国 际 电 信 联 盟

# ITU-T X.1215

(01/2019)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全设计

# 结构化威胁信息表达式的用例

ITU-T X.1215 建议书

国际电信联盟

ITU-T X 系列建议书

**数据网、开放系统通信和安全性**

| | |
|---|---|
| 公用数据网 | X.1–X.199 |
| 开放系统互连 | X.200–X.299 |
| 网间互通 | X.300–X.399 |
| 报文处理系统 | X.400–X.499 |
| 号码簿 | X.500–X.599 |
| OSI组网和系统概貌 | X.600–X.699 |
| OSI管理 | X.700–X.799 |
| 安全 | X.800–X.849 |
| OSI应用 | X.850–X.899 |
| 开放分布式处理 | X.900–X.999 |
| 信息和网络安全 | |
| 一般安全问题 | X.1000–X.1029 |
| 网络安全 | X.1030–X.1049 |
| 安全管理 | X.1050–X.1069 |
| 生物测定 | X.1080–X.1099 |
| 安全应用和服务(1) | |
| 组播安全 | X.1100–X.1109 |
| 家庭网络安全 | X.1110–X.1119 |
| 移动安全 | X.1120–X.1139 |
| 网页安全 | X.1140–X.1149 |
| 安全协议(1) | X.1150–X.1159 |
| 对等网络安全 | X.1160–X.1169 |
| 网络身份安全 | X.1170–X.1179 |
| PITV安全 | X.1180–X.1199 |
| 网络空间安全 | |
| **计算网络安全** | **X.1200–X.1229** |
| 反垃圾信息 | X.1230–X.1249 |
| 身份管理 | X.1250–X.1279 |
| 安全应用和服务(2) | |
| 应急通信 | X.1300–X.1309 |
| 泛在传感器网络安全 | X.1310–X.1319 |
| 智能电网安全 | X.1330–X.1339 |
| 验证邮件 | X.1340–X.1349 |
| 物联网（IoT）安全 | X.1360–X.1369 |
| 智能交通系统 (ITS) 安全 | X.1370–X.1389 |
| 分布式账簿技术安全 | X.1400–X.1429 |
| 安全协议(2) | X.1450–X.1459 |
| 网络安全信息交换 | |
| 网络安全综述 | X.1500–X.1519 |
| 脆弱性/状态信息交换 | X.1520–X.1539 |
| 事件/事故/探索法信息交换 | X.1540–X.1549 |
| 政策的交换 | X.1550–X.1559 |
| 探索法和信息要求 | X.1560–X.1569 |
| 标示和发现 | X.1570–X.1579 |
| 确保交换 | X.1580–X.1589 |
| 云计算安全 | |
| 云计算安全综述 | X.1600–X.1601 |
| 云计算安全设计 | X.1602–X.1639 |
| 云计算安全最佳实践和指导原则 | X.1640–X.1659 |
| 云计算安全实现 | X.1660–X.1679 |
| 其他云计算安全 | X.1680–X.1699 |

欲了解更详细信息，请查阅ITU-T建议书目录。

**ITU-T X.1215 建议书**

# 结构化威胁信息表达式的用例


## 摘要

ITU-T X.1215建议书提供了结构化威胁信息表达式（STIX）语言如何用于支持网络威胁情报（CTI）和信息共享的各种用例。

本建议书还描述了STIX语言的概念和功能。STIX语言的目标是支持网络威胁管理中涉及的一系列用例，包括分析网络威胁、说明网络威胁的指标特征、管理响应活动以及共享网络威胁信息。利用这类信息，可就如何最好地抵御威胁做出安全决策。目的是支持进行更有效的分析，并持续交换网络威胁信息。STIX系列规范[b-STIX2.0]由结构化信息标准促进组织（OASIS）负责充实完善。



## 历史沿革

| 版本 | 建议书名称 | 批准日期 | 研究组 | 唯一标识* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1215 | 2019-01-30 | 17 | 11.1002/1000/13849 |

## 关键词

网络威胁情报、信息共享、安全、STIX。


* 欲查阅此建议书，请在网络浏览器的地址字段内输入URL http://handle.itu.int/，然后再输入该建议书的唯一ID，例如：http://handle.itu.int/11.1002/1000/11830-en。

## 前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

## 注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

## 知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

# 目录

# ITU-T X.1215 建议书

# 结构化威胁信息表达式的用例

## 1 范围

本建议书旨在提供结构化威胁信息表达式（STIX）的各种用例，STIX是一种描述网络威胁信息的结构化语言。STIX语言的目标是支持网络威胁管理中涉及的一系列用例，包括分析网络威胁、说明网络威胁的攻击指标特征、管理响应活动以及共享网络威胁信息。这些用例通常很简单，并不能体现STIX语言的完整表达性或灵活性。用例通常包括一些描述用例活动的某种散文、STIX内容表示和充分验证的STIX内容文档由于2016年发布的STIX版本1.0使用可扩展标记语言（XML）格式，而版本2.0采用JavaScript对象表示法（JSON），本建议书介绍了XML中用例的实施。建议使用STIX 2.0中所述的要求。

## 2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

## 3 定义

### 3.1 在其他地方定义的术语

本建议书使用了下列他处定义的术语：

**3.1.1 实体Entity** [b-STIX2.0.1]：任何可单独识别的存在（例如，组织、个人、团体等）。

**3.1.2 STIX对象STIX object** [b-STIX2.0.1]：STIX域对象（SDO）或STIX关系对象（SRO）。

**3.1.3 结构化威胁信息表达式 （STIX） structured threat information expression （STIX）** [b-STIX2.0.1]：用于交换网络威胁情报（CTI）的语言和序列化格式。

**3.1.4 可信自动交换指标信息trusted automated eXchange of indicator information（TAXII）**[b-STIX2.0.1]：用于网络威胁信息通信的应用层协议。

### 3.2 本建议书定义的术语

无。

## 4 缩写词和首字母缩略语

本建议书采用了下列缩写词和首字母缩略语：

| | |
|---|---|
| CAPEC | 通用攻击模式列表和分类 |
| COA | 应对措施 |
| CnC | 命令与控制 |
| CTI | 网络威胁情报 |
| CVE | 公共漏洞和暴露 |
| C2 | 命令与控制 |
| DLL | 动态链接库 |
| EDR | 事件数据记录仪 |
| JSON | JavaScript Object Notation |
| OS | Operating System |
| SDO | STIX域对象（图中的“节点”） |
| SMBv2 | 服务器消息块版本2 |
| SRO | STIX关系对象（一种表示图中“边缘”的机制） |
| STIX | 结构化威胁信息表达式 |
| TAXII | 可信自动交换指标信息 |
| TTP | 战术、技术和程序 |
| TLP | 交通信号灯协议 |
| XML | Extensible Markup Language |

## 5 惯例

无。

## 6 STIX概述

### 6.1 STIX的概念

为实时响应网络威胁，不仅应提供单个的安全系统，还应提供全球协作的安全管理系统，因为全球性问题无法通过单个实体和单个域来解决。因此，全球网络威胁情报（CTI）是一个组织安全计划的重要组成部分，可从内部和外部获得。结构化威胁信息表达式（STIX）是网络威胁情报和信息共享的解决方案之一，这是一种用于描述网络威胁信息的结构化语言。STIX提供富有表现力的、灵活的、可扩展的、可自动化和可读的网络威胁信息结构化表示。

### 6.2 STIX中的对象

#### 6.2.1 STIX 1.2中的对象

STIX 1.2采用七个已定义的STIX域对象（SDO），如下所示：

1) 攻击活动（Campaign）：STIX攻击活动表示的是一组结合起来表达共同意图或所需效果的战术、技术和程序（TTP）、事件或威胁实施者。

2) 应对措施（Course of action）：STIX应对措施部件用于传递有关可能针对攻击而采取的行动或者作为攻击前预防措施的行动的信息。

3) 目标漏洞利用（Exploit target）：STIX目标漏洞利用传递有关可能被攻击者利用的软件、系统或网络中的技术漏洞、弱点或错误配置的信息。

4) 安全事件（Incident）：STIX事件传递有关网络安全事件的信息。

5) 攻击指标（Indicator）：STIX指标传递与环境信息相结合的具体表征模式。

6) 威胁实施者（Threat actor）：STIX威胁实施者传递用于表征或确定（或表征并确定）攻击者的信息。

7) TTP：TTP是一个军事术语，指的是“战术、技术和程序”。

### 6.2.2 STIX 2.0中的对象

STIX 2.0采用STIX用于表示网络威胁信息的、一组经定义的域对象和关系对象。STIX 2.0定义了12个STIX SDO，如下所示：

1) 攻击模式（Attack pattern）：攻击模式是一类TTP，描述攻击者试图破坏目标的方式。

2) 攻击活动（Campaign）：攻击活动是一组敌对行为，描述在一段时间内针对具体目标集的一系列恶意活动或攻击（有时称为攻击波）。

3) 应对措施（Course of action）：应对措施是为防止攻击或应对正在发生的攻击而采取的行动。

4) 身份（Identity）：身份可代表实际的个人、组织或团体（如ACME、公司）以及个人、组织或团体（如金融部门）。

5) 攻击指标（Indicator）：攻击指标包含可用于检测可疑或恶意网络活动的模式。

6) 入侵集（Intrusion set）：入侵集是一组具有共同属性、被认为由单个组织精心策划的敌对行为和资源。

7) 恶意软件（Malware）：恶意软件是一类TTP，亦称为恶意的代码和恶意的软件，是指通常以隐蔽的方式嵌入系统、意图破坏受害者数据、应用或操作系统（OS）机密性、完整性或可用性或者以其他方式扰乱或破坏受害者的程序。

8) 观测数据（Observed data）：观测数据使用本规范第3部分和第4部分中定义的网络表征规范传递在系统和网络上监测到的信息。

9) 报告（Report）：报告是专注于一个或多个主题的威胁情报集，如威胁实施者、恶意软件或攻击技术的描述，包括背景描述和相关细节。

10) 威胁实施者（Threat actor）：威胁实施者被认为是企图实施恶意行动的实际个人、团体或组织。

11) 工具（Tool）：工具是威胁实施者可用来执行攻击的合法软件。了解威胁实施者如何以及何时使用此类工具对于了解攻击活动如何实施而言非常重要。

12) 漏洞（Vulnerability）：漏洞是指“软件中可被黑客直接用来接入系统或网络的错误”。

STIX 2.0定义了两个STIX关系对象（SRO），如下所示：

1) 关系（Relationship）：关系对象用于将两个SDO联系在一起，以描述其彼此之间的关系。

2) 见证（Sighting）：见证表示CTI中的要素被监测到的信念（如攻击指标、恶意软件、工具、威胁实施者）。

### 6.3 STIX中的特性和工具

STIX提供以下特性：

– JSON/XML样式：STIX 2.0使用JSON样式来表示六个对象和属性。此外，STIX 1.0使用XML模式。

– STIX域对象：STIX中的所有对象都位于顶层。这些对象被称为STIX SDO。一些对象属性直接引用另一个对象的身份（如created_by_ref），但大多数关系使用顶层关系对象来表示。

– STIX 2.0关系对象：STIX 2.0引入了一个顶层关系对象，它通过一个经命名的关系类型来将另外两个顶层对象联系起来。

STIX应提供以下各种各样的工具集：

– STIX验证工具：STIX验证工具是验证STIX JSON内容是否符合2.0规范要求的有用资源。

– 模式验证工具：STIX模式是表示STIX攻击指标SDO中网络表征对象的表达式，将有助于构建用于显示网络活动之情报的模型。此工具只是确保模式化语法符合模式化表达式的要求。

– STIX可视化：STIX可视化工具旨在帮助将此JSON转换为更简洁、更清晰的图表。

– STIX升级工具：升级工具有助于实现这一目的，并将尽力实现从1.x到2.0的转换。

– STIX模式匹配工具：模式匹配工具提供了一种将STIX观测数据与STIX攻击指标模式进行比较的方法。

## 7 STIX 2.0的用例

本建议书提供了各种各样的用例，以说明如何使用STIX语言来支持网络威胁情报和信息共享环境。其目标是支持网络威胁管理中涉及的一系列用例（UC），包括：分析网络威胁（UC1，第7.2.1节）、说明网络威胁的攻击指标模式（UC2，第7.2.2节）、管理响应活动（UC3，第7.2.3节）和共享网络威胁信息（UC4）。本建议书未涉及共享网络威胁信息（UC4）。在图1中概述了一个STIX用例示例。STIX 1.0用例见附件A。

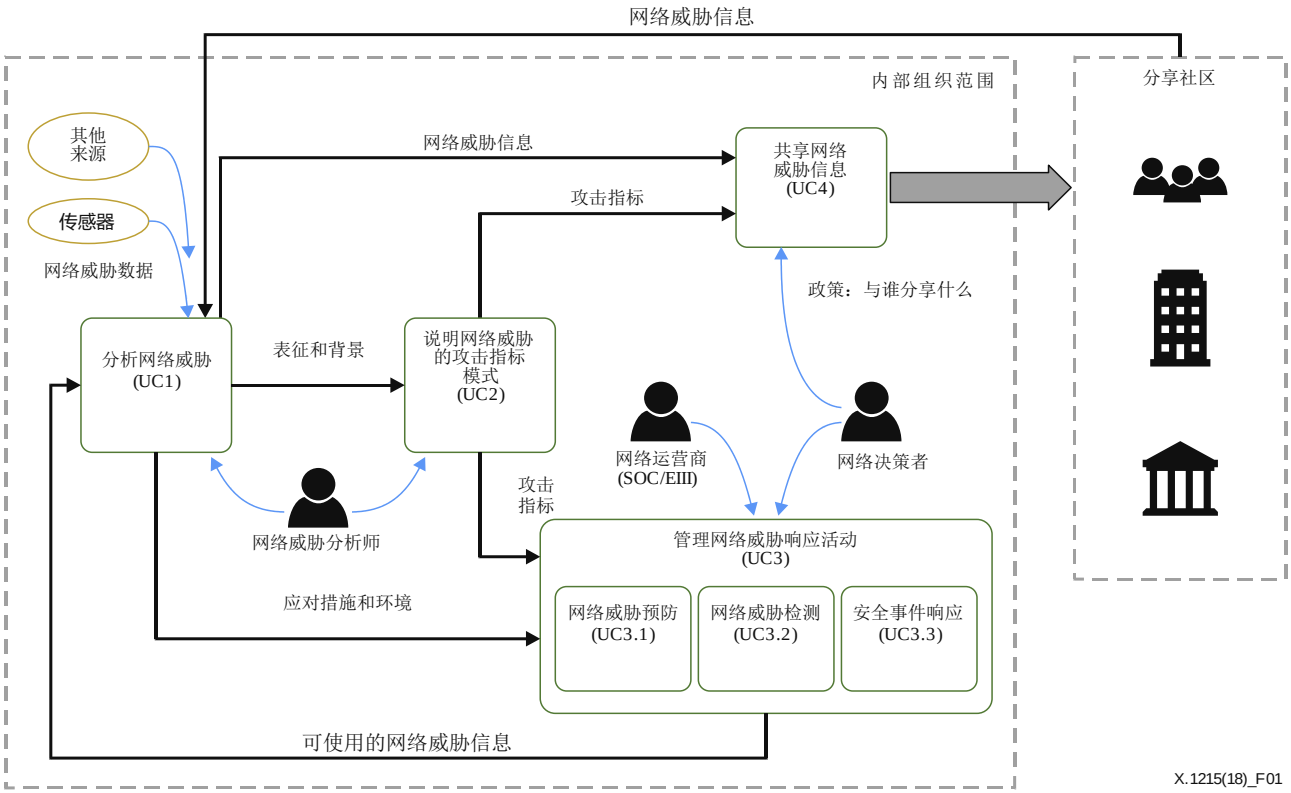


**图1 – STIX用例概述**

## 7.1 STIX 2.0的勒索软件用例

勒索软件是一种感染计算机系统的恶意软件，限制对受害者数据的访问并索要赎金。由于对计算机的访问受到限制，受害者将被迫向开发恶意程序的实体付款以取消限制。勒索软件攻击通常通过使用一个特洛伊木马程序来实施，即伪装成为一个合法文件，在它作为电子邮件的一个附件到达时，诱骗用户下载或打开。

最近，WannaCry勒索软件开始影响全球范围内的计算机；它在计算机之间自动传播而无需用户交互。与通过电子邮件附件传播的普通勒索软件不同，WannaCry感染媒介只需要易受攻击的系统连接到互联网。WannaCry勒索软件对各种各样的文件进行加密，如文档文件、压缩文件、数据库文件和虚拟机文件。

本节概述了勒索软件用例，以说明如何使用STIX 2.0语言来支持针对WannaCry勒索软件的网络威胁管理。

### 7.1.1 分析网络威胁

本节提供了勒索软件（WannaCrypt）分析得到的信息，恶意代码攻击在世界范围内报告了这些信息，使用的是服务器消息块版本2（SMBv2）远程代码执行漏洞勒索软件。

#### 7.1.1.1 身份

可将观测者的信息定义为身份对象。

#### 7.1.1.2 观测到的数据

观测到收到了有关传输通知的电子邮件，其中包含egg文件存档，监测到52个命令与控制（CnC）服务器域（在此示例中仅有两个CnC服务器域）。

```
{
   "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

报告称，监测到针对个人计算机的勒索软件攻击；攻击模式是使用恶意软件的、有针对性攻击的活动，可将使用恶意软件的关系对象创建为攻击模式。

```
{
   "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 漏洞

报告称，漏洞与公共漏洞和暴露(CVE)-2017-0147和CVE-2017-0143有关，这是利用Microsoft Windows上SMBv2远程代码执行漏洞（17.3.14补丁版，MS17-010）的勒索软件。可创建使用针对此漏洞的恶意软件的关系对象。

```
{
 "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 攻击活动和威胁实施者

报告称，两个对象被定义为针对有关勒索软件攻击的信息的攻击活动和威胁实施者。确定可针对攻击活动和威胁实施者创建“归因（attributed-to）”关系、可针对攻击活动和攻击模式创建“使用（uses）”关系、可针对攻击活动和漏洞创建“目标（targets）”关系。

```
{
      "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 说明网络威胁的攻击指标特征

#### 7.1.2.1 攻击指标

报告称，恶意软件分发站点URL被定义为URL监视的指标类型，并可创建表示恶意软件的关系对象。

```
{
      "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 管理响应活动

#### 7.1.3.1 应对措施

注意到，补救方法有“禁用SMB协议”和“软件漏洞修复”，可将其定义为应对措施（COA）对象。可创建用于缓解针对每个对象的恶意软件的关系对象。

```
{
   "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 利用关系图描述攻击情况

图 2 显示了用于描述用例的所有STIX对象之间的关系。

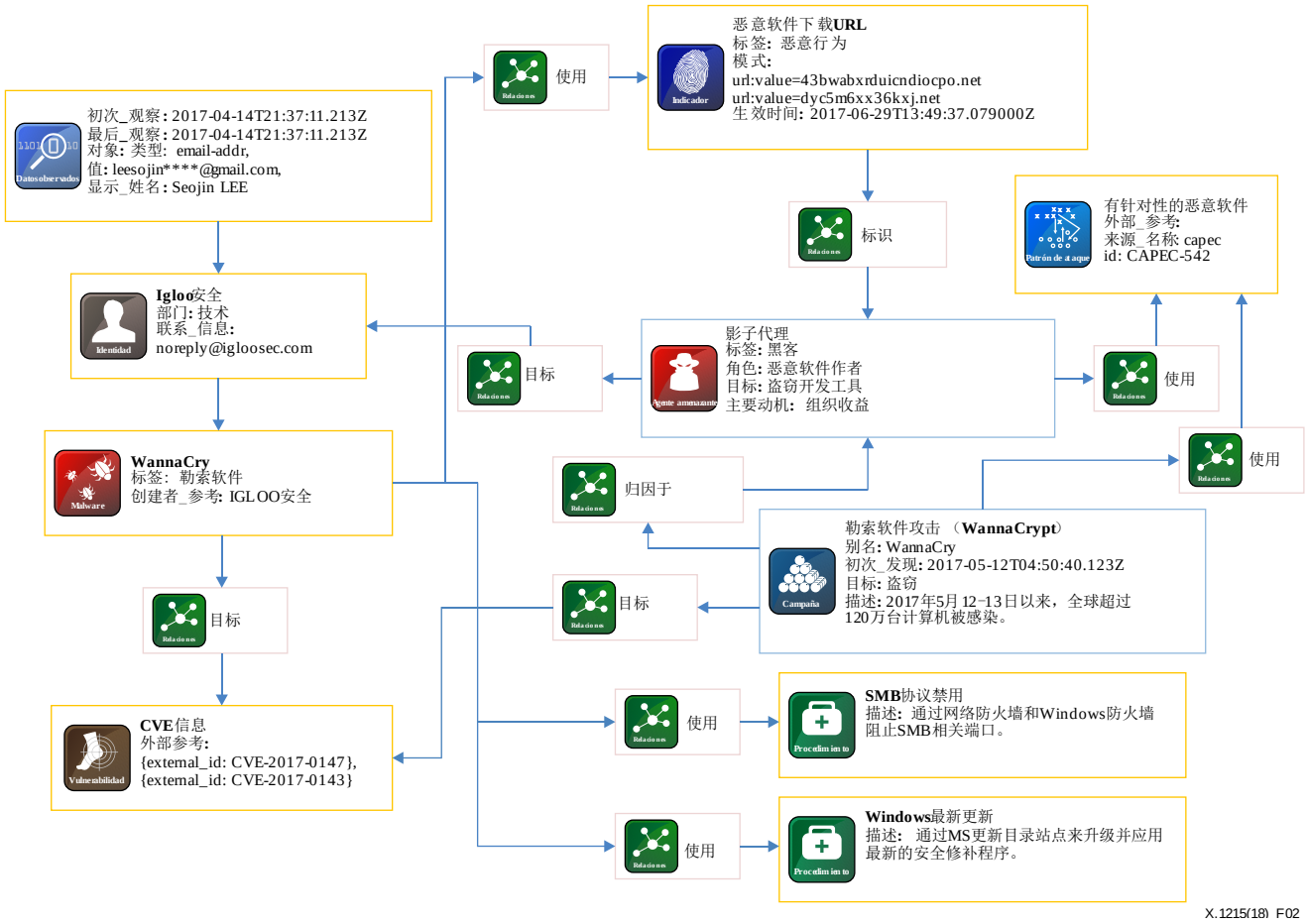


**图2 – 用于描述用例的STIX对象之间的关系**

总而言之，以下内容描述了包含所有对象的STIX捆绑包对象，以检测、分析由所谓的WannaCry勒索软件执行的恶意攻击并对其做出响应。

```
{
   "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 针对加密货币交易所的网络攻击用例

本节描述了所谓的“Lazarus APT小组”威胁实施者在2018年6月20日对韩国加密货币交易所进行的攻击用例。

在该情形中，威胁实施者向加密货币交易所的工作人员发送了一个带有恶意代码的钓鱼电子邮件。该钓鱼电子邮件附带一个恶意的postscript隐藏文档文件，该文件可以在之后下载恶意动态链接库（DLL），并利用Hangul文字处理器的漏洞执行postscript，从而将恶意的DLL文件安装在用户的PC上。该恶意DLL文件获得用户PC的控制权并访问可接入交易所内部的服务器。结果是，攻击者得以访问交易所的加密货币钱包并从中提取大量资金。

### 7.2.1 UC1：分析网络威胁

2018年6月至7月间，发生并报告了多起有关加密货币交易所受到攻击的案例。因此，对所谓的“BC-Company”公司的加密货币交易遭受的黑客事件进行了分析。

#### 7.2.1.1 身份

观测者的基本识别信息可以用身份对象来建模。观察到该安全事件的组织和事件发生处可以建模为身份对象。

为识别STIX报告对象的发起者，安全监控公司WINS和IGLOO表示为身份对象。安全事件的目标被建模为一个属性名为“BC-Company.com”的身份对象，它是一个假名。该对象在稍后讨论的目标对象的where_sighted_refs中予以指定，用作攻击模式和恶意软件的攻击目标。

```
{
"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 观测到的数据

观测到的数据表示机器生成的原始信息，与支配情报断言的指标不同。观测到的数据对象包含在系统和网络上捕获的网络可观察信息（如IP地址、文件和URL）。在这种情况下，观察一个文件。另一个参考sighting_of_ref包含发现的SDO的ID，在此作为观测到的数据对象。

加密货币交易所观察到一个通过电子邮件传递的文件。该文件的名称和发件人的电子邮

件地址用观测到的数据对象来表示。在他处发现的观测到的数据对象用目击对象来表示。观测到的位置通过where_sighted_refs属性表示。

```
{
    "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 战术、技术和程序

本节描述用于表征攻击者行为方式和本质的特征。

攻击源自一个钓鱼电子邮件中的附件，当中使用了两种类型的恶意代码来实施攻击。通过攻击模式对象将钓鱼攻击指定为通用攻击模式枚举和分类(CAPEC)-163。自钓鱼电子邮件发送的恶意代码利用CVE-2015-2545漏洞下载恶意DLL。因此，恶意软件的标签被标记为漏洞利用和病毒释放器。在之后收到恶意DLL的情况下，远程访问木马被标记为一个控制用户PC的恶意代码。

两个恶意代码之间的关系被定义为“相关”类型，以此表明恶意文档与恶意DLL之间存在关联。

攻击者在实施鱼叉式网络钓鱼时，使用了经过高度伪装的文档。由于攻击的目标是加密货币交易所，因此使用“目标”类型的关系对象。


```
{
    "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 漏洞

在此使用了CVE-2015-2545漏洞，这是一个在Hangul文字处理器文档中隐藏恶意postscript并使其运行的漏洞。漏洞对象用于模拟该漏洞。关系对象也指明恶意代码与漏洞之间的关联。


```
{
    "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 攻击活动和威胁实施者

为盗取加密货币交易所中存储的加密货币，Lazarus APT Group发送了嵌有恶意代码的渔叉式网络钓鱼电子邮件。

威胁实施者对象的目标在“目标”属性中表示为“窃取加密货币”。由于创建了一个恶意文档，因此“角色”属性设为角色属性中的“恶意软件_作者”。由于它被用于犯罪行为，因此“标签”属性设为“犯罪_辛迪加”。

对加密货币交易所的攻击通过活动对象来表示，“目的”属性设为“盗窃”。

攻击活动中使用的攻击技术和恶意代码对象通过使用“使用”类型的关系对象来表示。

```
        {
            "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：详细说明网络威胁的指标模式

#### 7.2.2.1 指标

指标对象用于标识恶意文档和恶意DLL。恶意文档在指标对象中的模式属性表示下载恶意DLL的URL或文件哈希值。在这种情形下，指标对象中的恶意DLL模式表示命令与控制（C2）URL以及文件的哈希值。这使其有可能注册为一种策略。具有“指示”类型的若干关系对象表示两个恶意代码之间的关系。


```
{
    "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：管理网络威胁响应活动

#### 7.2.3.1 应对措施

在本攻击情形中，响应团队的应对措施分为检测和响应。首先执行恶意文档，然后开始攻击。

恶意文档的哈希值以恶意软件分析工具（如YARA）中的安全政策进行注册。当带有哈希值的文件运行时，事件数据记录器（EDR）可以检测到攻击。此外，作为响应，网络安全设备通过阻止下载恶意DLL的URL来阻止下载恶意DLL，从而避免PC的控制权被盗取。如果恶意DLL被拦劫，那么网络设备可以通过阻止到C2 URL的流量来阻止恶意活动。


```
{
    "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 关系图和捆绑对象

图3显示了用于描述用例的所有对象之间的关系。

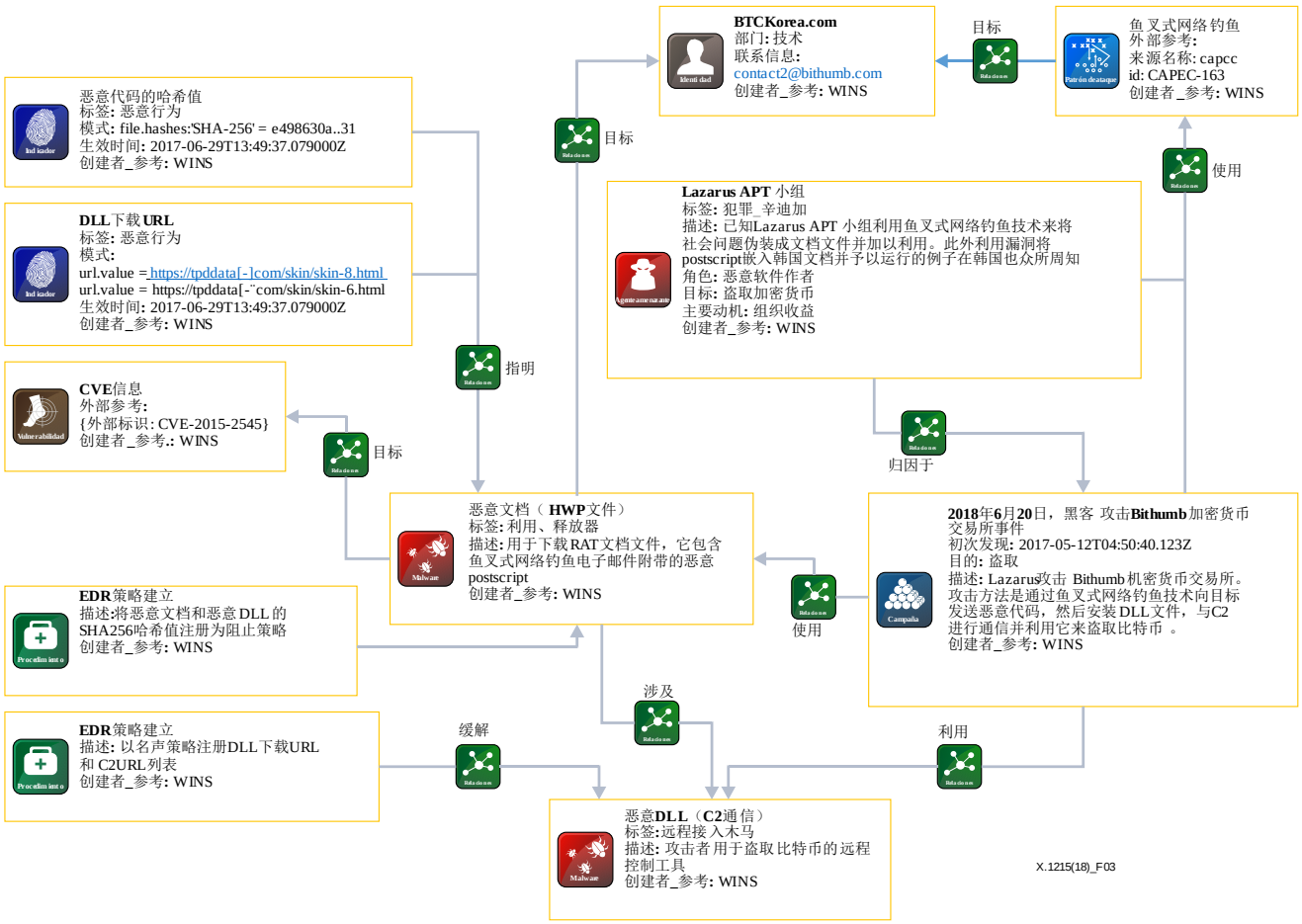


**图3 – 用来描述用例的各STIX对象之间的关系**

总而言之，以下内容描述了包含所有对象的STIX捆绑包对象，以检测、分析由所谓的Lazarus执行的恶意攻击并对其做出响应。

```
{
    "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"
            ]
        }
    ]
}
```

# 附件A

## STIX 1.0中的勒索软件用例

（此附件是本建议书不可分割的组成部分）

本附件通过概述勒索软件的用例介绍了如何使用STIX1.0语言来支持针对WannaCry勒索软件的网络威胁管理。

### A.1 分析网络威胁

本节提供了勒索软件（WannaCrypt）分析得到的信息，恶意代码攻击在世界范围内报告了这些信息，使用的是服务器消息块版本2（SMBv2）远程代码执行漏洞勒索软件。

#### A.1.1 观察

观测到收到了有关传输通知的电子邮件，其中包含egg文件存档，监测到52个命令与控制（CnC）服务器域。

```
<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

据报告，观测到了针对个人计算机的勒索软件攻击。攻击模式是使用恶意软件进行的有针对性的攻击活动，攻击目标是组织中的信息属性。

```
<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 利用目标

报告称，该漏洞与漏洞（CVE-2017-0147、CVE-2017-0143）和操作系统Windows 10有关，是一款利用Microsoft Windows中SMBv2远程代码执行漏洞的勒索软件。

```
<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_
010</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_
010</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_
010</stixCommon:Reference>
        </et:References>
      </et:Vulnerability>
    </stixCommon:Exploit_Target>
  </stix:Exploit_Targets>
```

### A.1.4 安全事件

据报告，该安全事件被分类为未经授权的访问，资产是组织内的信息属性，受影响的对象及事件响应是盗窃。

```
<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 威胁实施者

据报告，攻击者的类型是恶意软件开发者，动机是财务和经济方面的目的，熟练程度是专家级，入侵者的意图是盗窃。

```
<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 攻击活动

据报告，已对为实现威胁实施者意图的相关事件、TTP和威胁实施者进行了描述。

```
<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 详细说明网络威胁的指标模式

### A.2.1 指标

据报告，对恶意电子邮件、渗漏、URL跟踪类型指标进行了定义，并关联了相关的观察、TTP和攻击活动。

```
<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 管理响应活动

### A.3.1 应对措施

注意到，有望通过软件漏洞补丁实施补救，不会因连接限制而产生任何影响，并且响应成本低，响应效果为中等。

```
<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</URI
Obj: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>
```

# 参考资料


[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

# ITU-T 系列建议书

| | |
|---|---|
| A 系列 | ITU-T 工作的组织 |
| D 系列 | 一般资费原则 |
| E 系列 | 综合网络运行、电话业务、业务运行和人为因素 |
| F 系列 | 非话电信业务 |
| G 系列 | 传输系统和媒质、数字系统和网络 |
| H 系列 | 视听及多媒体系统 |
| I 系列 | 综合业务数字网 |
| J 系列 | 有线网络和电视、声音节目及其它多媒体信号的传输 |
| K 系列 | 干扰的防护 |
| L 系列 | 环境与 ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、安装和保护 |
| M 系列 | 电信管理，包括 TMN 和网络维护 |
| N 系列 | 维护：国际声音节目和电视传输电路 |
| O 系列 | 测量设备的技术规范 |
| P 系列 | 电话传输质量、电话设施及本地线路网络 |
| Q 系列 | 交换和信令 |
| R 系列 | 电报传输 |
| S 系列 | 电报业务终端设备 |
| T 系列 | 远程信息处理业务的终端设备 |
| U 系列 | 电报交换 |
| V 系列 | 电话网上的数据通信 |
| **X 系列** | **数据网、开放系统通信和安全性** |
| Y 系列 | 全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市 |
| Z 系列 | 用于电信系统的语言和一般软件问题 |

瑞士印刷
2019年，日内瓦