Международный союз электросвязи

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

# X.1215

(01/2019)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

---

# Сценарии использования структурированного представления информации об угрозах

Рекомендация МСЭ-Т X.1215

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

**СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ**

| | |
|---|---|
| СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ | X.1–X.199 |
| ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ | X.200–X.299 |
| ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ | X.300–X.399 |
| СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ | X.400–X.499 |
| СПРАВОЧНИК | X.500–X.599 |
| ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ | X.600–X.699 |
| УПРАВЛЕНИЕ В ВОС | X.700–X.799 |
| БЕЗОПАСНОСТЬ | X.800–X.849 |
| ПРИЛОЖЕНИЯ ВОС | X.850–X.899 |
| ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА | X.900–X.999 |
| БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ | |
| Общие аспекты безопасности | X.1000–X.1029 |
| Безопасность сетей | X.1030–X.1049 |
| Управление безопасностью | X.1050–X.1069 |
| Телебиометрия | X.1080–X.1099 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Безопасность многоадресной передачи | X.1100–X.1109 |
| Безопасность домашних сетей | X.1110–X.1119 |
| Безопасность подвижной связи | X.1120–X.1139 |
| Безопасность веб-среды | X.1140–X.1149 |
| Протоколы безопасности | X.1150–X.1159 |
| Безопасность одноранговых сетей | X.1160–X.1169 |
| Безопасность сетевой идентификации | X.1170–X.1179 |
| Безопасность IPTV | X.1180–X.1199 |
| БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА | |
| **Кибербезопасность** | **X.1200–X.1229** |
| Противодействие спаму | X.1230–X.1249 |
| Управление определением идентичности | X.1250–X.1279 |
| БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ | |
| Связь в чрезвычайных ситуациях | X.1300–X.1309 |
| Безопасность повсеместных сенсорных сетей | X.1310–X.1319 |
| Безопасность "умных" электросетей | X.1330–X.1339 |
| Сертифицированная электронная почта | X.1340–X.1349 |
| Безопасность интернета вещей (IoT) | X.1360–X.1369 |
| Безопасность интеллектуальных транспортных систем (ИТС) | X.1370–X.1389 |
| Безопасность технологии распределенного реестра | X.1400–X.1429 |
| Протоколы безопасности | X.1450–X.1459 |
| ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ | |
| Обзор кибербезопасности | X.1500–X.1519 |
| Обмен информацией об уязвимости/состоянии | X.1520–X.1539 |
| Обмен информацией о событии/инциденте/эвристических правилах | X.1540–X.1549 |
| Обмен информацией о политике | X.1550–X.1559 |
| Эвристические правила и запрос информации | X.1560–X.1569 |
| Идентификация и обнаружение | X.1570–X.1579 |
| Гарантированный обмен | X.1580–X.1589 |
| БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ | |
| Обзор безопасности облачных вычислений | X.1600–X.1601 |
| Проектирование безопасности облачных вычислений | X.1602–X.1639 |
| Передовой опыт и руководящие указания в области облачных вычислений | X.1640–X.1659 |
| Обеспечение безопасности облачных вычислений | X.1660–X.1679 |
| Другие вопросы безопасности облачных вычислений | X.1680–X.1699 |

*Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.*

# Рекомендация МСЭ-Т X.1215

## Сценарии использования структурированного представления информации об угрозах


**Резюме**

В Рекомендации МСЭ-Т X.1215 представлены различные сценарии возможного использования языка структурированного представления информации об угрозах (STIX) в поддержку сбора оперативной информации об угрозах (CTI) и совместного использования этой информации.

В настоящей Рекомендации описаны также понятия и функциональность языка STIX. Этот язык предназначен для поддержки целого ряда сценариев использования, связанных с управлением киберугрозами, включая анализ киберугроз, описание шаблонов индикаторов киберугроз, управление ответными действиями и совместное использование информации о киберугрозах. При наличии такой информации может быть принято решение по обеспечению безопасности, определяющее наиболее эффективный способ защиты от угрозы. Данный язык предназначен для поддержки более эффективного анализа и непрерывного обмена информацией о киберугрозах. Сопровождение пакета спецификаций STIX [b-STIX2.0] находится в ведении Организации по развитию стандартов структурированной информации (OASIS).



**Хронологическая справка**

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-Т X.1215 | 30.01.2019 г. | 17-я | 11.1002/1000/13849 |

**Ключевые слова**

Оперативная информация об угрозах, совместное использование информации, безопасность, STIX.


* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

## ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

## ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

## ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

# Содержание

# Рекомендация МСЭ-Т X.1215

## Сценарии использования структурированного представления информации об угрозах

### 1 Сфера применения

Цель настоящей Рекомендации – представить различные сценарии использования структурированного представления информации об угрозах (STIX), то есть структурированного языка описания информации о киберугрозах. Данный язык предназначен для поддержки целого ряда сценариев использования, связанных с управлением киберугрозами, включая анализ киберугроз, описание шаблонов индикаторов киберугроз, управление ответными действиями и совместное использование информации о киберугрозах. Эти сценарии использования обычно просты по сути и не передают в полной мере всю выразительность или гибкость языка STIX. Сценарии использования включают, как правило, определенный текст, описывающий действия в рамках данного сценария, представление контента STIX и документы, содержащие полностью проверенный контент STIX. Реализация этих сценариев использования представлена на расширяемом языке разметки (XML), так как в STIX версии 1.2, выпущенной в 2016 году, используется схема XML, а в версии 2.0 используется нотация объектов JavaScript (JSON). Рекомендуется использовать требования, описанные в STIX 2.0.

### 2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

### 3 Определения

#### 3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах

**3.1.1 объект (entity)** [b-STIX2.0.1]: все, что имеет индивидуально идентифицируемую форму существования (например, организация, лицо, группа и т. д.).

**3.1.2 объект STIX (STIX object)** [b-STIX2.0.1]: объект домена STIX (SDO) или объект связей STIX (SRO).

**3.1.3 структурированное представление информации об угрозах (STIX) (structured threat information expression, STIX)** [b-STIX2.0.1]: язык и формат сериализации, используемые для обмена оперативной информацией о киберугрозах (CTI).

**3.1.4 надежный автоматический обмен информацией об индикаторах** (trusted automated eXchange of indicator information) (TAXII) [b-STIX2.0.1]: протокол прикладного уровня для передачи информации о киберугрозах.

#### 3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

## 4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | | |
|---|---|---|---|
| CAPEC | Common Attack Pattern Enumeration and Classification | | Перечень и классификация общеизвестных схем атак |
| COA | Course Of Action | | Действие |
| CnC | Command and Control | | Управление и контроль |
| CTI | Cyber Threat Intelligence | | Оперативная информация о киберугрозах |
| CVE | Common Vulnerability and Exposures | | Общеизвестные уязвимости и незащищенности |
| C2 | Command and Control | | Управление и контроль |
| DLL | Dynamic Link Library | | Библиотека динамической компоновки |
| EDR | Event Data Recorder | | Регистратор данных о событиях |
| JSON | JavaScript Object Notation | | Нотация объектов JavaScript |
| OS | Operating System | ОС | Операционная система |
| SDO | STIX Domain Object (a "node" in a graph) | | Объект STIX "домен" ("узел" на графе) |
| SMBv2 | Server Message Block version 2 | | Блок сообщений сервера версии 2 |
| SRO | STIX Relationship Object (one mechanism to represent an "edge" in a graph) | | Объект STIX "связь" (механизм для представления "ребра" графа) |
| STIX | Structured Threat Information Expression | | Структурированное представление информации об угрозах |
| TAXII | Trusted Automated exchange of Indicator Information | | Надежный автоматический обмен информацией об индикаторах |
| TTP | Tactic, Technique, and Procedure | | Тактики, техника действий и порядок их выполнения |
| TLP | Traffic Light Protocol | | Протокол маркировки информации |
| XML | Extensible Markup Language | | Расширяемый язык разметки |

## 5 Условные обозначения

Отсутствуют.

## 6 Обзор STIX

### 6.1 Понятия STIX

Для реагирования на киберугрозы в реальном времени следует обеспечивать не только отдельную систему безопасности, но и глобальную совместную систему безопасности, так как существуют глобальные проблемы, которые невозможно разрешить силами какого-либо одного объекта или одного домена [b-STIX2.0]. Вследствие этого, важным компонентом программы обеспечения безопасности любой организации является глобальная оперативная информация о киберугрозах (CTI), которая может быть получена из внутренних и внешних источников. Одним из решений получения информации о киберугрозах и ее совместного использования является структурированное представление информации об угрозах (STIX) – структурированный язык описания информации о киберугрозах. STIX обеспечивает структурированное представление информации о киберугрозах, которое является выразительным, гибким, расширяемым, автоматизируемым и удобочитаемым.

### 6.2 Объекты в STIX

#### 6.2.1 Объекты в STIX 1.2

В настоящей Рекомендации должны быть приняты семь объектов домена STIX (SDO), которые описаны ниже.

1) Кампания (campaign): кампания STIX представляет собой набор тактик, техники действий и порядка их выполнения (TTP), инцидентов или злоумышленников, которые – вместе – выражают общее намерение или желаемый результат.

2) Действие (course of action): действие STIX – это компонент, который используется для передачи информации о действиях, которые могут быть выполнены либо в ответ на атаку, либо в качестве предупредительных мер до атаки.

3) Цель эксплойта (exploit target): цель эксплойта STIX передает информацию о технической уязвимости, слабости или ошибке конфигурации в программном обеспечении, системах или сетях, которые может использовать противник.

4) Инцидент (incident): инцидент STIX передает информацию о нарушении кибербезопасности.

5) Индикатор (indicator): индикатор STIX представляет конкретные наблюдаемые шаблоны в сочетании с контекстной информацией.

6) Злоумышленник (threat actor): злоумышленник STIX передает информацию, которая характеризует или идентифицирует (или и то и другое) противника.

7) TTP: TTP – это военный термин, который расшифровывается как "тактики, техника действий и порядок их выполнения ".

### 6.2.2 Объекты в STIX 2.0

В настоящей Рекомендации должен быть принят набор объектов "домен" STIX (SDO) и объектов "связь" STIX (SRO), которые определены в [b-STIX2.0-Part 2] для представления информации о киберугрозе.

В [b-STIX2.0-Part 2] определены двенадцать SDO, которые описаны ниже.

1) Схема атаки (attack pattern*)*: схемы атаки – это тип TTP, который описывает способы, с помощью которых противники пытаются поразить цель.

2) Кампания (campaign): кампания – это объединение в группу враждебного поведения, которое описывает набор злоумышленных действий или атак (иногда называемых волнами), предпринимаемых в течение некоторого период времени в отношении конкретного набора целей.

3) Действие (course of action): действие – это мера, принимаемая либо для предотвращения атаки, либо в ответ на осуществляемую атаку.

4) Идентичность (identity): идентичности могут представлять фактически существующих отдельных лиц, организации или группы (например, ACME, Inc.), а также классы лиц, организаций или групп (например, финансовый сектор).

5) Индикатор (indicator): индикаторы содержат шаблон, который может использоваться для обнаружения подозрительной или злонамеренной киберактивности.

6) Серия вторжений (intrusion set): серия вторжений – это сгруппированный набор враждебных действий и ресурсов, обладающих общими свойствами, которыми, как предполагается, руководит одна организация.

7) Вредоносная программа (malware): вредоносная программа – это тип TTP, который называется также вредоносным кодом или вредоносным программным обеспечением и означает программу, которая внедряется в систему, как правило скрытно, с целью нарушения конфиденциальности, целостности или доступности данных, приложений или операционной системы (ОС) объекта воздействия или же иным образом затрагивает или разрушает объект воздействия.

8) Данные наблюдения (observed data): данные наблюдения представляют информацию, которая наблюдалась в системах и сетях, с использованием спецификации кибернаблюдаемых результатов, определенных в частях 3 и 4 настоящей спецификации.

9) Отчет (report): отчеты – это наборы оперативной информации об угрозах по одной или нескольким темам, например описание злоумышленника, вредоносной программы или метода атаки, включая контекст и связанные с ним подробные данные.

10) Злоумышленник (threat actor): злоумышленники – это фактически существующие отдельные лица, группы или организации, которые, как полагают, действуют со злоумышленным намерением.

11) Инструмент (tool): инструменты – это законное программное обеспечение, которое может использоваться злоумышленниками для осуществления атак. Знание о способе и времени использования злоумышленниками таких инструментов может быть важным для понимания порядка осуществления кампаний.

12) Уязвимость (vulnerability): уязвимость – это "ошибка в программном обеспечении, которую взломщик может использовать напрямую для получения доступа в систему или сеть".

В [b-STIX2.0-Part 2] определены два SRO, которые описаны ниже.

1) Связь (relationship): объект "связь" используется для связывания двух SDO, с тем чтобы описать, как они взаимосвязаны между собой.

2) Визуальное обнаружение (sighting): визуальное обнаружение означает утверждение, что в CTI что-то (например, индикатор, вредоносная программа, инструмент, злоумышленник) было замечено.

### 6.3 Характеристики и инструменты в STIX

STIX обеспечивает нижеследующие характеристики.

– Схемы JSON/XML: в STIX 2.0 используется схема JSON для представления шести объектов и свойств. В STIX версии 1.0 используется схема XML.

– Объект STIX "домен": все объекты в STIX находятся на верхнем уровне. Эти объекты обозначаются аббревиатурой SDO STIX. В некоторых свойствах объектов используется прямая ссылка на идентификатор другого объекта (например, created_by_ref), но большинство связей описываются с использованием объекта "связь" верхнего уровня.

– Объект STIX 2.0 "связь": в STIX 2.0 введен объект "связь" верхнего уровня, который связывает два других объекта верхнего уровня через поименованный тип связи.

В настоящей Рекомендации должен использоваться нижеследующий набор инструментов, которые определены в [b-STIX2.0 tool].

– Валидатор STIX: валидатор STIX – это полезный ресурс для проверки соответствия контента STIX JSON спецификации 2.0.

– Валидатор шаблонов: шаблоны STIX – это выражения, которые представляют кибернаблюдаемые объекты в индикаторе SDO STIX. Они полезны для моделирования оперативной информации, которая указывает на киберактивность. Этот инструмент просто проверяет, что синтаксис составления шаблона соответствует представлению шаблона.

– Визуализация STIX: инструмент визуализации STIX предоставлен в помощь при преобразовании схемы JSON в более лаконичную и четкую диаграмму.

– Лифт STIX: элеваторный инструмент способствует реализации этого преобразования и обеспечивает лучшее из возможного преобразование 1.x в 2.0.

– Сопоставитель шаблонов STIX: инструмент сопоставления шаблонов обеспечивает способ сравнения данных наблюдения STIX и шаблонов индикаторов STIX.

## 7 Сценарии использования STIX 2.0

В настоящей Рекомендации представлены различные сценарии возможного использования языка STIX для поддержки сбора оперативной информации о киберугрозах и совместного использования информации. Язык предназначен для поддержки целого ряда сценариев использования (UC), связанных с управлением киберугрозами, включая анализ киберугроз (UC1, пункт 7.2.1), описание шаблонов индикаторов для киберугроз (UC2, пункт 7.2.2), управление ответными действиями на киберугрозу (UC3, пункт 7.2.3) и совместное использование информации о киберугрозах (UC4). Совместное использование информации о киберугрозах (UC4) в настоящей Рекомендации не рассматривается. Обзор примера сценария использования STIX отражен на рисунке 1. Сценарий использования STIX 1.0 представлен в Приложении A.

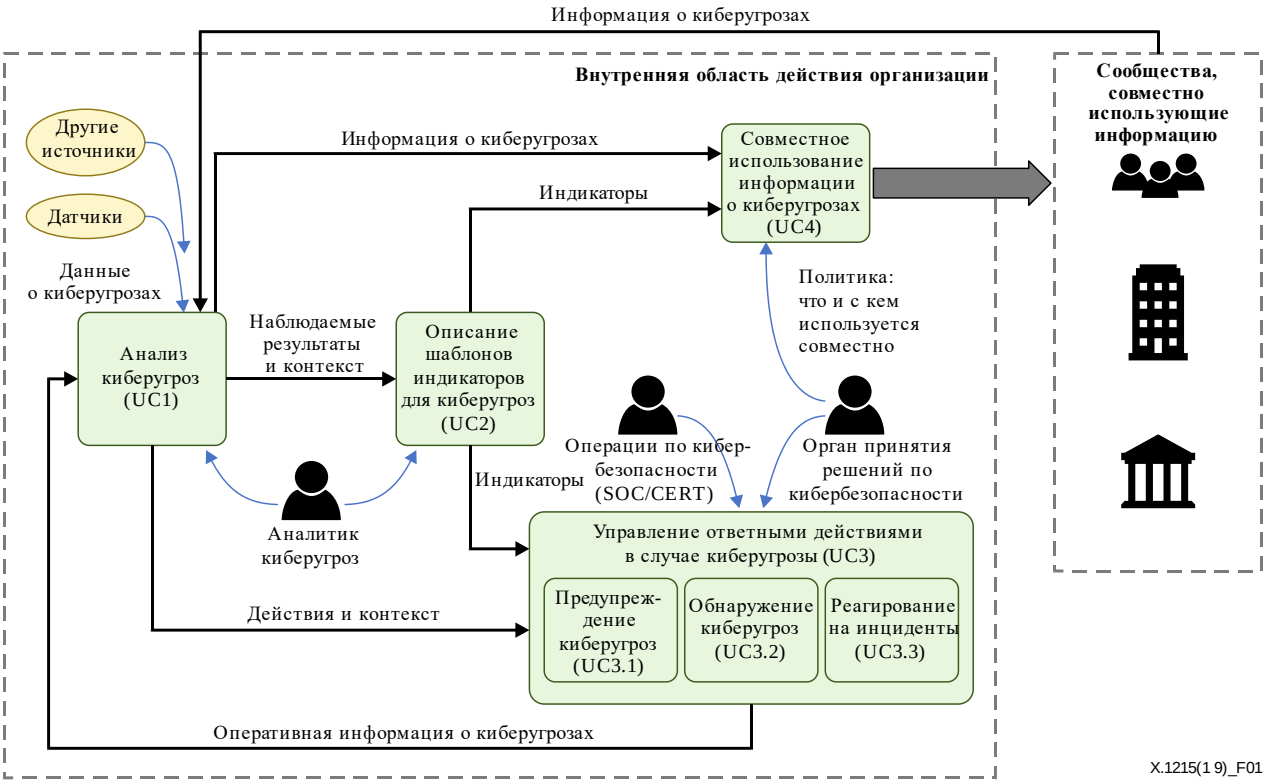


**Рисунок 1 − Обзор сценария использования STIX**

## 7.1 Сценарий использования STIX 2.0 в случае программы-вымогателя

Программа-вымогатель – это разновидность вредоносного программного обеспечения, которое заражает компьютерные системы, ограничивает доступ к данным объекта воздействия и требует уплаты выкупа. Ограниченный доступ к компьютеру вынуждает объект воздействия платить разработавшей вредоносную программу структуре, для того чтобы снять ограничения. Атаки программ-вымогателей осуществляются, как правило, с использованием программы-трояна, замаскированной под законный файл, который обманутый пользователь загружает или открывает, если файл поступает к нему как вложение в электронном письме.

Недавно по всему миру началась атака на компьютеры программы-вымогателя WannaCry; эта программа автоматически распространяется между компьютерами без взаимодействия с пользователем. В отличие от обычных программ-вымогателей, которые распространяются через вложения в электронном письме, для заражения WannaCry требуется только, чтобы уязвимые системы были подсоединены к интернету. Программа-вымогатель WannaCry шифрует разные файлы как файлы документов, сжатые файлы, файлы баз данных и файлы виртуальных машин.

В данном разделе описан сценарий, иллюстрирующий возможность использования языка STIX 2.0 для поддержки управления киберугрозами, предназначенного для борьбы с программой-вымогателем WannaCry.

### 7.1.1 Анализ киберугроз

В данном разделе представлена анализируемая информация о программе-вымогателе (WannaCrypt), полученная по факту предпринимаемых по всему миру атак вредоносного кода с использованием программы-вымогателя, которая нацелена на уязвимость удаленного выполнения кода протокола блока сообщений сервера версии 2 (SMBv2).

#### 7.1.1.1 Идентичность

Информация о наблюдателе может быть определена как объект "идентичность".

#### 7.1.1.2 Данные наблюдения

Обнаружено, что электронное письмо с уведомлением об отправке было получено с архивом файлов .egg и наблюдалось 52 домена сервера "управление и контроль" (CnC) (в данном примере только два домена сервера CnC).

```
{
   "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

Получены данные о том, что наблюдалась атака программы-вымогателя, нацеленная на отдельный компьютер; схема атаки – действие целевой атаки с использованием вредоносной программы, и объект "связь" (relationship), который использует вредоносную программу, может быть создан как схема атаки.

```
{
   "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 Уязвимость

Получены данные, что уязвимость относится к общеизвестным уязвимостям и незащищенностям (CVE)-2017-0147 и CVE-2017-0143, и программа-вымогатель использует уязвимость удаленного выполнения кода SMBv2 (выпуск исправления 17.3.14 MS17-010) в Microsoft Windows. Может быть создан объект "связь" (relationship), который использует вредоносную программу, нацеленную на данную уязвимость.

```
{
 "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 Кампания и злоумышленник

Получены данные, что два объекта определены как кампания и злоумышленник в составе информации об атаке программы-вымогателя. Определено, что для кампании и злоумышленника может быть создана связь "отнесено к" (attributed-to), для кампании и схемы атаки – связь "использует" (uses), для кампании и уязвимости – связь "цели" (targets).

```
{
      "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 Описание шаблонов индикаторов для киберугроз

#### 7.1.2.1 Индикатор

Получены данные, что URL сайта распространения программы-вымогателя определяется как индикатора типа "контроль URL" (URL watch), и может быть создан объект "связь" (relationship), представляющий вредоносную программу.

```
{
      "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 Управление ответными действиями

#### 7.1.3.1 Действие

Получены данные, что существуют средства защиты "отключение протокола SMB" (disabling the SMB protocol) и "исправление уязвимости программного обеспечения" (software vulnerability patching), которые можно определить как объекты "действие" (COA). Может быть создан объект "связь" (relationship), смягчающий воздействие вредоносной программы, для каждого объекта.

```
{
   "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 Обзор сценариев атаки с использованием диаграммы связей

На рисунке 2 показаны связи между всеми объектами STIX, которые служат для описания сценария использования.

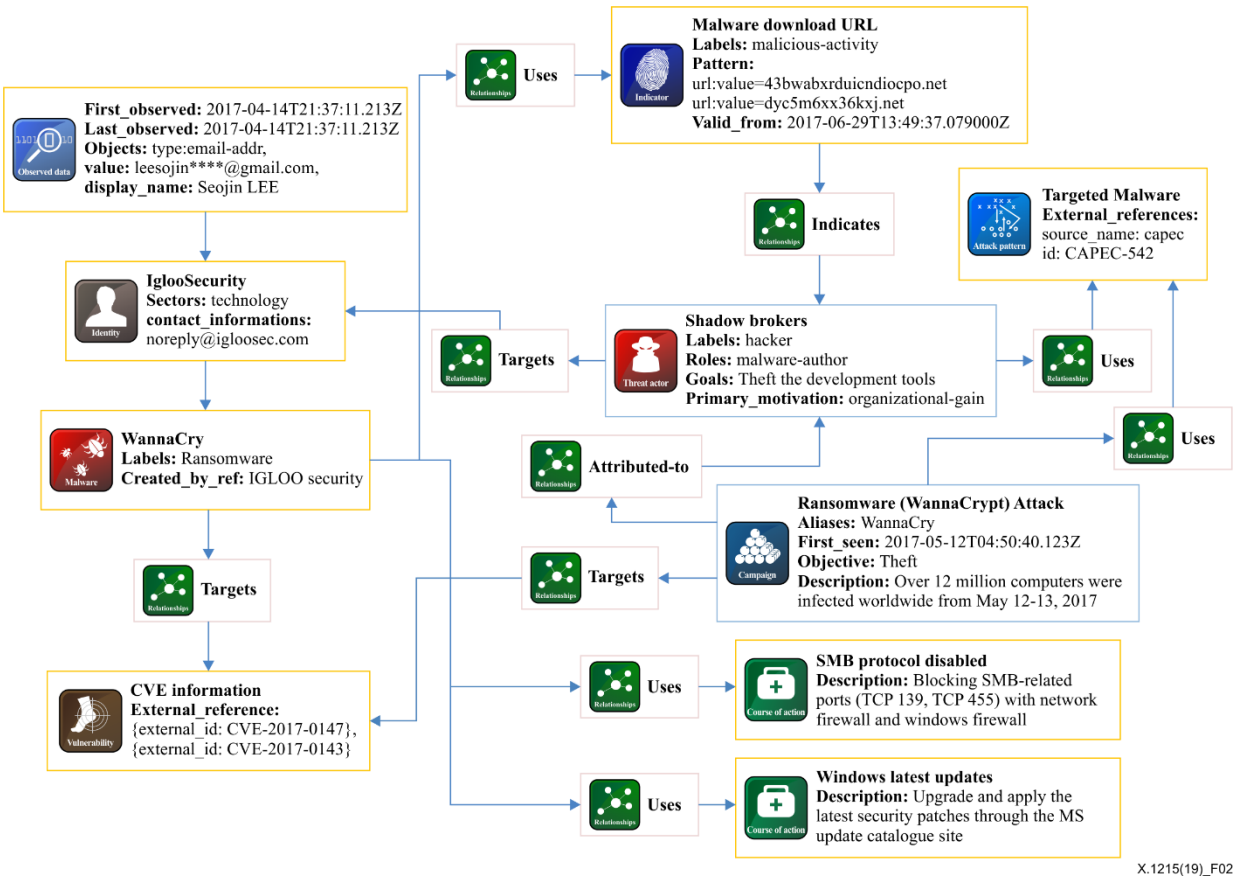


**Рисунок 2 – Связь между объектами STIX для описания варианта использования**

В качестве резюме: ниже описан пакет (bundle) объектов STIX, который включает все объекты, используемые для обнаружения и анализа злонамеренных атак, совершаемых программой-вымогателем, которую называют WannaCry, а также для противодействия таким атакам.

```
{
  "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 Сценарий использования в случае кибератаки на обмен криптовалюты

В данном разделе описан случай атаки на обмен криптовалюты в Корее, которую осуществил злоумышленник, называемый "Lazarus APT group", 20 июня 2018 года.

В этом сценарии злоумышленник отправил фишинговую электронную почту, содержащую вредоносный код, сотрудникам, выполнявшим обмен криптовалюты. Фишинговая электронная почта сопровождалась скрытым текстовым файлом в формате PostScript, который мог позже загрузить вредоносные библиотеки динамической компоновки (DLL). Текстовый файл использовал уязвимость текстового процессора Hangul для запуска файла PostScript, в результате чего на компьютер пользователя был установлен файл DLL. Вредоносный файл DLL захватил контроль над пользовательским компьютером и получил доступ к серверам, открытым во время операций обмена. Вследствие этого, атакующий смог получить доступ к кошельку, используемому для обмена криптовалюты, и изъял значительную сумму средств из этого кошелька.

#### 7.2.1 UC1: Анализ киберугроз

Об атаках на обмен криптовалюты сообщалось несколько раз в период с июня по июль 2018 года. В данном сценарии проводится анализ инцидента взлома, целью которого был обмен криптовалюты компании "BC-Company".

##### 7.2.1.1 Идентичность

Базовую информацию, идентифицирующую наблюдателя, можно моделировать с помощью объекта "идентичность" (identity). Организация, зафиксировавшая этот инцидент, и место, где этот инцидент произошел, могут быть смоделированы как объекты "идентичность".

Для идентификации автора объекта "отчет STIX" организации, осуществляющие мониторинг безопасности – WINS и IGLOO Security, представлены как объекты "идентичность". Цель инцидента моделируется как объект "идентичность", имеющий свойство "BC-Company.com", которое является псевдонимом. Этот объект описан в поле where_sighted_refs объекта "визуальное обнаружение" (sighting), который рассматривается ниже, и используется в качестве цели атаки для схем атаки и вредоносной программы.

```
{
"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 Данные наблюдения

Данные наблюдения представляют собой генерируемую машиной первичную информацию и отличаются от индикаторов, которые обусловливают более интеллектуальные заключения. Объект "данные наблюдения" (observed-data) содержит кибернаблюдаемую информацию, собранную в системах и сетях, например IP-адреса, файлы и URL. В данном случае наблюдался файл. Другая ссылка, "sighting_of_ref", содержит идентификатор SDO, который был обнаружен, что в данном случае является объектом "данные наблюдения".

В процессе обмена криптовалюты наблюдался файл, переданный по электронной почте. Имя файла и адрес электронной почты отправителя представлены как объект "данные наблюдения". Объекты "данные наблюдения", которые наблюдаются в других местах, представлены как объекты "визуальное обнаружение" (sighting). Наблюдаемое местоположение представлено свойством where_sighted_rerfs.

```
        {
            "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 Тактики, техника действий и порядок их выполнения

В данном разделе описаны основные качества, характеризующие содержание и проявление злоумышленного поведения.

Источником атаки было вложение в фишинговой электронной почте, и для атаки использовались два типа вредоносных кодов. Фишинговые атаки описаны в Перечне и классификации общеизвестных схем атак (CAPEC) с номером 163 и представлены объектом "схема атаки" (attack pattern). Вредоносный код, поступивший из фишинговой электронной почты, загружает вредоносную DLL, которая использует уязвимость CVE-2015-2545. Таким образом, объекты "вредоносная программа" (malware) имеют метки "эксплойт" (exploit) и "сбрасыватель" (dropper). В случае вредоносных библиотек DLL, появляющихся позже, троян удаленного доступа имеет метку "вредоносный код" (malicious code), который захватывает контроль над пользовательским компьютером.

Связь между двумя вредоносными кодами описана как тип "связан с" (related-to), что указывает на наличие связи между вредоносным документом и вредоносной DLL.

Осуществляя направленный фишинг, атакующий использовал сильно замаскированный документ. Данная атака направлена на обмен криптовалюты, поэтому используется объект "связь" (relationship) типа "цель" (target).


```
{
    "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 Уязвимость

В данном случае используется уязвимость CVE-2015-2545, которая скрывает вредоносный PostScript в документе текстового процессора Hangul и заставляет его выполняться. Для моделирования данной уязвимости используется объект "уязвимость" (vulnerability). Объект "связь" (relationship) показывает также связь между вредоносным кодом и уязвимостью.


```
{
    "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 Кампания и злоумышленник

Группа Lazarus APT распространяет в рамках направленного фишинга электронную почту, в которую встроен вредоносный код, с целью кражи криптовалюты, сохраняющейся в процессе обмена криптовалюты.

Цель объекта "злоумышленник" (threat-actor) представлена в свойстве "цели" (goals) как "украсть криптографическую валюту" (steal cryptographic currency). В силу того, что был создан вредоносный документ, для свойства "роли" (roles) установлено значение "автор вредоносной программы" (malware-author). Он использовался для совершения преступления, поэтому для свойства "метка" (label) установлено значение "преступное сообщество" (crime-syndicate).

Атака на процесс обмена криптовалюты представлена как объект "кампания" (campaign), свойству "задача" (objective) присвоено значение "кража" (Theft).

Объекты, соответствующие методам осуществления атаки и вредоносному коду, используемым при проведении кампании, представлены объектами "связь" (relationship) типа "используют" (use).


```
        {
            "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: описание шаблонов индикаторов для киберугроз

#### 7.2.2.1 Индикатор

Объекты "индикатор" (indicator) идентифицируют вредоносные документы и вредоносные DLL. Для вредоносных документов свойство "шаблон" (pattern) в объекте "индикатор" представлено либо как URL, либо как хеш-значения файлов для загрузки вредоносных DLL. В данном сценарии шаблоны вредоносных DLL в объекте "индикатор" представляют собой URL управления и контроля (C2) и хеш-значение файла. Это позволяет зарегистрировать политику. Несколько объектов "связь" (relationship) типа "указывает" (indicates) показывают связь между двумя вредоносными кодами.


```
{
    "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: управление ответными действиями в случае киберугрозы

#### 7.2.3.1 Действие

В данном сценарии атаки действие группы реагирования разделяется на обнаружение и реагирование. Сначала запускается выполнение вредоносного документа, затем начинается атака.

Хеш-значение вредоносного документа регистрируется в рамках политики обеспечения безопасности в инструменте анализа вредоносных программ, например YARA. Регистратор данных о событиях (EDR) может обнаружить атаку, когда выполняется файл с хеш-значением. Кроме того, устройства обеспечения сетевой безопасности реагирует, блокируя трафик к загруженному URL вредоносной DLL, с тем чтобы заблокировать загрузку вредоносной DLL и не допустить кражи прав контроля над компьютером. В случае если вредоносная DLL взломана, сетевое устройство может блокировать вредоносную активность, блокируя трафик к URL C2.


```
{
    "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 Диаграмма связей и комплект объектов

На рисунке 3 показана связь между всеми объектами для описания данного сценария использования.

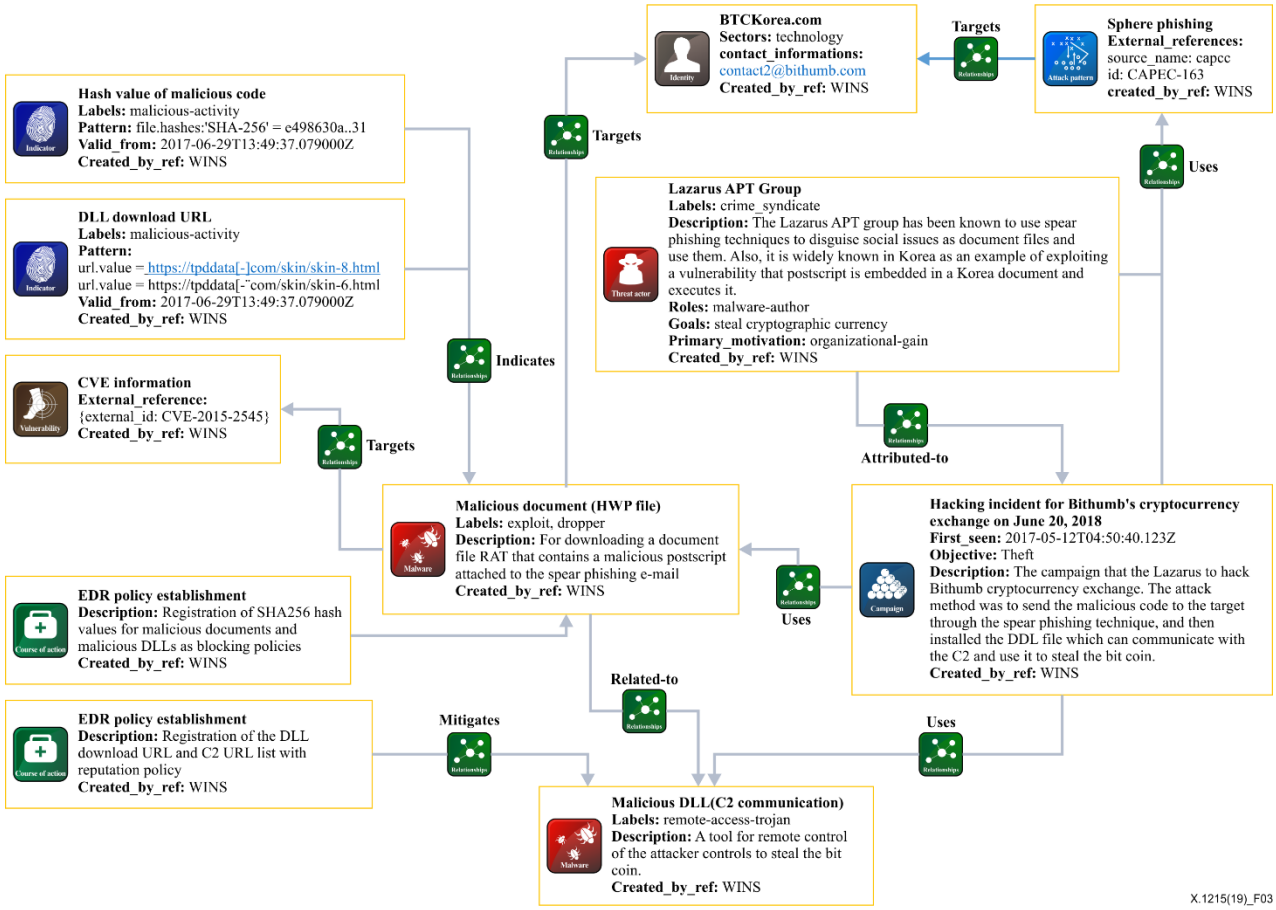


**Рисунок 3 – Связь между объектами STIX для описания сценария использования**

В качестве резюме: ниже описан комплект (bundle) объектов STIX, который включает все объекты, используемые для обнаружения и анализа злонамеренных атак, совершаемых группой Lazarus, а также для противодействия таким атакам.

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

# Приложение A

## Сценарий использования STIX 1.2 в случае программы-вымогателя

(Данное Приложение является неотъемлемой частью настоящей Рекомендации)

В данном Приложении описан сценарий, иллюстрирующий возможность использования языка STIX 1.2 для поддержки управления киберугрозами, предназначенного для борьбы с программой-вымогателем WannaCry.

### A.1 Анализ киберугроз

В данном разделе представлена анализируемая информация о программе-вымогателе (WannaCrypt), полученная по факту предпринимаемых по всему миру атак вредоносного кода с использованием программы-вымогателя, которая нацелена на уязвимость удаленного выполнения кода протокола SMBv2.

#### A.1.1 Наблюдаемые результаты

Обнаружено, что электронное письмо с уведомлением об отправке было получено с архивом файлов .egg и наблюдалось 52 домена сервера CnC.

```
<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

Получены данные о том, что наблюдалась атака программы-вымогателя, нацеленная на отдельный компьютер; схема атаки – действие целевой атаки с использованием вредоносной программы, и целью атаки является информация, которой владеет организация.

```
<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 Цель эксплойта

Получены данные, что используемая уязвимость является уязвимостью (CVE-2017-0147, CVE-2017-0143) и ОС Windows 10, и программа-вымогатель использует уязвимость удаленного выполнения кода SMBv2 в 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_
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 Инцидент

Получены данные, что категорией является "несанкционированный доступ" (unauthorized access), целевые ресурсы – информация, которой обладает организация, затронутые объекты, а также ответные меры в связи с инцидентом – "кража" (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 Злоумышленник

Получены данные, что типом атакующего является "разработчик вредоносной программы" (malware developer), его мотивы – финансовые или экономические (financial or economic), квалификация – эксперт (expert), намерение нарушителя – кража (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 Кампания

Получены данные, что описаны относящиеся к инциденту TTP и злоумышленник, для того чтобы отразить намерение злоумышленника.

```
<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 Описание шаблонов индикаторов для киберугроз

### A.2.1 Индикатор

Получены данные, что определены типы индикаторов "вредоносная электронная почта" (malicious e-mail), "эксфильтрация" (exfiltration), "контроль URL" (URL watch) и соответствующие наблюдаемые результаты, TTP и кампания связаны.

```
<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 Управление ответными действиями

### A.3.1 Действие

Отмечено, что возможны защитные меры с помощью исправления уязвимости программного обеспечения, отсутствует воздействие в аспекте ограничения соединения, стоимость ответных мер низкая, эффективность ответных мер средняя.

```
<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>
```

# Библиография


[b-ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности*.

[b-RFC7159]Bray, T., Ed., The JavaScript Object Notation (JSON) (2014), *Data Interchange Format*, RFC 7159, DOI 10.17487/RFC7159.

[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

## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|---|---|
| Серия A | Организация работы МСЭ-Т |
| Серия D | Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ |
| Серия E | Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы |
| Серия F | Нетелефонные службы электросвязи |
| Серия G | Системы и среда передачи, цифровые системы и сети |
| Серия H | Аудиовизуальные и мультимедийные системы |
| Серия I | Цифровая сеть с интеграцией служб |
| Серия J | Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов |
| Серия K | Защита от помех |
| Серия L | Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений |
| Серия M | Управление электросвязью, включая СУЭ и техническое обслуживание сетей |
| Серия N | Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ |
| Серия O | Требования к измерительной аппаратуре |
| Серия P | Качество телефонной передачи, телефонные установки, сети местных линий |
| Серия Q | Коммутация и сигнализация, а также соответствующие измерения и испытания |
| Серия R | Телеграфная передача |
| Серия S | Оконечное оборудование для телеграфных служб |
| Серия T | Оконечное оборудование для телематических служб |
| Серия U | Телеграфная коммутация |
| Серия V | Передача данных по телефонной сети |
| **Серия X** | **Сети передачи данных, взаимосвязь открытых систем и безопасность** |
| Серия Y | Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города |
| Серия Z | Языки и общие аспекты программного обеспечения для систем электросвязи |

Отпечатано в Швейцарии
Женева, 2019 г.