTPs>
```

A.1.3 Exploit target

It is reported that the vulnerability is related to the vulnerability (CVE-2017-0147, CVE-2017-0143) and OS Windows 10, which is ransomware that exploited the SMBv2 remote code execution vulnerability in Microsoft Windows.

```
<stix:Exploit_Targets>
    <stixCommon:Exploit_Target                              xsi:type="et:ExploitTargetType"
id="IGL:vulnerability_8f38ecb0-baba-4746-9f97-6ddaec989d89"           timestamp="2014-02-
20T09:00:00.000000Z">
      <et:Title>SMBv2 related Vulnerability </et:Title>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0146</et:CVE_ID>
        <et:Affected_Software>
          <et:Affected_Software>
            <stixCommon:Observable>
              <cybox:Object>
                <cybox:Properties xsi:type="ProductObj:ProductObjectType">
                  <ProductObj:Product condition="Equals">Windows 10</ProductObj:Product>
                  <ProductObj:Version  condition="Equals"  apply_condition="ANY">1511  for
32-bit    systems##comma##1511    for    x64-based    Systems##comma##1607    for    32-bit
Systems##comma##1607 for x64-based Systems</ProductObj:Version>
```

```
                </cybox:Properties>
              </cybox:Object>
            </stixCommon:Observable>
          </et:Affected_Software>
        </et:Affected_Software>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0147</et:CVE_ID>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
      <et:Vulnerability>
        <et:CVE_ID>CVE-2017-0143</et:CVE_ID>
        <et:References>

<stixCommon:Reference>https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_01
0</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
    </stixCommon:Exploit_Target>
  </stix:Exploit_Targets>
```

A.1.4 Incident

It is reported that the classification is unauthorized access, the assets are information properties within an organization and the affected objects as well as incident responses are theft.

```
<stix:Incidents>
    <stix:Incident xsi:type="incident:IncidentType" id="IGL:incident_000009392">
      <incident:Time>
        <incident:First_Malicious_Action>2012-07-19T14:25:36+09:00
</incident:First_Malicious_Action>
        <incident:Incident_Reported>2012-10-30T00:00:00+09:00
</incident:Incident_Reported>
      </incident:Time>
      <incident:Categories>
        <incident:Category xsi:type="stixVocabs:IncidentCategoryVocab-1.0">Unauthorized
Access</incident:Category>
      </incident:Categories>
      <incident:Victim>
```

```
        <stixCommon:Name>Igloo</stixCommon:Name>
      </incident:Victim>
      <incident:Affected_Assets>
        <incident:Affected_Asset>
          <incident:Ownership_Class           xsi:type="stixVocabs:OwnershipClassVocab-
1.0">Internally-Owned</incident:Ownership_Class>
          <incident:Management_Class         xsi:type="stixVocabs:ManagementClassVocab-
1.0">Internally-Managed</incident:Management_Class>
          <incident:Location_Class            xsi:type="stixVocabs:LocationClassVocab-
1.0">Internally-Located</incident:Location_Class>
        </incident:Affected_Asset>
      </incident:Affected_Assets>
      <incident:Impact_Assessment>
        <incident:Effects>
          <incident:Effect      xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial
Loss</incident:Effect>
        </incident:Effects>
      </incident:Impact_Assessment>
      <incident:Status                        xsi:type="stixVocabs:IncidentStatusVocab-
1.0">Closed</incident:Status>
      <incident:Related_Indicators>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_01"/>
        </incident:Related_Indicator>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_02"/>
        </incident:Related_Indicator>
        <incident:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_03"/>
        </incident:Related_Indicator>
      </incident:Related_Indicators>
      <incident:Leveraged_TTPs>
        <incident:Leveraged_TTP>
          <stixCommon:TTP idref="IGL:ttp_000009392"/>
        </incident:Leveraged_TTP>
      </incident:Leveraged_TTPs>
      <incident:Attributed_Threat_Actors>
        <incident:Threat_Actor>
          <stixCommon:Threat_Actor idref="IGL:ta_000009392"/>
        </incident:Threat_Actor>
      </incident:Attributed_Threat_Actors>
      <incident:Intended_Effect>
        <stixCommon:Value                     xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </incident:Intended_Effect>
      <incident:Security_Compromise       xsi:type="stixVocabs:SecurityCompromiseVocab-
1.0">No</incident:Security_Compromise>
```

```
      <incident:Discovery_Method            xsi:type="stixVocabs:DiscoveryMethodVocab-
1.0">User</incident:Discovery_Method>
      <incident:COA_Taken>
        <incident:Course_Of_Action idref="IGL:coa_000009392"/>
      </incident:COA_Taken>
    </stix:Incident>
  </stix:Incidents>
```

A.1.5 Threat actor

It is reported that the type of attacker is a malware developer, the motivation is financial or economic, the proficiency is expert and the intruder's intent is theft.

```
<stix:Threat_Actors>
    <stix:Threat_Actor id="IGL:ta_000009392" xsi:type="ta:ThreatActorType">
      <ta:Description>
       It infected more than 120,000 computers worldwide during May 12-13, 2017. Damage
       caused by WannaCrypt, a variant of WannaCry, which has spread to about 100
       countries including Europe and Asia.
       The spread of malware is assumed by the hacker group 'Shadow Brokers' who
       claimed to have stolen hacking tools developed by the US National Security
       Agency (NSA).
       The type of attacker is malware developer, the motivation is financial or
       economic, the proficiency is an expert and the intruder's intent is theft.
      </ta:Description>
      <ta:Type>
      <stixCommon:Value xsi:type="stixVocabs:ThreatActorTypeVocab-1.0"> eCrime Actor -
Malware Developer                        </stixCommon:Value>
      </ta:Type>
      <ta:Motivation>
        <stixCommon:Value   xsi:type="stixVocabs:MotivationVocab-1.1">   Financial   or
Economic </stixCommon:Value>
      </ta:Motivation>
      <ta:Sophistication>
        <stixCommon:Value          xsi:type="stixVocabs:ThreatActorSophisticationVocab-
1.0">Expert</stixCommon:Value>
      </ta:Sophistication>
      <ta:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </ta:Intended_Effect>
      <ta:Observed_TTPs>
        <ta:Observed_TTP>
          <stixCommon:TTP idref=" IGL:ttp_000009392"/>
        </ta:Observed_TTP>
      </ta:Observed_TTPs>
    </stix:Threat_Actor>
  </stix:Threat_Actors>
```

A.1.6 Campaign

It is reported that the related incident, TTP and threat actor have been described to achieve the threat actor's intent.

```
<stix:Campaigns>
    <stix:Campaign xsi:type="campaign:CampaignType" id="IGL:campaign_000009392">
      <campaign:Title> Ransomware(WannaCrypt) Attack </campaign:Title>
      <campaign:Names>
        <campaign:Name>000009392</campaign:Name>
      </campaign:Names>
      <campaign:Intended_Effect>
        <stixCommon:Value                    xsi:type="stixVocabs:IntendedEffectVocab-
1.0">Theft</stixCommon:Value>
      </campaign:Intended_Effect>
      <campaign:Related_TTPs>
          <stixCommon:TTP idref="IGL:ttp_000009392"/>
        </campaign:Related_TTP>
      </campaign:Related_TTPs>
      <campaign:Related_Incidents>
        <campaign:Related_Incident>
          <stixCommon:Incident idref="IGL:incident_000009392"/>
        </campaign:Related_Incident>
      </campaign:Related_Incidents>
      <campaign:Related_Indicators>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_01"/>
        </campaign:Related_Indicator>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_02"/>
        </campaign:Related_Indicator>
        <campaign:Related_Indicator>
          <stixCommon:Indicator idref="IGL:indicator_000009392_03"/>
        </campaign:Related_Indicator>
      </campaign:Related_Indicators>
      <campaign:Attribution>
        <campaign:Attributed_Threat_Actor>
          <stixCommon:Threat_Actor idref="IGL:ta_000009392"/>
        </campaign:Attributed_Threat_Actor>
      </campaign:Attribution>
    </stix:Campaign>
  </stix:Campaigns>
```

A.2 Specifying indicator patterns for cyber threats

A.2.1 Indicator

It is reported that the malicious e-mail, exfiltration, URL watch type indicators are defined and the related observable, TTP, campaign are linked.

```
<stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_01">
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Malicious E-mail</indicator:Type>
      <indicator:Description> Ransomware infection with malicious mail as one of the indicators </indicator:Description>
      <indicator:Observable>
        <cybox:Observable_Composition operator="OR">
          <cybox:Observable idref="IGL:observable_000009392_01"/>
        </cybox:Observable_Composition>
      </indicator:Observable>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_02">
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Exfiltration</indicator:Type>
      <indicator:Description> SMB vulnerability attack as one of the Indicators </indicator:Description>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="IGL:indicator_000009392_03">
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">URL Watchlist</indicator:Type>
      <indicator:Description> malicious code distribution sites as one of the indicators </indicator:Description>
      <indicator:Observable>
        <cybox:Observable_Composition operator="OR">
          <cybox:Observable idref="IGL:observable_000009392_02"/>
```

```
          <cybox:Observable idref="IGL:observable_000009392_03"/>
        </cybox:Observable_Composition>
      </indicator:Observable>
      <indicator:Indicated_TTP>
        <stixCommon:TTP idref="IGL:ttp_000009392"/>
      </indicator:Indicated_TTP>
      <indicator:Related_Campaigns>
        <indicator:Related_Campaign>
          <stixCommon:Campaign idref="IGL:campaign_000009392"/>
        </indicator:Related_Campaign>
      </indicator:Related_Campaigns>
    </stix:Indicator>
    </stix:Indicators>
```

A.3 Managing response activities

A.3.1 Course of action

It is noted that the remedy is possible through a software vulnerability patch, no impact due to connection limit, cost of response is low and the effectiveness of response is medium.

```
<stix:Courses_Of_Action>
    <stix:Course_Of_Action xsi:type="coa:CourseOfActionType" id="IGL:coa_000009392">
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Remedy</coa:Stage>
      <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Patching</coa:Type>
      <coa:Parameter_Observables xsi:type="cybox:ObservablesType" cybox_major_version="2"
cybox_minor_version="1">
        <cybox:Observable idref="IGL:observable_000009392_01"/>
        <cybox:Observable idref="IGL:observable_000009392_02"/>
        <cybox:Observable idref="IGL:observable_000009392_03"/>
      </coa:Parameter_Observables>
      <coa:Impact>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">None</stixCommon:Value>
      </coa:Impact>
      <coa:Cost>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Low</stixCommon:Value>
      </coa:Cost>
      <coa:Efficacy>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Medium</stixCommon:Value>
      </coa:Efficacy>
    </stix:Course_Of_Action>
    <stix:Course_Of_Action    id="IGL:coa_000009393"    xsi:type="coa:CourseOfActionType"
version="1.1">
```

```
      <coa:Title>(For users who cannot use the latest Windows security patch) Disable the
SMB protocol </coa:Title>
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Response</coa:Stage>
      <coa:Type              xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Perimeter
Blocking</coa:Type>
      <coa:Objective>
        <coa:Description> Block SMB-related ports (TCP 139, TCP 445) using network
firewalls and Windows Firewall</coa:Description>
        <coa:Applicability_Confidence>
          <stixCommon:Value                    xsi:type="stixVocabs:HighMediumLowVocab-
1.0">High</stixCommon:Value>
        </coa:Applicability_Confidence>
      </coa:Objective>
      <coa:Parameter_Observables      cybox_major_version="2"      cybox_minor_version="1"
cybox_update_version="0">
        <cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19edb">
          <cybox:Object id="IGL:Port-d5bc7186-319d-44e0-85f4-0b65f59034a3">
            <cybox:Properties xsi:type="PortObj:PortObjectType">
              <PortObj:Port_Value>139</PortObj:Port_Value>
              <PortObj:Layer4_Protocol>TCP</PortObj:Layer4_Protocol>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19asd">
          <cybox:Object id="IGL:Port-d5bc7186-319d-44e0-85f4-0b65f59034a4">
            <cybox:Properties xsi:type="PortObj:PortObjectType">
              <PortObj:Port_Value>445</PortObj:Port_Value>
              <PortObj:Layer4_Protocol>TCP</PortObj:Layer4_Protocol>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      </coa:Parameter_Observables>
    </stix:Course_Of_Action>
    <stix:Course_Of_Action    id="IGL:coa_000009394"    xsi:type="coa:CourseOfActionType"
version="1.1">
      <coa:Title> Latest Windows Updates</coa:Title>
      <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Remedy</coa:Stage>
      <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Patching</coa:Type>
      <coa:Objective>
        <coa:Description> Download and apply version upgrades and latest security patches
through MS update catalog site </coa:Description>
        <coa:Applicability_Confidence>
          <stixCommon:Value                    xsi:type="stixVocabs:HighMediumLowVocab-
1.0">High</stixCommon:Value>
        </coa:Applicability_Confidence>
      </coa:Objective>
      <coa:Parameter_Observables      cybox_major_version="2"      cybox_minor_version="1"
cybox_update_version="0">
```

```
<cybox:Observable id="IGL:Observable-e04425e4-60a2-4d91-a9f9-0ca956f19adn">
          <cybox:Object id="IGL:Object-37be6630-b2df-4bf9-8750-3f45ca9e1923bb">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
              <URIObj:Value
condition="Equals">http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598</URIOb
j:Value>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      </coa:Parameter_Observables>
      <coa:Cost>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Low</stixCommon:Value>
      </coa:Cost>
      <coa:Efficacy>
        <stixCommon:Value                          xsi:type="stixVocabs:HighMediumLowVocab-
1.0">Medium</stixCommon:Value>
      </coa:Efficacy>
    </stix:Course_Of_Action>
</stix:Courses_Of_Action>
```

Bibliography

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-RFC7159] Bray, T., Ed., The JavaScript Object Notation (JSON) (2014), *Data Interchange Format*, RFC 7159, DOI 10.17487/RFC7159. http://www.rfc-editor.org/info/rfc7159.txt.

[b-STIX1.2.1] ASIS website, *STIX specifications*. https://www.oasis-open.org/standards#stix1.2.1

[b-STIX1.2.1-Part 1] OASIS website, *STIX specifications, Part 1: Overview*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part1-overview/stix-v1.2.1-cs01-part1-overview.html

[b-STIX2.0] Introduction to STIX https://oasis-open.github.io/cti-documentation/stix/intro.html

[b-STIX2.0-Part 1] OASIS, 2017, *STIX Version 2.0. Part 1: Part 1: STIX Core Concepts*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html

[b-STIX2.0-Part 2] OASIS, 2017, *STIX Version 2.0. Part 2: STIX Objects*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html

[b-STIX2.0-Part 3] OASIS, 2017, *STIX Version 2.0. Part 3: Cyber Observable Core Concepts*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part3-cyber-observable-core/stix-v2.0-cs01-part3-cyber-observable-core.html

[b-STIX2.0-Part 4] OASIS, 2017, *STIX Version 2.0. Part 4: Cyber Observable Objects*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part4-cyber-observable-objects/stix-v2.0-cs01-part4-cyber-observable-objects.html

[b-STIX2.0-Part 5] OASIS, 2017, *STIX Version 2.0. Part 5: STIX Patterning*. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part5-stix-patterning/stix-v2.0-cs01-part5-stix-patterning.html

[b-STIX2.0 tool] Getting Started with STIX 2.0. https://oasis-open.github.io/cti-documentation/stix/gettingstarted.html

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019