Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1546

(01/2014)

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

Intercambio de información de ciberseguridad – Intercambio de eventos/incidentes/heurística

Enumeración y caracterización de atributos de malware

Recomendación UIT-T X.1546

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	
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	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
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.1546

Enumeración y caracterización de atributos de malware

Resumen

El lenguaje de enumeración y caracterización de atributos de malware (software maligno) (MAEC) comprende enumeraciones de los atributos y comportamientos del malware con los que se forma un vocabulario común. Estas enumeraciones se sitúan a diversos niveles de abstracción: características observables de bajo nivel, comportamientos de nivel medio y taxonomías de alto nivel. La Recomendación UIT-T X.1546, primera versión del MAEC, se centra en la creación de la enumeración de atributos de malware de bajo nivel basándose en los escasos trabajos sobre el tema ya existentes. Así, en un primer momento podrá caracterizar los tipos más comunes de malware, incluidos los troyanos, gusanos y rootkits, pero en último término podrá aplicarse a tipos más sofisticados de malware.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1546	2014-01-24	17	11.1002/1000/12038

* 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 no 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

Introducción

La Recomendación UIT-T X.1546 sobre la utilización de la enumeración y caracterización de los atributos de malware (software maligno) (MAEC) es una norma comunitaria internacional sobre seguridad de la información destinada a fomentar la disponibilidad pública y abierta de contenidos de seguridad sobre el malware y su comportamiento. Esta Recomendación también quiere normalizar la transferencia de esta información por todo el espectro de herramientas y servicios de seguridad que pueden emplearse para supervisor y gestionar las defensas contra el malware. MAEC es un lenguaje utilizado para codificar los detalles del malware.

Con el lenguaje MAEC se quiere: 1) mejorar la comunicación persona-persona, persona-máquina, máquina-máquina y máquina-persona sobre malware, 2) reducir la posibilidad de que los investigadores dupliquen los análisis de malware, y 3) permitir una más rápida creación de contramedidas aprovechando las respuestas observadas en malware anteriores. El análisis de amenazas, la detección de intrusiones y la gestión de incidentes son procesos que se realizan para luchar contra todo tipo de ciberamenazas. Gracias a la codificación uniforme de los atributos de malware, MAEC ofrece un formato normalizado para la incorporación en esos procesos de información útil sobre el malware.

El software maligno, también llamado "malware", ha existido siempre, bajo una u otra forma, desde la aparición del primer virus de PC en 1971. En la actualidad es responsable de toda una gama de actividades malignas, que van desde la casi totalidad de la distribución de correos electrónicos basura (spam) por redes robot al robo de información sensible mediante ataques de ingeniería social concretos. Al ser efectivamente un agente autónomo que opera en nombre del atacante, el malware tiene la capacidad de realizar cualquier acción que pueda expresarse en código, por lo que representa una increíble amenaza para la ciberseguridad.

Por consiguiente, en la actualidad la protección de los sistemas informáticos contra el malware es una de las mayores preocupaciones de seguridad de la información tanto para organizaciones como para particulares, pues una única instancia de malware no detectado puede dañar los sistemas y poner en peligro los datos. La desconexión de las redes informáticas no anula por complete el riesgo de infección, como demuestran los malware que utilizan las tomas USB como vector de inserción. Por todo ello, hasta la fecha la mayor parte de los esfuerzos para luchar contra el malware se han concentrado en evitar los daños mediante una pronta detección.

Existen varios métodos comunes para detectar el malware, que se basan principalmente en la firma física y la heurística. Estos métodos son eficaces por su estrecho alcance, aunque cada uno de ellos tiene sus inconvenientes, como el hecho de que las firmas no sirven para tratar con malware del día cero, dirigido, polimórfico y demás nuevos tipos de malware. Del mismo modo, la detección heurística puede detector genéricamente ciertos tipos de malware y no otros, para los que no dispone de patrones, como los *rootkit* a nivel del núcleo. Así, parece más prudente decir que estos métodos, aunque útiles, aún no son totalmente fiables para tratar con los malware actuales.

La enumeración y caracterización de atributos de malware (MAEC) pretende eliminar las ambigüedades e inexactitudes de que sufren actualmente las descripciones de malware y reducir la dependencia de las firmas. De este modo, MAEC pretende mejorar la comunicación persona-persona, persona-máquina, máquina-máquina y máquina-persona sobre malware; reducir la posibilidad de que los investigadores dupliquen los análisis de malware; y permitir una más rápida creación de contramedidas aprovechando las respuestas observadas en malware anteriores. Como se verá más adelante, el lenguaje MAEC permite efectuar la correlación, la integración y la automatización destinadas a la compartición de información estructurada sobre malware basada en atributos tales que el comportamiento, las deformaciones y los patrones de ataque.

Como se ve en la Figura 1, MAEC se compone de un modelo de datos con diversos esquemas interconectados, representando así la gramática que define el lenguaje. Estos esquemas permiten

generar diversos resultados MAEC, que pueden considerarse usos específicos de la gramática mencionada.

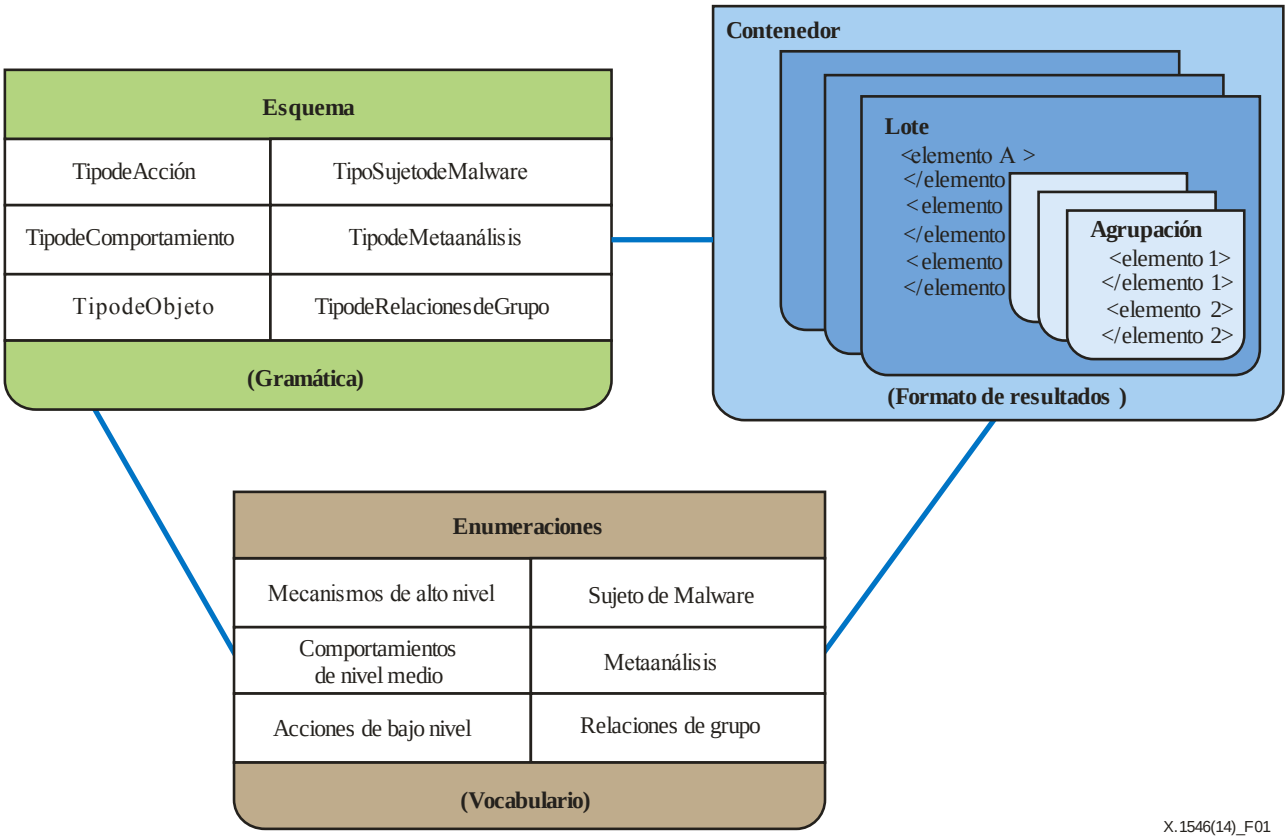

Figura 1 – Visión general del MAEC

El contenedor MAEC, el lote MAEC y la agrupación MAEC están previstos para utilizarse en situaciones diferentes, por lo que contienen tipos distintos de información sobre malware.

El lenguaje MAEC está relacionado tanto con el lenguaje de expresión ciberobservable (CybOX) como con el formato de intercambio de metadatos de malware (MMDEF) del ICSG del IEEE.

CybOX es un lenguaje normalizado para la especificación, captura, caracterización y comunicación de eventos o propiedades con estados observables en el dominio operativo. La ciberobservabilidad se aplica a numerosos dominios: evaluación y caracterización de amenazas (patrones de ataque detallados), caracterización de malware, gestión operativa de eventos, registro cronológico, conocimiento de la cibersituación, respuesta a incidentes, análisis forense digital y compartición de información sobre ciberamenazas, entre otros.

Prácticamente todos los campos de CybOX son optativos, por lo que se pueden utilizar los que se necesitan e ignorar los demás. CybOX puede utilizarse para especificar y caracterizar una amplia gama de ciberobjetos y puede emplearse para definir las composiciones relacionales y lógicas de múltiples objetos, acciones, eventos y/u observables.

La caracterización del malware con MAEC se basa en un mecanismo común (estructura y contenido) que CybOX utiliza para los ciberobservables en todos los usos posibles de MAEC y entre ellos. Mientras MAEC ofrece un contexto de análisis, indicadores, comportamientos y mecanismos, CybOX facilita los objetos y acciones generales utilizados en el ciberdominio operativo. Un ciberobservable es un *evento mensurable* o una *propiedad con estados* en el ciberdominio operativo. Como ejemplos de eventos mensurables pueden citarse la creación de claves de registros, la supresión de ficheros y la recepción de una petición HTTP GET request. Las propiedades con estados son, por

ejemplo, el troceo MD5 de un fichero, el valor de una clave de registro o la existencia de una exclusión mutua.

MAEC importa y amplía los objetos y acciones CybOX. En la Figura 2 se presenta un esquema extremadamente simplificado de CybOX. En verde se señalan los componentes CybOX que utiliza MAEC.

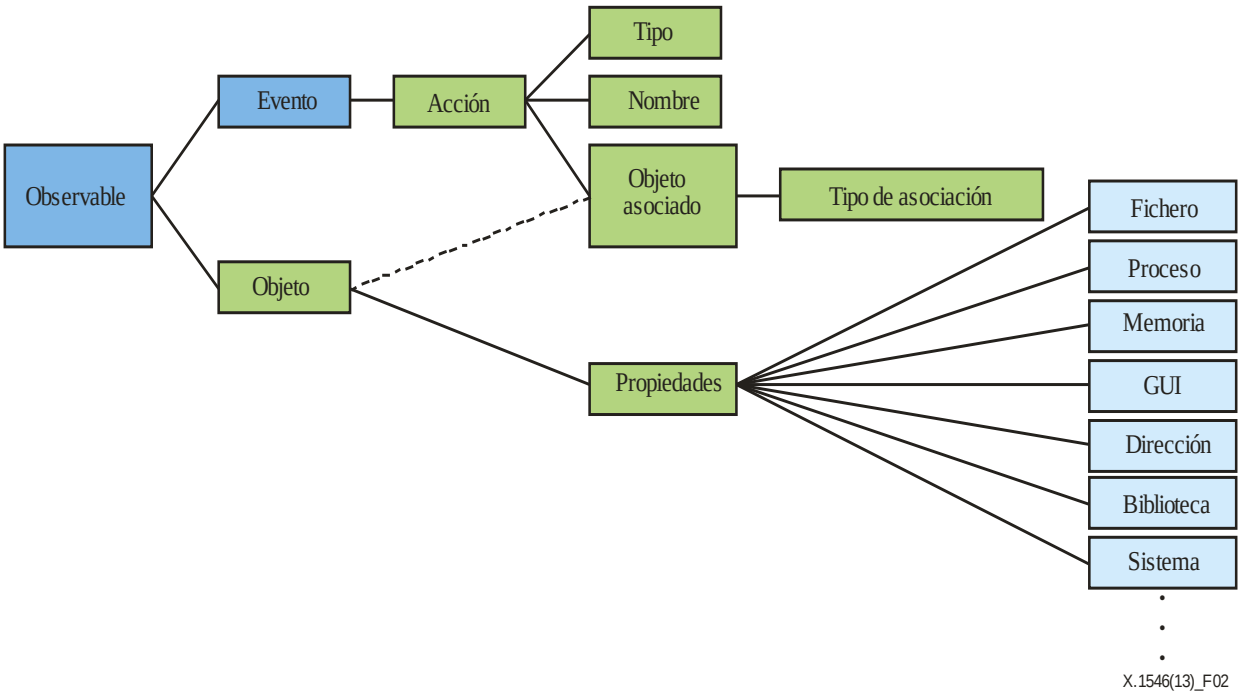

Figura 2 – Esquema simplificado del lenguaje de expresión ciberobservable (CybOX)

El concepto propiedades CybOX es un contenedor abstracto para diversos tipos de Objeto predefinidos (por ejemplo, fichero, proceso, memoria) que pueden ocuparlo. Las propiedades, señaladas en azul claro, son independientes del esquema CybOX núcleo.

El *Industry Connections Security Group* (ICSG) del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) está elaborando el MMDEF. El esquema original fue creado principalmente por un grupo de fabricantes de antivirus (AV) a fin de disponer de un medio para ampliar las muestras de malware compartidas con metadatos adicionales. Así, se pueden caracterizar algunas características estáticas, como el troceo y los nombres de ficheros, además de algunos comportamientos muy básicos.

La comunidad de la seguridad de la información contribuye al desarrollo del MAEC participando en la creación del lenguaje MAEC en las listas de debate de creadores del MAEC y en el portal de colaboración e integrando el lenguaje MAEC en sus herramientas y capacidades de depósito. La comunidad MAEC está formada por representantes de un amplio espectro de entidades de la industria, instituciones académicas y organizaciones gubernamentales de todo el mundo, que supervisan y colaboran en la creación del lenguaje MAEC y en las herramientas y servicios MAEC a través del depósito MAEC, que está disponible al público. Por tanto, MAEC refleja las opiniones y conocimientos del mayor número posible de analistas de malware y profesionales de la prevención de todo el mundo.

Esta Recomendación se ha preparado en colaboración con *The MITRE Corporation* tomando en consideración la importancia de conservar, en la medida de lo posible, la compatibilidad técnica entre esta Recomendación y los *Requirements and Recommendation for MAEC Compatibility*, versión 1.1, de 7 de julio de 2013.
[https://maec.mitre.org/compatible/Requirements_for_MAEC_Compatibility_V1.1.pdf].

Recomendación UIT-T X.1546

Enumeración y caracterización de atributos de malware

1 Alcance

Esta Recomendación ofrece un medio estructurado para fomentar la disponibilidad pública y abierta de contenidos de seguridad sobre el malware y su comportamiento, y para normalizar la transferencia de esta información por todo el espectro de herramientas y servicios de seguridad que pueden emplearse para supervisar y gestionar las defensas contra el malware.

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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[ISO/IEC 19757-3] ISO/IEC 19757-3:2006, *Information technology – Document Schema Definition Languages (DSDL) – Part 3: Rule-based validation – Schematron*.

[W3C XML Schema] W3C XML Schema Part 2 (2004), *W3C XML Schema Part 2: Datatypes*, Second Edition. <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 propietario [b-UIT-T X.1520]: Custodio (persona física o moral) responsable de la capacidad.

3.1.2 usuario [b-UIT-T X.1520]: Consumidor o potencial consumidor de la capacidad.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 capacidad: Función o funciones específicas de un producto, servicio o depósito.

3.2.2 resultados de prueba de capacidad: Datos que representan el resultado de la prueba de corrección.

3.2.3 contenido: Cualquier tipo de entidad de enumeración y caracterización de atributos de malware (MAEC), incluidos los documentos de formato de resultados MAEC, así como los elementos/tipos incorporados.

3.2.4 prueba de corrección: Proceso que determina si una herramienta ha aplicado correctamente el MAEC.

3.2.5 agrupación MAEC: forma normalizada de resultado MAEC donde se recogen todas las características derivadas del análisis de una sola instancia de malware, incluidos los comportamientos o acciones MAEC observados y cualquier objeto MAEC relacionado.

3.2.6 contenedor MAEC: forma normalizada de resultado MAEC donde se reúnen uno o más lotes MAEC.

3.2.7 formato de resultados MAEC: cualquiera de las tres formas normalizadas de resultados MAEC: contenedor, lote o agrupación MAEC.

3.2.8 lote MAEC: forma normalizada de resultado MAEC donde se caracterizan todos los datos conocidos de uno o más malware, incluidas las características derivadas del análisis (a través de las agrupaciones MAEC) y los análisis conexos u otros metadatos.

3.2.9 instancia de malware: copia específica de malware.

3.2.10 elemento de malware: comportamiento, atributo, logro, cabida útil, etc., relacionado con una instancia de malware, una familia de malware o una clase de instancias de malware.

3.2.11 patrón de malware: abstracción de algunos atributos comunes a una serie de instancias de malware (familias o clases). Un único patrón de malware puede asociarse a muchas instancias de malware diversas.

3.2.12 sujeto de malware: entidad MAEC que captura todos los detalles de una única instancia de malware, incluidos los metadatos de análisis, el contenido de análisis y la información de relación correspondientes.

3.2.13 producto: cualquier herramienta, servicio o depósito antimalware que tiene una o más capacidades.

3.2.14 depósito: recopilación implícita o explícita de elementos o patrones de malware que sirve de base a las herramientas o servicios de creación de contenido, por ejemplo, una base de datos de patrones de comportamiento, una serie de instancias de malware analizadas por una herramienta de compartimento estanco, o el resultado global de una herramienta de análisis binario estático o dinámico. Un depósito también puede ser una recopilación de formatos de resultados MAEC documentales.

3.2.15 examen: proceso mediante el cual se determina si una capacidad es compatible con MAEC.

3.2.16 autoridad de examen: entidad que realiza las pruebas de corrección y está autorizada para reconocer formalmente que una capacidad es compatible con MAEC.

3.2.17 muestra de examen: copia del resultado de la capacidad que se entrega a la autoridad de examen para que la utilice a fin de determinar si la capacidad es compatible con MAEC.

3.2.18 versión de examen: versión fechada de MAEC que se utiliza para determinar la compatibilidad MAEC de una capacidad.

3.2.19 servicio: actividades de análisis de malware, detección de malware o remedio contra el malware que realizan una o más capacidades.

3.2.20 herramienta: programa informático o dispositivo que tiene una o más funcionalidades. Una herramienta analiza el malware, lo detecta o le pone remedio utilizando diversos métodos, por ejemplo, herramienta de análisis estático, herramienta de análisis dinámico, escáner de firmas, escáner heurístico, etc. Una herramienta también puede realizar la autoría del contenido.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AV Antivirus

CybOX Expresión ciberobservable (*cyber-observable expression)*

ID Identificador

MAEC Enumeración y caracterización de atributos de malware (*malware attribute enumeration and characterization*)

MMDEF Formato de intercambio de metadatos de malware (*malware metadata exchange format)*

SIM Gestión de información de seguridad (*security information management)*

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

5 Convenios

En esta Recomendación MAEC se emplea como sustantivo.

6 Requisitos de alto nivel

En los siguientes párrafos se definen los conceptos, funciones y responsabilidades en relación con las cinco capacidades diferentes, cada una de las cuales apunta a una utilización diferente del lenguaje MAEC, que comprende la utilización adecuada de dicho lenguaje. Estas capacidades permiten a los miembros de la comunidad MAEC comprender fácilmente cómo utiliza un producto dado el lenguaje MAEC y cómo éste podría ajustarse a sus necesidades.

Los siguientes requisitos se aplican a todas las capacidades que soportan MAEC, independientemente de la funcionalidad específica que ejerzan (los requisitos específicos de las funcionalidades se presentan en la cláusula 10, Requisitos de compatibilidad específicos). Si una capacidad cumple con todos los requisitos aplicables, la autoridad de examen reconocerá oficialmente al propietario de la capacidad la compatibilidad MAEC.

Requisitos previos

6.1 El propietario de la capacidad será una entidad jurídica válida, es decir una organización o un particular concreto, con un número de teléfono, una dirección de correo electrónico y una dirección postal válidos.

6.2 El propietario de la capacidad acordará observar todos los requisitos de compatibilidad MAEC obligatorios, entre los cuales figuran los requisitos obligatorios para una funcionalidad específica.

6.3 El propietario de la capacidad proporcionará a la autoridad de examen los datos de un punto de contacto técnico calificado para responder preguntas sobre cualquier funcionalidad de la capacidad relacionada con MAEC, y coordinará la preparación de la capacidad para la prueba de corrección.

6.4 El propietario de la capacidad rellenará el formulario "Cuestionario de compatibilidad MAEC" y lo transmitirá a la autoridad de examen. Este formulario se devolverá al propietario de la capacidad una vez que la autoridad de examen haya procesado el formulario "Declaración de compatibilidad MAEC".

6.5 El propietario de la capacidad colaborará con la autoridad de examen con el fin de que el producto, servicio o depósito esté disponible para la prueba de corrección.

6.6 El propietario de la capacidad proporcionará a la autoridad de examen libre acceso a los elementos necesarios para efectuar la prueba de corrección, con inclusión de los resultados de las pruebas y/o las muestras de examen, con miras a determinar el cumplimiento con todos los requisitos de compatibilidad conexos.

6.7 Como parte de la recepción del reconocimiento oficial de la compatibilidad MAEC, el propietario de la capacidad convendrá en respaldar a la autoridad de examen en la realización de las actividades de prueba, e intercambiará los tipos de ficheros adecuados con otras organizaciones intentando demostrar la corrección de su capacidad. Esto se realizará bajo la gestión de la autoridad de examen y los esfuerzos de todos los involucrados se mantendrán a un nivel razonable.

6.8 La capacidad estará disponible para el público o un conjunto de consumidores.

6.9 La capacidad indicará claramente la o las versiones de MAEC y el o los esquemas conexos con que es compatible.

Varios

Estos requisitos se aplican a aspectos varios de la compatibilidad MAEC.

6.10 Si la capacidad no satisface todos los requisitos aplicables indicados (cláusulas 6.1 a 6.9), el propietario de la capacidad no anunciará que su capacidad es compatible con MAEC.

6.11 Si la capacidad no satisface todos los requisitos específicos aplicables a su funcionalidad (definidos en las cláusulas 10.1 a 10.27), el propietario de la capacidad no anunciará que su capacidad es compatible con MAEC.

6.12 El propietario de la capacidad deberá recibir la aprobación formal de la autoridad de examen antes de anunciar que su capacidad es compatible con MAEC.

7 Corrección

Estos requisitos se aplican a los errores de corrección relacionados con la compatibilidad MAEC, incluidos, entre otros, los errores relativos a la validación del esquema y a la utilización no válida de estructuras y elementos MAEC concretos.

7.1 El propietario de la capacidad debe disponer de un medio para hacer que el usuario presente los errores de corrección encontrados en el uso de MAEC y en cualquier contenido MAEC producido por la capacidad.

7.2 El propietario de la capacidad debe haber establecido un plan para corregir cualquier error de corrección que se le comunique.

7.3 El propietario de la capacidad debe corregir dentro de un período de tiempo razonable cualquier error de corrección que se le comunique.

8 Documentación

La documentación que se proporciona con una capacidad compatible con MAEC ha de cumplir los siguientes requisitos.

8.1 El producto contendrá en su documentación una breve descripción de MAEC y de la compatibilidad MAEC, que puede estar basada en extractos literales de documentos del sitio web de MAEC.

8.2 En la documentación de la capacidad deberá indicarse claramente la cobertura de MAEC y sus esquemas asociados, incluidos los importados de los trabajos realizados con la expresión ciberobservable (CybOX) y el formato de intercambio de metadatos de malware (MMDEF), ya sea indicando los elementos u objetos CybOX individuales que no se soportan o los elementos y objetos CybOX que sí se soportan. Por ejemplo, si una capacidad solicita el reconocimiento formal de la compatibilidad MAEC como herramienta o servicio de creación de contenido de análisis dinámico y no soporta el objeto fichero CybOX y/o las acciones asociadas con el objeto fichero CybOX, en la documentación de la capacidad se indicará explícitamente tal incompatibilidad.

8.3 En la documentación de la capacidad se debe indicar claramente el procedimiento que debe aplicar el usuario para presentar los errores de corrección encontrados en un contenido MAEC elaborado por el producto.

8.4 Si la documentación incluida con la capacidad incluye un índice, éste debe contener referencias a documentación relacionada con MAEC bajo el término "MAEC".

9 Validez

Los siguientes requisitos se derivan de la necesidad de que las capacidades compatibles con MAEC trabajen con documentos válidos. Esto ayuda a garantizar que la información se formatea correctamente y que la estructura del documento se ajusta al lenguaje MAEC.

9.1 La capacidad validará todo el contenido OVAL (tanto el producido como el consumido) utilizando la validación de W3C XML schema (véase [W3C XML Schema]), tomando como base la versión del lenguaje MAEC que debe cumplir.

9.2 La capacidad comunicará al usuario cualesquiera errores de validación de W3C XML schema.

9.3 La capacidad validará todo el contenido OVAL (tanto el producido como el consumido) utilizando la validación Schematron (véase [ISO/IEC 19757-3]), tomando como base la versión del lenguaje MAEC que debe cumplir.

9.4 La capacidad comunicará al usuario cualesquiera errores de validación Schematron.

10 Requisitos de capacidad específicos

Los siguientes requisitos se aplican únicamente a las capacidades cuyos propietarios solicitan la compatibilidad MAEC con respecto a la funcionalidad en cuestión. Una capacidad compatible con MAEC facilitará al menos una funcionalidad específica: creación de contenido, almacenaje de contenido o consumo de contenido.

Creación de contenido	Herramienta o servicio que crea o participa en el proceso de creación de nuevos ficheros MAEC, incluidos los que reúnen en un único fichero los documentos de formato de resultados MAEC existentes. Se definen los siguientes subtipos de la funcionalidad creación de contenido: • Creación de contenido de análisis estático: Herramienta o servicio que realiza un análisis estático de una o más instancias de malware y presenta los resultados en un documento de formato de resultados MAEC. • Creación de contenido de análisis dinámico: herramienta o servicio que realiza un análisis dinámico (es decir, una ejecución dirigida) de una instancia de malware y presenta los resultados en un documento de formato de resultados MAEC. • Creación de contenido de autoría: herramienta o servicio que soporta la creación y edición manuales de documentos de formato de resultados MAEC.
Almacenaje de contenido	Depósito de contenido MAEC que se pone a disposición de la comunidad (gratuitamente).
Consumo de contenido	Herramienta o servicio que acepta los documentos de formato de resultados MAEC como insumo y muestra su contenido al usuario o lo utiliza para realizar algún tipo de acción (remedio, gestión de información de seguridad (SIM), etc.).

Creación de contenido general

Estos requisitos se aplican a todas las herramientas y servicios que pretenden ofrecer resultados de contenido MAEC.

10.1 Una herramienta o servicio que ofrezca contenido MAEC generará al menos un tipo de formato de resultados MAEC (agrupación, lote o contenedor MAEC.

10.2 Todas las herramientas o servicios que pretendan ofrecer resultados para una única instancia de malware y no captar información sobre sus propios atributos generarán una única agrupación para dicha instancia de malware.

10.3 Una herramienta o servicio que pretende ofrecer resultados para una única instancia de malware y/o captar información sobre sus propios atributos debe generar uno o más lotes MAEC con uno o más sujetos de malware MAEC incorporados por cada una de las instancias de malware que analiza. Sin no genera lotes MAEC, deberá generar contenedores MAEC que contengan los lotes MAEC incorporados.

10.4 Una herramienta o servicio que pretende ofrecer resultados para más de una serie o grupo de instancias de malware debe generar uno o más contenedores MAEC con uno o más lotes MAEC incorporados por cada serie o grupo de instancias de malware que analiza.

10.5 Una herramienta o servicio que pretende captar información sobre sus propios atributos documentará, como mínimo, su nombre, versión y fabricante utilizando las entidades correspondientes en el sujeto de malware MAEC y, por consiguiente, generará lotes MAEC o contenedores con lotes MAEC incorporados.

10.6 Una herramienta o servicio que genera lotes MAEC ha de ser capaz de generar agrupaciones MAEC independientes.

10.7 Una herramienta o servicio que genera contenedores MAEC ha de ser capaz de generar lotes MAEC independientes.

10.8 Una herramienta o servicio debe utilizar en todo el contenido MAEC que genere su parte de espacio nombre constante exclusivo del identificador (ID).

Creación de contenido de análisis estático

Estos requisitos se aplican a todas las herramientas y servicios de análisis estático que pretenden crear contenido MAEC.

10.9 Al generar un fichero de formato de resultados MAEC, una herramienta o servicio de análisis estático hade comunicar sus conclusiones utilizando las entidades MAEC más adecuadas (incluidas, entre otras, las acciones, objetos y comportamientos MAEC y/o clasificaciones AV), así como el formato de resultados MAEC más oportuno.

Creación de contenido de análisis dinámico

Estos requisitos se aplican a todas las herramientas y servicios de análisis dinámico que pretenden crear contenido MAEC.

10.10 Al generar un fichero de formato de resultados MAEC, una herramienta o servicio de análisis dinámico ha de comunicar sus conclusiones utilizando las entidades MAEC más adecuadas (incluidas, entre otras, las acciones y comportamientos MAEC), así como el formato de resultados MAEC más oportuno.

Creación de contenido de autoría

Estos requisitos se aplican a todas las herramientas y servicios que pretenden crear contenido MAEC o facilitar la creación o modificación de contenido MAEC.

10.11 Una herramienta o servicio de autoría debe fomentar la reutilización de sujetos, comportamientos, acciones, objetos y posibles indicadores de malware existentes.

10.12 Una herramienta o servicio de autoría debe permitir que el usuario invoque la validación de un documento escrito en lenguaje MAEC y comunicar al usuario todos los errores W3C XML Schema y Schematron.

10.13 Una herramienta o servicio de autoría permitirá al usuario importar y editar contenido MAEC existente (lo que comprende todos los formatos de resultados MAEC).

10.14 Una herramienta o servicio de autoría permitirá al usuario exportar el contenido creado como documentos de formato de resultados MAEC válidos.

10.15 Una herramienta o servicio de autoría debe evitar duplicar el contenido para el usuario.

10.16 Una herramienta o servicio de autoría ofrecerá valores y capacidades superiores a la capacidad de un editor de lenguaje de marcación extensible (XML), según determine la autoridad de examen.

Almacenaje de contenido

Estos requisitos se aplican a todos los depósitos que pretenden ofrecer una recopilación de contenido MAEC.

10.17 Cada contenedor, lote, sujeto de malware, análisis, agrupación, acción, objeto, comportamiento, posible indicador, recopilación de comportamientos, recopilación de acciones, recopilación de objetos y recopilación de posibles indicadores MAEC tendrá un ID exclusivo que lo diferencie de todos los demás contenedores, lotes, sujetos de malware, análisis, agrupaciones, acciones, objetos, comportamientos, posibles indicadores, recopilaciones de comportamientos, recopilaciones de acciones, recopilaciones de objetos y recopilaciones de posibles indicadores MAEC recogidos en el depósito.

10.18 Cada acción y objeto MAEC debe tener un ID; ese ID será exclusivo y diferente de los ID de todas las demás acciones y objetos recogidos en el depósito.

10.19 La porción espacio nombre del ID será constante para todo el contenido MAEC y exclusiva del depósito.

10.20 Todos los contenedores, lotes, sujetos de malware, análisis, agrupaciones, acciones, objetos, comportamientos, posibles indicadores, recopilaciones de comportamientos, recopilaciones de acciones, recopilaciones de objetos y recopilaciones de posibles indicadores MAEC tendrán el mismo ID durante toda su existencia. No se podrá reescribir un elemento existente con otros fines, pues es posible que los usuarios lo utilicen como referencia en su propio contenido.

10.21 El propietario del depósito documentará el proceso mediante el cual un usuario puede extraer actualizaciones de contenido.

Consumo de contenido

Estos requisitos se aplican a todas las herramientas y servicios que pretenden consumir contenido MAEC. Téngase en cuenta la distinción entre "consumir" (procesar información de manera inteligente) y "analizar" (extraer contenido concreto de un documento más largo).

10.22 Una herramienta o servicio que consume contenido MAEC consumirá al menos un tipo de formato de resultados MAEC (agrupación, lote o contenedor).

10.23 Una herramienta o servicio que consume contenido MAEC soportará el análisis sintáctico de cada tipo de formato de resultados MAEC para extraer los tipos incorporados que consume, independientemente de la ubicación de esos tipos en el documento de formato de resultados. Por ejemplo, una herramienta o servicio que consume sólo agrupaciones debe poder asimismo analizar lotes y contenedores para extraer el contenido de la agrupación.

10.24 Si una herramienta o servicio sólo necesita información de análisis técnico asociada con una instancia de malware, consumirá agrupaciones MAEC.

10.25 Si una herramienta o servicio necesita información de análisis técnico asociada con una instancia de malware además de metadatos de análisis e información de relación, consumirá lotes MAEC.

10.26 Si una herramienta o servicio necesita información de análisis asociada con múltiples series o grupos de instancias de malware, consumirá contenedores MAEC.

10.27 Si la herramienta o servicio no consume los ficheros de formato de resultados MAEC durante el tiempo de ejecución, el propietario de la capacidad documentará el proceso mediante el cual un usuario puede presentarle ficheros de formato de resultados MAEC para su interpretación por la herramienta o servicio. En la documentación se indicará claramente en qué plazo de tiempo se ponen a disposición de la herramienta o servicio los ficheros presentados al propietario de la capacidad.

11 Requisitos de la autoridad de examen

Los siguientes requisitos pertenecen al a compatibilidad MAEC que debe respetar la autoridad de examen.

11.1 La autoridad de examen identificará claramente la versión de examen de la capacidad y la versión del documento de requisitos de compatibilidad MAEC, además de la versión del lenguaje MAEC utilizada para determinar la observancia oficial de los requisitos de compatibilidad MAEC para cada capacidad.

11.2 La autoridad de examen especificará el o los tipos de funcionalidad de la capacidad (creación de contenido, almacenaje de contenido o consumo de contenido).

11.3 La autoridad de examen definirá y publicará muestras de materiales de prueba.

11.4 La autoridad de examen publicará información sobre la manera de participar en las pruebas de corrección de modo que las organizaciones puedan prepararse con la mayor antelación posible.

11.5 La autoridad de examen proporcionará un punto de contacto para la organización de las pruebas de corrección de las capacidades que declaran soporte de MAEC y que hayan rellenado el formulario "Cuestionario de compatibilidad MAEC".

11.6 La autoridad de examen puede volver a someter a prueba una capacidad cuya compatibilidad con MAEC se haya reconocido oficialmente, si lo estima conveniente.

12 Revocación

Si la autoridad de examen aprueba la compatibilidad con MAEC, pero posteriormente tiene evidencias de que ya no se están cumpliendo los requisitos, podrá revocar su aprobación y ya no se reconocerá oficialmente la compatibilidad MAEC de la capacidad. A continuación se indican los requisitos que debe tener en cuenta la autoridad de examen para revocar el reconocimiento.

12.1 La autoridad de examen dará al propietario de la capacidad un aviso de revocación al menos dos (2) meses antes de la fecha en que esté prevista la revocación.

12.2 La autoridad de examen puede retrasar la fecha de revocación.

12.3 Si la autoridad de examen concluye que las actuaciones o demandas del propietario de la capacidad son deliberadamente erróneas, puede obviar el periodo de aviso. La autoridad de examen puede interpretar como desee la expresión "deliberadamente erróneas".

12.4 Si la autoridad de examen determina que las actuaciones del propietario de la capacidad en relación con los requisitos de compatibilidad son deliberadamente erróneas, la revocación estará vigente por un periodo mínimo de un año.

12.5 La autoridad de examen identificará los requisitos específicos que no se cumplen.

12.6 Si el propietario de la capacidad considera que se cumplen los requisitos, podrá responder al aviso de revocación proporcionando detalles específicos que demuestren por qué la capacidad cumple los requisitos cuyo cumplimiento se ha cuestionado.

12.7 Si durante el periodo de aviso el propietario de la capacidad la modifica para que cumpla los requisitos en cuestión, la autoridad de examen debe detener la revocación de esa capacidad.

12.8 La autoridad de examen publicará la revocación del reconocimiento oficial de la correcta compatibilidad con MAEC de esa capacidad.

12.9 La autoridad de examen podrá hacer públicos los motivos de la revocación.

Bibliografía

[b-UIT-T X.1520] Recomendación ITU-T X.1520 (2011), *Vulnerabilidades y exposiciones comunes*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2014