Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1215

(01/2019)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Expresión estructurada de información sobre amenazas: casos de uso

Recomendación UIT-T X.1215

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1215

Expresión estructurada de información sobre amenazas: casos de uso

Resumen

En la Recomendación UIT-T X.1215 se presentan varios casos de uso relativos a la manera de utilizar el lenguaje de expresión estructurada de información sobre amenazas (STIX, *structured threat information expression*) para la inteligencia de ciberamenazas (CTI, *cyber threat intelligence*) y la compartición de información.

En esta Recomendación se describen también los conceptos y funcionalidades del lenguaje STIX. Está destinado a dar soporte a diversos casos de uso relacionados con la gestión de ciberamenazas, incluido el análisis de las ciberamenazas, la especificación de indicadores modelo de ciberamenazas, la gestión de la respuesta y la compartición de información sobre ciberamenazas. Con esta información es posible tomar decisiones de seguridad sobre la mejor defensa contra las amenazas. Está previsto para soportar un análisis más eficaz y el intercambio continuo de información sobre ciberamenazas. El mantenimiento de la serie de especificaciones de STIX [b-STIX2.0] es responsabilidad de la Organización para la Promoción de las Normas de Información Estructurada (OASIS).

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1215	2019-01-30	17	11.1002/1000/13849

Palabras clave

Compartición de información, inteligencia de ciberamenazas, seguridad, STIX.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1215

Expresión estructurada de información sobre amenazas: casos de uso

1 Alcance

El objetivo de esta Recomendación es presentar diversos casos de uso de la expresión estructurada de información sobre amenazas (STIX), que es un lenguaje estructurado para describir información sobre ciberamenazas, previsto para soportar diversos casos de uso de gestión de ciberamenazas, incluido el análisis de las ciberamenazas, la especificación de los patrones indicadores de ciberamenazas, la gestión de la respuesta y la compartición de información sobre ciberamenazas. Estos casos de uso suelen ser fundamentalmente simples y no permiten explotar al máximo la expresividad o flexibilidad del lenguaje STIX. Por norma general los casos de uso contienen una descripción textual de las actividades en cuestión, representaciones del contenido STIX y documentos con contenido STIX totalmente validados. Se presenta una muestra de los casos de uso en lenguaje de marcación extensible (XML), pues la versión 1.2 de STIX, publicada en 2016, utiliza el esquema XML, mientras que la versión 2.0 emplea la notación de objeto JavaScript (JSON). Se recomienda utilizar los requisitos descritos en STIX 2.0.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. La referencia a un documento en el marco de esta Recomendación no le confiere carácter de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 entidad [b-STIX2.0.1]: Todo lo que tenga una existencia individual identificable (por ejemplo, una organización, una persona, un grupo, etc.).

3.1.2 objeto STIX [b-STIX2.0.1]: Un objeto de dominio STIX (SDO, *STIX Domain Object*) o un objeto de relación STIX (SRO, *STIX Relationship Object*).

3.1.3 expresión estructurada de información sobre amenazas (STIX) [b-STIX2.0.1]: Lenguaje y formato de serialización utilizados para intercambiar inteligencia de ciberamenazas (CTI, *cyber threat intelligence*).

3.1.4 intercambio automatizado fiable de información sobre indicadores (TAXII) [b-STIX2.0.1]: Protocolo de capa de aplicación para la comunicación de información sobre ciberamenazas.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Siglas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

CAPEC Enumeración y clasificación de pautas de ataques comunes (*common attack pattern enumeration and classification*)

COA Procedimiento (*course of action*)

CnC Mando y control (*command and control*)

CTI Inteligencia de ciberamenazas (*cyber threat intelligence*)

CVE Vulnerabilidad y exposición comunes (*common vulnerability and exposures*)

C2 Mando y control (*command and control*)

DLL Biblioteca de enlaces dinámicos (*dynamic link library*)

EDR Registrador de datos de eventos (*event data recorder*)

JSON Notación de objeto JavaScript (*JavaScript Object Notation*)

OS Sistema operativo (*operating system*)

SDO Objeto de dominio STIX (un "nodo" en un gráfico) (*STIX domain object (a "node" in a graph)*)

SMBv2 Bloque de mensajes de servidor versión 2 (*server message block version 2*)

SRO Objeto de relación STIX (mecanismo para representar un "borde" en un gráfico) (*STIX relationship object (one mechanism to represent an "edge" in a graph)*)

STIX Expresión estructurada de información sobre amenazas (*structured threat information expression*)

TAXII Intercambio automático fiable de información sobre indicadores (*trusted automated exchange of indicator information*)

TTP Táctica, técnica y procedimiento (*tactic, technique, and procedure*)

TLP Protocolo ligero de tráfico (*traffic light protocol*)

XML Lenguaje de marcación extensible (*extensible markup language*)

5 Convenios

Ninguno.

6 Aspectos generales de STIX

6.1 Conceptos de STIX

Para poder responder en tiempo real a las ciberamenazas, no solo hace falta un sistema de seguridad individual, sino también un sistema de gestión de la seguridad cooperativo global, pues hay problemas globales, que ni una sola entidad, ni un solo dominio pueden solucionar. Por consiguiente, la inteligencia de ciberamenazas (CTI, *cyber threat intelligence*) mundial es un componente importante de los programas de seguridad de las organizaciones, que puede obtenerse de fuentes internas y externas. Una de las soluciones para la inteligencia de ciberamenazas y la compartición de información es la expresión estructurada de información sobre amenazas (STIX, *structured threat information expression*), que es un lenguaje estructurado para describir la información sobre ciberamenazas. STIX ofrece una representación estructurada de la información sobre ciberamenazas expresiva, flexible, extensible, automatizable y legible.

6.2 Objetos de STIX

6.2.1 Objetos de STIX 1.2

STIX 1.2 tiene los siguientes siete objetos de dominio STIX (SDO, *STIX domain objects*) definidos:

1) Campaña: una campaña STIX es una serie de tácticas, técnicas y procedimientos (TTP, *tactic, technique, and procedures*), incidentes o agentes amenazantes que, juntos, expresan una intención común o un efecto deseado.
2) Procedimiento: el componente procedimiento STIX se utiliza para transmitir información sobre los procedimientos que se pueden ejecutar en respuesta a un ataque o como medida preventiva antes de un ataque.
3) Objetivo explotable: un objetivo explotable STIX transmite información sobre una vulnerabilidad técnica, un punto débil o una configuración errónea del software, el sistema o la red que un adversario puede explotar.
4) Incidente: un incidente STIX transmite información sobre un incidente de ciberseguridad.
5) Indicador: un indicador STIX transmite información sobre patrones observables específicos combinada con información contextual.
6) Agente amenazante: un agente amenazante STIX transmite la información que caracteriza o identifica al adversario (o ambas cosas).
7) TTP: término militar que significa "tácticas, técnicas y procedimientos".

6.2.2 Objetos de STIX 2.0

STIX 2.0 tiene el conjunto de objetos de dominio y objetos de relación definido que STIX utiliza para representar la información sobre ciberamenazas. STIX 2.0 tiene definidos los siguientes doce SDO:

1) Patrón de ataque: es un tipo de TTP que describe la manera en que los adversarios atacan los objetivos en peligro.
2) Campaña: es un grupo de comportamientos del adversario que describe una serie de actividades malignas o ataques (en ocasiones denominados olas) que se dan a lo largo de un periodo de tiempo contra un conjunto específico de objetivos.
3) Procedimiento: medida que se toma para prevenir un ataque o en respuesta a un ataque en curso.
4) Identidad: las identidades pueden representar a personas, organizaciones o grupos reales (por ejemplo, ACME S.A.) así como a clases de personas, organizaciones o grupos (por ejemplo, el sector financiero).
5) Indicador: los indicadores contienen un patrón que puede utilizarse para detectar actividades sospechosas o malignas en el ciberespacio.
6) Conjunto de intrusiones: conjunto de comportamientos y recursos adversos con propiedades comunes que se consideran orquestados por una única organización.
7) Malware: tipo de TTP, también conocido como código maligno o software maligno. Se refiere a un programa insertado en un sistema, generalmente de manera oculta, con el objetivo de poner en peligro la confidencialidad, la integridad o la disponibilidad de los datos, aplicaciones o sistemas operativos (OS, *operating system*) de la víctima o de molestarla o perjudicarla.
8) Datos observados: en datos observados se transmite la información observada en los sistemas y redes con la especificación ciberobservable definida en las partes 3 y 4 de esta recomendación.
9) Informe: recopilación de datos de inteligencia de amenazas centrada en uno o más temas, como la descripción de un agente amenazante, un malware o una técnica de ataque, además de su contexto y detalles.

10) Agente amenazante: personas, grupos u organizaciones reales cuyas operaciones se consideran malignas.

11) Herramienta: software legítimo que pueden utilizar los agentes amenazantes para llevar a cabo sus ataques. Saber cómo y cuándo los agentes amenazantes utilizan esas herramientas puede ser importante para entender cómo se realizan las campañas.

12) Vulnerabilidad: una vulnerabilidad es "un error del software que puede ser directamente utilizado por un pirata informático para acceder a un sistema o una red".

En STIX 2.0 se definen los dos siguientes objetos de relación STIX (SRO, *STIX relationship objects*):

1) Relación: el objeto relación se utiliza para vincular dos SDO a fin de describir cómo se relacionan mutuamente.

2) Avistamiento: denota la creencia de que se ha visto algo en la CTI (por ejemplo, un indicador, un malware, una herramienta, un agente amenazante).

6.3 Características y herramientas de STIX

STIX contiene las siguientes características:

– Esquemas JSON/XML: STIX 2.0 utiliza el esquema JSON para representar los seis objetos y propiedades. Además, STIX 1.0 utiliza el esquema XML.

– Objeto de dominio STIX: todos los objetos de STIX están en el nivel superior. Estos objetos se denominan SDO STIX. Algunas de las propiedades de los objetos utilizan una referencia directa al id de otro objeto (por ejemplo, *created_by_ref*), pero la mayoría de relaciones se expresan utilizando el objeto de relación de nivel superior.

– Objeto de relación STIX 2.0: STIX 2.0 presenta un objeto de relación de nivel superior que vincula dos otros objetos de nivel superior mediante un tipo de relación denominada.

STIX debe ofrecer las siguientes herramientas:

– Validador STIX: la herramienta validador STIX es un recurso útil para validar que el contenido JSON STIX se ajusta a la especificación 2.0.

– Validador de patrón: los patrones STIX son expresiones que representan objetos observables dentro de un SDO indicador STIX. Resultan útiles para modelar la inteligencia indicadora de la ciberactividad. Esta herramienta simplemente se asegura de que la sintaxis del patrón se ajusta a la expresión del patrón.

– Visualización STIX: la herramienta visualización STIX ayuda a convertir el JSON en un diagrama más conciso y legible.

– Elevador STIX: la herramienta elevador contribuye a ese objetivo y ofrece la mejor conversión posible de 1.x a 2.0.

– Comparador de patrones STIX: la herramienta comparador de patrones ofrece un medio para comparar los datos observados STIX y los patrones del indicador STIX.

7 Casos de uso de STIX 2.0

En esta Recomendación se presentan varios casos de uso para ilustrar cómo se puede utilizar el lenguaje STIX para la inteligencia de ciberamenazas y la compartición de información. Está previsto para utilizarse en diversos casos de uso (UC, use cases) en el contexto de la gestión de ciberamenazas, que incluye: el análisis de ciberamenazas (UC1, cláusula 7.2.1), la especificación de patrones indicadores de ciberamenazas (UC2, cláusula 7.2.2), la gestión de las actividades de respuesta frente a ciberamenazas (UC3, cláusula 7.2.3) y la compartición de información sobre ciberamenazas (UC4). En esta Recomendación no se aborda la compartición de información sobre ciberamenazas (UC4). En la Figura 1 se ilustra un ejemplo de caso de uso STIX. En el Anexo A puede encontrarse un caso de uso de STIX 1.0.

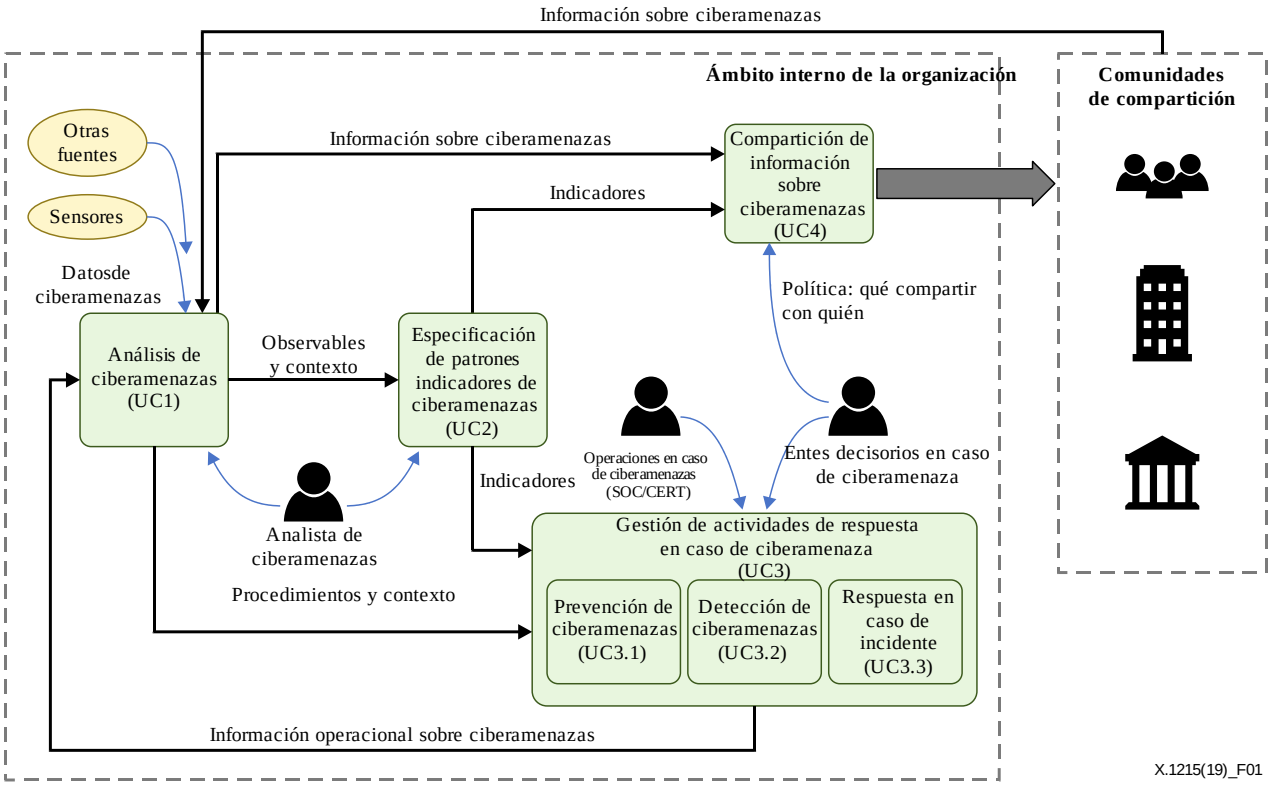

Figura 1 – Caso de uso de STIX

7.1 Caso de uso ransomware con STIX 2.0

El ransomware es un tipo de software maligno que infecta los sistemas informáticos, limita el acceso a los datos de la víctima y exige un rescate. Al estar limitado el acceso al ordenador, la víctima se ve obligada a pagar el rescate a la entidad que ha creado el programa maligno para que ésta suprima la restricción. Los ataques por ransomware suelen llevarse a cabo con un troyano disfrazado de fichero legítimo e induciendo al usuario a descargarlo o abrirlo cuando llega como adjunto a un correo electrónico.

Hace poco el ransomware WannaCry empezó a atacar a ordenadores de todo el mundo. Se propagaba automáticamente de un ordenador a otro sin interacción del usuario. A diferencia de los ransomware ordinarios, que se propagan como adjuntos a correos electrónicos, el vector de infección de WannaCry solo necesitaba que los sistemas vulnerables en cuestión estuviesen conectados a Internet. WannaCry encripta diversos ficheros, como los de documentos, los comprimidos, los de bases de datos y los de máquinas virtuales.

En esta cláusula se muestra cómo se puede utilizar el lenguaje STIX 2.0 en caso de ransomware para ayudar en la gestión contra la ciberamenaza que plantea un ransomware como WannaCry.

7.1.1 Análisis de ciberamenazas

En esta cláusula se presenta la información analizada del ransomware (WannaCrypt) extraída de ataques de código maligno de todo el mundo utilizando un ransomware de vulnerabilidad con ejecución de código a distancia de bloque de mensajes de servidor versión 2 (SMBv2).

7.1.1.1 Identidad

La información de un observador puede definirse como un objeto Identidad.

7.1.1.2 Datos observados

Se observa la recepción de un correo electrónico con una notificación de envío postal con un archivo de ficheros EGG y 52 dominios de servidor de mando y control (CnC, *command and control*) (solo dos dominios de servidor CnC en este ejemplo).


```
{
   "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

Se observa un ataque de ransomware dirigido a un único ordenador. El patrón de ataque es la actividad de un ataque dirigido mediante malware; y puede crearse un objeto de relación que utiliza el malware como patrón de ataque.

```
{
   "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 Vulnerabilidad

Se indica que la vulnerabilidad está relacionada a las vulnerabilidades y exposiciones comunes (CVE)-2017-0147 y CVE-2017-0143, que el ransomware que explota la vulnerabilidad con ejecución de código a distancia SMBv2 (parche 17.3.14, MS17-010) de Microsoft Windows. Puede crearse un objeto de relación que utiliza el malware cuyo objetivo es esta vulnerabilidad.

```
{
 "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 Campaña y agente amenazante

Se indica que se definen dos objetos como campaña y agente amenazante para la información sobre el ataque de ransomware. Se define que puede crearse la relación "atribuido a" para la campaña y el agente amenazante, la relación "utiliza" para la campaña y el patrón de ataque y la relación "destinado a" para la campaña y la vulnerabilidad.


```
{
      "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 Especificación de patrones indicadores de ciberamenazas

7.1.2.1 Indicador

Se indica que el URL del sitio de distribución del malware se define como un indicador de tipo de URL y se puede crear el objeto de relación que representa el malware.


```
{
      "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 Gestión de las actividades de respuesta

7.1.3.1 Procedimiento

Se indica que hay remedios, como "desactivación del protocolo SMB" y "parche de la vulnerabilidad del software", que pueden definirse como objetos de procedimiento (COA). Puede crearse un objeto de relación que mitiga el malware para cada objeto.


```
{
   "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 Diagrama general de las relaciones en caso de ataque

En la Figura 2 se muestran las relaciones entre todos los objetos STIX utilizados para describir un caso de uso.

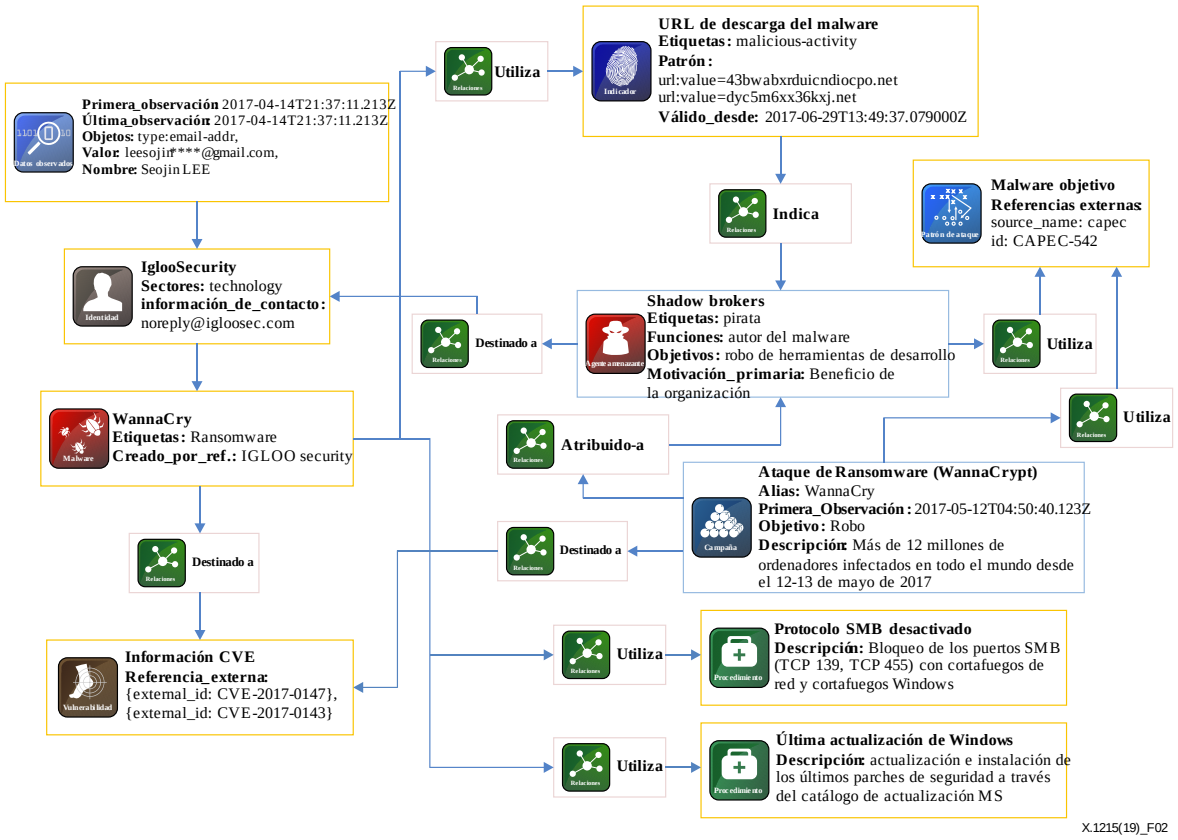

Figura 2 – Relación entre los objetos STIX utilizados para describir un caso de uso

Para resumir a continuación se describen los objetos agrupados STIX que contienen todos los objetos para detectar, analizar y responder a los ataques malignos llevados a cabo por el ransomware denominado WannaCry.

```
{
  "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 Caso de uso de ciberataque a un intercambio de criptomoneda

En esta cláusula se describe un caso de uso del ataque llevado a cabo por el denominado "Lazarus APT group", agente amenazante, el 20 de junio de 2018, contra un cambista de criptomoneda en Corea.

En este caso, el agente amenazante envió un correo electrónico suplantando la identidad de una entidad legítima (peska) con código maligno al personal del cambista de criptomoneda. Ese correo-e iba acompañado de un fichero de documento oculto en postscript maligno capaz de descargar posteriormente bibliotecas de enlaces dinámicos (DLL, *dynamic link libraries*) malignas. El fichero de documento explotaba la vulnerabilidad del procesador de texto Hangul para ejecutar el postscript y, así, instalar el fichero DLL maligno en el PC del usuario. El fichero DLL maligno tomaba el control del PC del usuario y accedía a los servidores a los que solo se podía acceder desde el interior. De este modo el atacante podía acceder a la cartera de criptomoneda del cambista y retirar una cantidad sustancial de dinero.

7.2.1 UC1: Análisis de ciberamenazas

Hay varios informes de ataques a cambistas de criptomoneda llevados a cabo entre junio y julio de 2018. En este caso se analiza el ataque de piratería llevado a cabo contra la empresa de cambio de criptomoneda denominada "BC-Company".

7.2.1.1 Identidad

La información de identificación básica del observador puede modelizarse con el objeto identidad. La organización que observa el incidente y el lugar donde ha ocurrido pueden modelizarse como objetos identidad.

Para identificar el origen del objeto informe STIX, las empresas de supervisión de seguridad, WINS e IGLOO security, se representan como objetos identidad. El objetivo del incidente se modeliza como un objeto identidad con la propiedad denominada "BC-Company.com", que es un pseudónimo.

Ese objeto se identifica en el *where_sighted_refs* del objeto avistamiento, que se abordará más adelante, y se utiliza como objetivo del ataque en patrón de ataque y malware.


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


7.2.1.2 Datos observados

Datos observados representa la información bruta generada por una máquina y es diferente de indicadores, que contienen una afirmación de inteligencia. El objeto datos observados contiene información observada en el ciberespacio, capturada de sistemas y redes, como direcciones IP, ficheros y URL. En este caso, se observa un fichero. En otra referencia, *sighting_of_ref*, se presenta el ID del SDO avistado, que en este caso es el objeto datos observados.

El cambista de criptomoneda observó un fichero entregado por correo-e. El nombre del fichero y la dirección de correo electrónico del emisor se representan mediante el objeto *ObservedData*. Los objetos datos observados que se observan en otros lugares se representan como objetos avistamiento. El emplazamiento observado se representa mediante la propiedad *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 Tácticas, técnicas y procedimientos

En esta cláusula se describe la naturaleza del comportamiento del adversario y cómo se caracteriza.

El ataque procedió de un adjunto de correo-e de peska y se utilizaron dos tipos de códigos malignos. Los ataques de peska se especifican como enumeración y clasificación de pautas de ataques comunes (CAPEC)-163 mediante el objeto patrón de ataque. El código maligno introducido por el correo-e de peska descarga la DLL maligna que explota la vulnerabilidad CVE-2015-2545. Por consiguiente, las etiquetas de los objetos malware son explotar y entregar. En el caso de las DLL malignas recibidas posteriormente, el troyano de acceso a distancia se etiqueta como código maligno que toma el control del PC del usuario.

La relación entre los dos códigos malignos se especifica con un tipo "relacionado con", que indica que hay una relación entre el documento maligno y la DLL maligna.

Para realizar la peska específica, el atacante utilizó un documento muy disimulado. Dado que el ataque tenía por objetivo un cambista de criptomoneda, se utiliza un objeto relación de tipo "dirigido a".


```
{
    "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 Vulnerabilidad

Se explota aquí la vulnerabilidad CVE-2015-2545, que oculta un postscript maligno en el procesador de texto Hangul y lo ejecuta. Se utiliza el objeto vulnerabilidad para modelizar esa vulnerabilidad. El objeto relación también indica la relación entre el código maligno y la vulnerabilidad.


```
{
    "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 Campaña y agente amenazante

Lazarus APT Group envió sus correos-e de peska específica con un código maligno integrado para robar la criptomoneda almacenada por el cambista de criptomoneda.

El objetivo de objeto agente amenazante se representa como "robar moneda criptográfica" en la propiedad "objetivos". Dado que se creó un documento maligno, la propiedad "funciones" se pone a "autor del malware" en la propiedad funciones; y como se utilizó para cometer un delito, la propiedad "etiqueta" se pone a "banda criminal".

El ataque al cambista de criptomoneda se representa con el objeto campaña y se pone la propiedad "objetivo" a "robo".

Las técnicas de ataque y los objetos código maligno utilizados en la campaña se representan mediante objetos de relación con el tipo "utiliza".


```
        {
            "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: Especificación de patrones indicadores de ciberamenazas

7.2.2.1 Indicador

El objeto indicador identifica los documentos malignos y las DLL malignas. La propiedad patrón del objeto indicador de los documentos malignos representa los URL o los valores generadores de fichero para la descarga de las DLL malignas. En este caso, los patrones DLL maligna del objeto indicador representan el URL mando y control (C2) URL y el valor generador de fichero. De este modo se puede registrar como política. Varios objetos relación con tipo "indica" señalan la relación entre dos códigos malignos.

```
{
    "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: Gestión de las actividades de respuesta en caso de ciberamenaza

7.2.3.1 Procedimiento

En este ataque, el procedimiento aplicado por el equipo de intervención se divide en detección y respuesta. En primer lugar, se ejecuta el documento maligno y luego empieza el ataque.

El valor generador del documento maligno se registra en la política de seguridad de la herramienta de análisis de malware, como puede ser YARA. El registro de datos de evento (EDR, *event data recorder*) puede detectar el ataque cuando se ejecuta el fichero con el valor generador. Además, el dispositivo de seguridad de red responde bloqueando el tráfico al URL de descarga de la DLL maligna de modo que se bloquea la descarga de la DLL maligna y no se roban los derechos de control del PC. En caso de pirateo de una DLL maligna, el dispositivo de red puede bloquear la actividad maligna bloqueando el tráfico al 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 Diagrama de relación y objeto agrupado

En la Figura 3 se muestran las relaciones entre todos los objetos utilizados para describir el caso de uso.

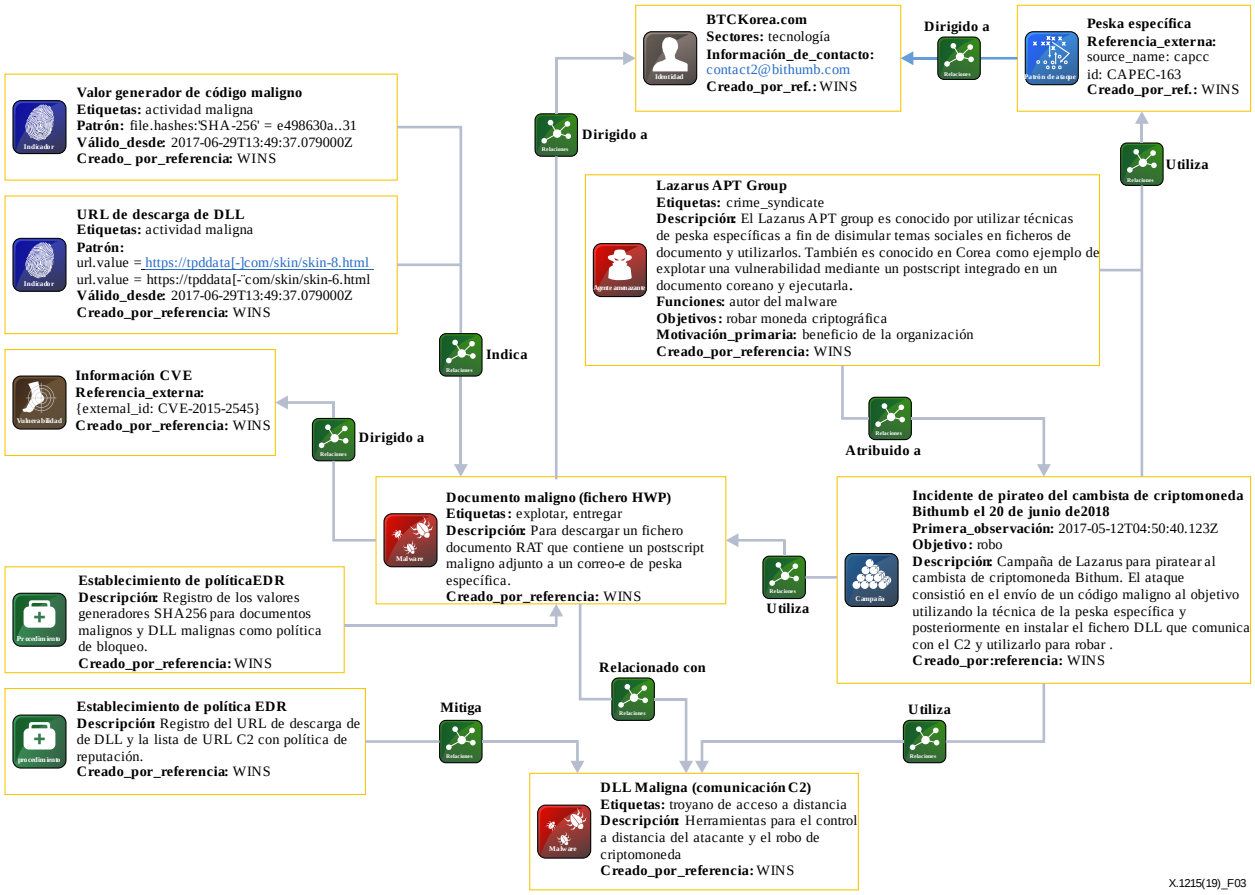

Figura 3 – Relación entre los objetos STIX utilizados para describir el caso de uso

Para resumir, a continuación, se describe el objeto agrupado STIX que contiene todos los objetos para detectar, analizar y responder a los ataques malignos llevados a cabo por Lazarus.

```
{
    "type": "bundle",
    "id": "bundle--42d953f0-0a5c-4b82-b223-b22ec85da222",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "campaign",
            "id": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.850Z",
            "modified": "2018-07-20T10:03:57.850Z",
            "name": "Hacking incident for BC-Company on June 20, 2018",
            "description": "The Lazarus APT group launched a campaign to hack the BC-Company cryptocurrency exchange. The attack method was to send the malicious code to the target through the spear phishing technique, and then installed the DLL file which was able to communicate with the C2 server and use them to steal the Bit coin.",
            "objective": "Theft"
        },
```

```
        {
            "type": "relationship",
            "id": "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692"
        },
        {
            "type": "course-of-action",
            "id": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
            "created": "2018-07-20T10:03:57.883Z",
            "modified": "2018-07-20T10:03:57.883Z",
            "name": "Establishment of EDR policy ",
            "description": "Registration of DLL downloading URL and a list of C2 URLs as
a reputation policy"
        },
        {
            "type": "relationship",
            "id": "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "related-to",
            "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "malware",
            "id": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.847Z",
            "modified": "2018-07-20T10:03:57.847Z",
            "name": "Malicious DLL (C2 communication)",
            "description": "A tool for remote control of the attacker controls to steal
the bit coin.",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
            "created": "2018-07-20T10:47:50.725Z",
```

```
            "modified": "2018-07-20T10:47:50.725Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "relationship",
            "id": "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
            "created": "2018-07-20T10:47:50.726Z",
            "modified": "2018-07-20T10:47:50.726Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
            "target_ref": "malware--dc6df47d-1a83-493f-adf6-393bb05eac40"
        },
        {
            "type": "report",
            "id": "report--91ed4b5a-5375-42cf-be5c-5fecff6d6da6",
            "created": "2018-07-20T10:03:57.897Z",
            "modified": "2018-07-20T10:03:57.897Z",
            "name": "Report on hacking incident for crypto currency exchange on
2018/06/20.",
            "published": "2018-07-20T10:03:57.897114Z",
            "object_refs": [
                "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
                "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
                "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
                "malware--dc6df47d-1a83-493f-adf6-393bb05eac40",
                "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
                "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
                "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
                "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
                "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
                "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
                "indicator--5587be4e-640a-40cd-9a07-4201cfffed7b",
                "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
                "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
                "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
                "identity--650de76c-7638-4026-8900-ec7de2fc757f",
                "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
                "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
                "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
                "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
                "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
                "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
                "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
```

```
                "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
                "relationship--b94654a3-88bc-4963-9c63-9cd4c71f17d1",
                "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
                "relationship--8d345e2f-26ea-4994-97c2-097dccba5e89",
                "relationship--c3e6cdb7-abcf-4f9a-8f10-1319fd244072",
                "relationship--8e336a27-4a9a-4a4d-8645-92e8c3524d31",
                "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21"
            ],
            "labels": [
                "threat-report"
            ]
        },
        {
            "type": "identity",
            "id": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.843Z",
            "modified": "2018-07-20T10:03:57.843Z",
            "name": "WINS",
            "identity_class": "organization",
            "sectors": [
                "technology"
            ],
            "contact_information": "sangpil@wins21.co.kr"
        },
        {
            "type": "relationship",
            "id": "relationship--de382dc8-ee33-4c5e-9bc1-29896f631e06",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "targets",
            "source_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "target_ref": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16"
        },
        {
            "type": "course-of-action",
            "id": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
            "created": "2018-07-20T10:03:57.884Z",
            "modified": "2018-07-20T10:03:57.884Z",
            "name": "EDR policy establishment”,
            "description": "Registration of DLL downloading URL and a list of C2 URLs as
a reputation policy"
        },
```

```
    {
        "type": "relationship",
        "id": "relationship--f1f37e38-e091-48d0-863b-0d80fdf7606b",
        "created": "2018-07-20T10:03:57.888Z",
        "modified": "2018-07-20T10:03:57.888Z",
        "relationship_type": "mitigates",
        "source_ref": "course-of-action--ae0a2b4f-861b-4805-b562-08ba4692b48b",
        "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
    },
    {
        "type": "relationship",
        "id": "relationship--bd273ecb-2781-42fc-891a-e339df63d602",
        "created": "2018-07-20T10:03:57.887Z",
        "modified": "2018-07-20T10:03:57.887Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
        "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
    },
    {
        "type": "vulnerability",
        "id": "vulnerability--91deaa68-9102-4b9f-95f1-ee43fa8f5a16",
        "created": "2018-07-20T10:03:57.885Z",
        "modified": "2018-07-20T10:03:57.885Z",
        "name": "CVE information",
        "external_references": [
            {
                "source_name": "cve",
                "external_id": "CVE-2015-2545"
            }
        ]
    },
    {
        "type": "relationship",
        "id": "relationship--cfe0de62-c75c-42f8-961e-12b418520a6a",
        "created": "2018-07-20T10:03:57.888Z",
        "modified": "2018-07-20T10:03:57.888Z",
        "relationship_type": "mitigates",
        "source_ref": "course-of-action--400190bf-a8be-4ee5-a605-e714194abd00",
        "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
    },
    {
        "type": "indicator",
        "id": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
        "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
```

```
            "created": "2018-07-20T10:03:57.875Z",
            "modified": "2018-07-20T10:03:57.875Z",
            "name": "C2 URL",
            "pattern": "[url:value = 'https://tpddata.com/skin/skin-6.html' OR url:value
= 'https://tpddata.com/skin/skin-8.html']",
            "valid_from": "2018-07-20T10:03:57.875238Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "attack-pattern",
            "id": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.851Z",
            "modified": "2018-07-20T10:03:57.851Z",
            "name": "Sphere Phishing",
            "external_references": [
                {
                    "source_name": "capec",
                    "external_id": "CAPEC-163"
                }
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--dd26321c-9f0a-4bd0-8efa-b8d95185d07d",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "attribute-to",
            "source_ref": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "target_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3"
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--4ea08c4d-2895-4d63-b81e-3be90bdb6e00",
            "created_by_ref": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.848Z",
            "modified": "2018-07-20T10:03:57.848Z",
            "name": "Lazarus APT Group",
            "description": "The Lazarus APT group has been known to use spear phishing
techniques to disguise social issues as document files and use them. Also, it is widely
known in Korea as an example of exploiting a vulnerability that implements postscript in
a Hangul document.",
```

```
            "roles": [
                "malware-author"
            ],
            "goals": [
                "Steal cryptographic currency"
            ],
            "primary_motivation": "organizational-gain",
            "labels": [
                "crime-syndicate"
            ]
        },
        {
            "type": "identity",
            "id": "identity--650de76c-7638-4026-8900-ec7de2fc757f",
            "created": "2018-07-20T10:03:57.886Z",
            "modified": "2018-07-20T10:03:57.886Z",
            "name": "BC-Company.com",
            "identity_class": "organization"
        },
        {
            "type": "malware",
            "id": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.845Z",
            "modified": "2018-07-20T10:03:57.845Z",
            "name": "Malicious document(HWPfile)",
            "description": "A purpose for downloading the RAT in the document file that
contains the postscript in the attachment of the spear fishing e-mail ",
            "labels": [
                "exploit",
                "dropper"
            ]
        },
        {
            "type": "identity",
            "id": "identity--471f30f8-a2b5-4478-80ee-94af783486fe",
            "created": "2018-07-20T10:03:57.844Z",
            "modified": "2018-07-20T10:03:57.844Z",
            "name": "IGLOO Security",
            "identity_class": "organization",
            "sectors": [
                "technology"
            ],
            "contact_information": "noreply@igloosec.co.kr"
        },
```

```
        {
            "type": "relationship",
            "id": "relationship--d43720f8-a45f-4fc9-be69-191fee09249b",
            "created": "2018-07-20T10:03:57.888Z",
            "modified": "2018-07-20T10:03:57.888Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--d882ce3b-c1d1-496a-8ecd-d923f4e6f692",
            "target_ref": "identity--650de76c-7638-4026-8900-ec7de2fc757f"
        },
        {
            "type": "observed-data",
            "id": "observed-data--45eeee3b-a455-404e-8612-613168eeb693",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
"first_observed": "2018-07-20T10:03:57.887095Z",
            "last_observed": "2018-07-20T10:03:57.887101Z",
            "number_observed": 1,
            "objects": {
                "0": {
                    "type": "email-addr",
                    "value": "****@hanmail.net"
                },
                "1": {
                    "type": "file",
                    "name": " ICT staff profile.hwp"
                }
            }
        },
        {
            "type": "sighting",
            "id": "sighting--99f5d054-ac33-4970-abd9-6ddfd75b4d21",
            "created": "2018-07-20T10:03:57.896Z",
            "modified": "2018-07-20T10:03:57.896Z",
            "count": 1,
            "sighting_of_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2",
            "observed_data_refs": [
                "observed-data--45eeee3b-a455-404e-8612-613168eeb693"
            ],
            "where_sighted_refs": [
                "identity--650de76c-7638-4026-8900-ec7de2fc757f"
            ]
        },
```

```
        {
            "type": "relationship",
            "id": "relationship--c591ea62-ef8a-42c9-85f2-081f4bcb2681",
            "created": "2018-07-20T10:03:57.889Z",
            "modified": "2018-07-20T10:03:57.889Z",
            "relationship_type": "uses",
            "source_ref": "campaign--ee7d0bb2-0610-48b2-b5b4-5cd3d17605d3",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "relationship",
            "id": "relationship--6d62221c-26ab-413c-b41e-1c526b3cf82c",
            "created": "2018-07-20T10:03:57.887Z",
            "modified": "2018-07-20T10:03:57.887Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--37e121c1-7cd7-4830-a062-20687decefa7",
            "target_ref": "malware--d3ce73ac-b65d-429d-b669-cd3137c437d2"
        },
        {
            "type": "indicator",
            "id": "indicator--13f1be15-9457-4b27-85e9-14886e7f442f",
            "created_by_ref": "identity--c3657c2a-6cd4-4815-8dc4-60a50cf32c62",
            "created": "2018-07-20T10:03:57.853Z",
            "modified": "2018-07-20T10:03:57.853Z",
            "name": "Hash value of malicious document",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'e498630abe9a91485ba42698a35c2a0d8e13fe5cccde65479bf3033c45e7d431']",
            "valid_from": "2018-07-20T10:03:57.853427Z",
            "labels": [
                "malicious-activity"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--1d774b78-3ac1-4b3d-ac45-a18d698b2d55",
            "created_by_ref": "identity--0b4f8e07-e259-4110-8510-341604590fb5",
                   "created": "2018-07-20T10:47:50.715Z",
            "modified": "2018-07-20T10:47:50.715Z",
            "name": "Hash value of malicious DLL",
            "pattern":                    "[file:hashes.'SHA-256'                    =
'5b1663d5eb565caccca188b6ff8a36291da32f368211e6437db2dc2e9cd']",
            "valid_from": "2018-07-20T10:47:50.71577Z",
            "labels": [
                "malicious-activity"
            ]
        },
```

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

Anexo A

Caso de uso de ransomware con STIX 1.0

(Este anexo forma parte integrante de la presente Recomendación.)

En este anexo se expone un caso de uso de ransomware para ilustrar cómo puede utilizarse el lenguaje STIX 1.0 para la gestión de ciberamenazas contra el ransomware WannaCry.

A.1 Análisis de ciberamenazas

En esta cláusula se presenta la información analizada del ransomware (WannaCrypt), obtenida de ataques de código maligno llevados a cabo en todo el mundo utilizando un ransomware de vulnerabilidad de ejecución de código a distancia SMBv2.

A.1.1 Datos observables

Se observa la recepción de una notificación de envío por correo-e con un archivo de ficheros EGG y 52 dominios de servidor 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

Se indica la observación de un ataque de ransomware dirigido a un ordenador individual. El patrón de ataque es la actividad del ataque dirigido mediante malware y el objetivo del ataque son las propiedades información de la organización.

```
<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 Objetivo explotado

Se indica que la vulnerabilidad explotada por el ransomware es la vulnerabilidad de ejecución de código a distancia SMBv2 (CVE-2017-0147, CVE-2017-0143) y el sistema operativo Windows 10 de 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 Incidente

Se indica que la clasificación es acceso no autorizado, los activos son las propiedades información de una organización y los objetos afectados, así como las respuestas al incidente, son robo.

```
<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 Agente amenazante

Se indica que el tipo de atacante es un creador de malware, el motivo es financiero o económico, la calificación es experto y la intención del intruso es el robo.

```
<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 Campaña

Se indica que el incidente relacionado, los TTP y el agente amenazante se han descrito para definir la intención del agente amenazante.

```
<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 Especificación de los patrones indicadores de ciberamenazas

A.2.1 Indicador

Se indica que se definen los indicadores correo-e maligno, exfiltración y URL a los que están vinculados los correspondientes datos observables, TTP y campaña.

```
<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 Gestión de las actividades de respuesta

A.3.1 Procedimiento

Se señala que puede lograrse un remedio con un parche de vulnerabilidad de software, el límite de conexión no tiene consecuencias, el coste de la respuesta es bajo y la eficacia de la respuesta es media.

```
<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>
```

Bibliografía

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

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

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

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

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

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

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

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

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

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

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019